



# **Administering Avaya Aura™ System Manager**

GA Release 6.0  
June 2010

## Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

## Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

## Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

## Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

## Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be

accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

## Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

## Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://www.avaya.com/support/Copyright/>.

## Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

## Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: <http://www.avaya.com/support/>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: [securityalerts@avaya.com](mailto:securityalerts@avaya.com).

## Trademarks

Avaya, the Avaya logo, Avaya Aura™ System Manager are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

## Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: <http://www.avaya.com/support>

## Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>

## Contents

|  |           |
|--|-----------|
| <b>Chapter 1: Avaya Aura System Manager overview.....</b>        | <b>15</b> |
| <b>Chapter 2: What is new in this release.....</b>               | <b>17</b> |
| <b>Chapter 3: Log on to System Manager.....</b>                  | <b>19</b> |
| Logging onto the System Manager web interface.....               | 19        |
| <b>Chapter 1: Managing elements.....</b>                         | <b>21</b> |
| Managing application instances.....                              | 21        |
| Managing application instances.....                              | 21        |
| Creating a new application instance.....                         | 21        |
| Viewing details of an application instance.....                  | 22        |
| Modifying an application instance.....                           | 23        |
| Deleting an application instance.....                            | 23        |
| Modifying an access point.....                                   | 23        |
| Assigning applications to an application instance.....           | 24        |
| Removing assigned applications.....                              | 24        |
| Creating a new port.....   | 25        |
| Modifying the port information.....                              | 25        |
| Deleting a port.....   | 26        |
| Creating an access point.....                                    | 26        |
| Deleting an access point.....                                    | 27        |
| Application Management field descriptions.....                   | 27        |
| Application Details field descriptions.....                      | 28        |
| Delete Application Confirmation field descriptions.....          | 34        |
| Assign Applications field descriptions.....                      | 34        |
| Import Applications field descriptions.....                      | 34        |
| Import Status field descriptions.....                            | 37        |
| Managing certificates.....                                       | 38        |
| About Trust Management.....                                      | 38        |
| Setting SCEP enrollment password.....                            | 38        |
| Adding trusted certificates.....                                 | 39        |
| Viewing trusted certificates.....                                | 40        |
| Removing trusted certificates.....                               | 41        |
| Viewing identity certificates.....                               | 41        |
| Replacing an identity certificate.....                           | 42        |
| Enrollment Password field descriptions.....                      | 42        |
| Trusted Certificates field descriptions.....                     | 43        |
| Add Trusted Certificate field descriptions.....                  | 43        |
| View Trust Certificate field descriptions.....                   | 45        |
| Delete Trusted Certificate Confirmation field descriptions.....  | 46        |
| Identity Certificates field descriptions.....                    | 46        |
| Replace Identity Certificate field descriptions.....             | 47        |
| System Manager- Communication Manager capabilities Overview..... | 48        |
| <b>Chapter 2: Managing endpoints.....</b>                        | <b>51</b> |
| Endpoints.....   | 51        |
| Endpoint Management.....   | 51        |
| Adding an endpoint.....  | 52        |

|   |    |
|---|----|
| Using Native Name.....                          | 52 |
| Editing an endpoint.....                        | 53 |
| Viewing an endpoint.....                        | 53 |
| Deleting an endpoint.....                       | 54 |
| Editing endpoint extensions.....                | 54 |
| Bulk adding endpoints.....                      | 55 |
| Bulk editing endpoints.....                     | 55 |
| Endpoint List.....                              | 56 |
| Filtering endpoints.....                        | 56 |
| Using Advanced Search.....                      | 57 |
| Add station Template.....                       | 57 |
| Edit Endpoint Extension field descriptions..... | 77 |
| Bulk Add Endpoint field descriptions.....       | 78 |
| Bulk Edit Endpoint field descriptions.....      | 79 |

**Chapter 3: Managing features.....81**

|  |     |
|--|-----|
| Communication Manager objects.....           | 81  |
| Communication Manager objects.....           | 81  |
| Adding Communication Manager objects.....    | 82  |
| Editing Communication Manager objects.....   | 83  |
| Viewing Communication Manager objects.....   | 83  |
| Deleting Communication Manager objects.....  | 84  |
| Filtering Communication Manager objects..... | 84  |
| Announcements.....                           | 85  |
| What is an announcement?.....                | 85  |
| Announcement List.....                       | 85  |
| Adding an announcement.....                  | 87  |
| Editing an announcement.....                 | 87  |
| Viewing an announcement.....                 | 88  |
| Deleting an announcement.....                | 88  |
| Saving an announcement.....                  | 88  |
| Backing up announcements.....                | 89  |
| Backing up all announcements.....            | 89  |
| Downloading announcements.....               | 90  |
| Restoring announcements.....                 | 90  |
| Restoring all announcements.....             | 91  |
| Moving an announcement.....                  | 91  |
| Broadcasting announcements.....              | 91  |
| File Transfer Settings in announcements..... | 92  |
| List Usage Extension in announcements.....   | 92  |
| Filtering the Announcements list.....        | 93  |
| Announcements field descriptions.....        | 93  |
| Audio Groups.....                            | 96  |
| What is an audio group?.....                 | 96  |
| Adding an audio group.....                   | 96  |
| Editing an audio group.....                  | 97  |
| Viewing an audio group.....                  | 97  |
| Deleting an audio group.....                 | 98  |
| More actions in audio groups.....            | 98  |
| Audio Groups field descriptions.....         | 99  |
| Messaging Class of Service.....              | 100 |

|  |            |
|--|------------|
| Viewing Class of Service.....                        | 100        |
| Class of Service List field descriptions.....        | 101        |
| Subscribers.....                                     | 101        |
| Subscriber Management.....                           | 101        |
| Adding a Subscriber.....                             | 102        |
| Editing a Subscriber.....                            | 102        |
| Viewing a Subscriber.....                            | 103        |
| Deleting a Subscriber.....                           | 103        |
| Subscriber List.....                                 | 104        |
| Filtering Subscribers.....                           | 104        |
| Subscribers (CMM) field descriptions.....            | 105        |
| Subscribers (MM) field descriptions.....             | 107        |
| Class of service.....                                | 110        |
| Class of Service.....                                | 110        |
| Editing Class of Service data.....                   | 111        |
| Viewing Class of Service data.....                   | 111        |
| Filtering the Class of Service list.....             | 112        |
| Class of Service field descriptions.....             | 112        |
| <b>Chapter 4: Managing inventory.....</b>            | <b>115</b> |
| Discovery Management.....                            | 115        |
| Discovery Management.....                            | 115        |
| SNMP Access list.....                                | 115        |
| Setting the order in the SNMP Access list.....       | 116        |
| Adding an SNMP Access profile.....                   | 117        |
| Editing an SNMP Access profile.....                  | 117        |
| Deleting an SNMP Access profile.....                 | 117        |
| SNMP Access field descriptions.....                  | 118        |
| Subnet(s) list.....                                  | 119        |
| Adding a subnet.....                                 | 120        |
| Editing a subnet.....                                | 120        |
| Deleting a subnet.....                               | 120        |
| CM Access list.....                                  | 121        |
| Filtering Subnet(s) and CM Access lists.....         | 121        |
| Adding a Communication Manager Access profile.....   | 122        |
| Editing a Communication Manager Access profile.....  | 122        |
| Deleting a Communication Manager Access profile..... | 122        |
| CM Access profile field descriptions.....            | 123        |
| Discovery.....                                       | 123        |
| Device Discovery.....                                | 123        |
| Discovering devices.....                             | 124        |
| Filtering Network Subnet(s).....                     | 124        |
| Discovering Devices field descriptions.....          | 125        |
| Discovered Inventory.....                            | 126        |
| Discovered Inventory.....                            | 126        |
| Network Device Inventory list.....                   | 126        |
| Viewing the Network Device Inventory list.....       | 126        |
| Filtering the Inventory list.....                    | 127        |
| Using Advanced Search in Discovered Inventory.....   | 127        |
| Network Device Inventory list field description..... | 128        |
| Synchronization of Data.....                         | 128        |

|  |             |
|--|-------------|
| Synchronizing Communication Manager and Messaging data.....        | 128         |
| Initializing Synchronization.....                                  | 129         |
| Incremental Synchronization.....                                   | 130         |
| Synchronizing Messaging Data.....                                  | 130         |
| Saving Communication Manager translations.....                     | 130         |
| Element Cut Through.....   | 131         |
| Element Cut Through User Reference.....                            | 131         |
| System Basics.....   | 133         |
| System Planning.....   | 144         |
| Managing Telephones.....   | 167         |
| Telephone Features.....  | 203         |
| Managing Attendant Consoles.....                                   | 239         |
| Managing Telephone Displays.....                                   | 254         |
| Handling Incoming Calls.....                                       | 264         |
| Routing Outgoing Calls.....  | 319         |
| Multimedia Calling — Multimedia Applications Server Interface..... | 340         |
| Screen References.....   | 418         |
| Configure Options.....   | 1060        |
| <b>Chapter 6: Managing templates.....</b>                          | <b>1061</b> |
| Templates.....   | 1061        |
| Template Management.....   | 1061        |
| Template Versioning.....   | 1061        |
| Adding Endpoint templates.....                                     | 1062        |
| Editing Endpoint templates.....                                    | 1062        |
| Viewing Endpoint templates.....                                    | 1063        |
| Deleting Endpoint templates.....                                   | 1063        |
| Duplicating Endpoint templates.....                                | 1063        |
| Distribution of templates.....                                     | 1064        |
| Viewing Associated Endpoints.....                                  | 1064        |
| Adding Subscriber templates.....                                   | 1065        |
| Editing Subscriber templates.....                                  | 1065        |
| Viewing Subscriber templates.....                                  | 1066        |
| Deleting Subscriber templates.....                                 | 1066        |
| Duplicating Subscriber templates.....                              | 1067        |
| Viewing Associated Subscribers.....                                | 1067        |
| Template List.....   | 1067        |
| Filtering Templates.....   | 1068        |
| Add station Template.....  | 1069        |
| Subscriber Templates (CMM) field descriptions.....                 | 1088        |
| Subscriber Templates (MM) field descriptions.....                  | 1090        |
| <b>Chapter 7: Managing events.....</b>                             | <b>1095</b> |
| Managing alarms.....   | 1095        |
| Alarming.....  | 1095        |
| Alarming field descriptions.....                                   | 1095        |
| Alarming field descriptions.....                                   | 1096        |
| Viewing alarms.....  | 1099        |
| Changing status of an alarm.....                                   | 1099        |
| Exporting alarms.....  | 1099        |
| Filtering alarms.....  | 1100        |
| Searching for alarms.....  | 1100        |

|   |      |
|---|------|
| Managing logs.....                                    | 1101 |
| Logging.....  | 1101 |
| Log Types.....  | 1101 |
| Viewing log details.....                              | 1102 |
| Searching for logs.....                               | 1103 |
| Filtering logs.....                                   | 1103 |
| Logging field descriptions.....                       | 1104 |
| Logging field descriptions.....                       | 1107 |
| Managing log settings.....                            | 1108 |
| Accessing the Log Settings service.....               | 1108 |
| Viewing loggers for a log file.....                   | 1109 |
| Logging Settings field descriptions.....              | 1109 |
| Editing a logger in a log file.....                   | 1110 |
| Managing harvested logs.....                          | 1114 |
| Log Harvester.....                                    | 1114 |
| Accessing log harvest.....                            | 1115 |
| Creating a new log harvesting profile.....            | 1115 |
| Viewing the harvested log files in an archive.....    | 1116 |
| Deleting a profile.....                               | 1116 |
| Submitting a request for harvesting log files.....    | 1117 |
| Viewing details of a log harvesting request.....      | 1117 |
| Searching for a text in a log file.....               | 1118 |
| Viewing the contents of the harvested log files.....  | 1118 |
| Downloading harvested log files.....                  | 1119 |
| Filtering log harvesting profiles.....                | 1120 |
| Filtering log harvesting requests.....                | 1121 |
| Viewing details of a log harvesting profile.....      | 1122 |
| Log Harvester field descriptions.....                 | 1122 |
| Create New Profile field descriptions.....            | 1123 |
| Profile Criteria View field descriptions.....         | 1124 |
| Harvest Archives field descriptions.....              | 1124 |
| Search Archives field descriptions.....               | 1126 |
| Harvest - View Harvest detail field descriptions..... | 1126 |

**Chapter 8: Managing Licenses.....1129**

|   |      |
|---|------|
| WebLM overview.....                                     | 1129 |
| Obtaining the license file.....                         | 1130 |
| Accessing WebLM.....                                    | 1131 |
| Installing a license file.....                          | 1131 |
| Viewing license capacity of features for a product..... | 1132 |
| Viewing peak usage for a licensed product.....          | 1132 |
| Removing a license file.....                            | 1133 |
| Viewing server properties.....                          | 1133 |
| WebLM Home field descriptions.....                      | 1134 |
| Install License field descriptions.....                 | 1134 |
| View License Capacity field descriptions.....           | 1134 |
| View Peak Usage field descriptions.....                 | 1135 |
| Uninstall License field descriptions.....               | 1136 |
| Server Properties field descriptions.....               | 1136 |
| Enterprise licensing.....                               | 1137 |
| Configuring enterprise licensing.....                   | 1137 |

|  |      |
|--|------|
| Adding a local WebLM server.....   | 1138 |
| Modifying a local WebLM server configuration.....                          | 1139 |
| Removing a local WebLM server.....   | 1139 |
| Viewing the license capacity of licensed features for a product.....       | 1140 |
| Viewing the connectivity status of local WebLM servers.....                | 1140 |
| Validating connectivity to local WebLM servers for a product.....          | 1141 |
| Viewing usage by WebLM.....  | 1141 |
| Viewing allocations by features.....                                       | 1142 |
| Viewing enterprise usage of a license feature.....                         | 1142 |
| Changing allocations of licensed features for a local WebLM server.....    | 1142 |
| Viewing periodic status of master and local WebLM servers.....             | 1143 |
| Specifying overuse limit for licensed features.....                        | 1143 |
| Querying usage of feature licenses for master and local WebLM servers..... | 1144 |
| Viewing allocations by local WebLM.....                                    | 1144 |
| Viewing usage summary.....   | 1145 |
| View by Feature field descriptions.....                                    | 1145 |
| View by Local WebLM field descriptions.....                                | 1145 |
| Enterprise Configuration field descriptions.....                           | 1146 |
| View Local WebLMs field descriptions.....                                  | 1148 |
| Add Local WebLM field descriptions.....                                    | 1148 |
| Modify Local WebLM field descriptions.....                                 | 1150 |
| Delete Local WebLM field descriptions.....                                 | 1151 |
| Usage Summary field descriptions.....                                      | 1152 |
| Usage by WebLM field descriptions.....                                     | 1152 |
| Enterprise Usage field descriptions.....                                   | 1153 |
| Query Usage field descriptions.....  | 1154 |
| Allocations by Features field descriptions.....                            | 1155 |
| Allocations by Local WebLM field descriptions.....                         | 1156 |
| Change Allocations field descriptions.....                                 | 1157 |
| Periodic Status field descriptions.....                                    | 1158 |
| Overuse field descriptions.....  | 1159 |

**Chapter 9: Managing groups, roles and resources.....1161**

|  |      |
|--|------|
| Managing groups.....                                   | 1161 |
| Manage groups.....                                     | 1161 |
| Group Management.....                                  | 1161 |
| Viewing Groups.....                                    | 1162 |
| Creating groups.....                                   | 1162 |
| Modifying Groups.....                                  | 1163 |
| Creating duplicate groups.....                         | 1163 |
| Deleting groups.....                                   | 1164 |
| Moving groups.....                                     | 1165 |
| Importing groups.....                                  | 1165 |
| Synchronizing resources for a resource type.....       | 1166 |
| Switching to table view.....                           | 1166 |
| Switching to tree view.....                            | 1167 |
| Assigning resources to a group.....                    | 1168 |
| Searching for resources.....                           | 1169 |
| Searching for resources based on group membership..... | 1170 |
| Filtering groups.....                                  | 1171 |
| Filtering resources.....                               | 1171 |

|   |      |
|---|------|
| Searching Groups.....   | 1172 |
| Removing assigned resources from a group.....                         | 1173 |
| Group Management field descriptions.....                              | 1173 |
| View Group field descriptions.....                                    | 1176 |
| New Group field descriptions.....                                     | 1177 |
| Edit Group field descriptions.....                                    | 1179 |
| Delete Group Confirmation field descriptions.....                     | 1181 |
| Duplicate Group field descriptions.....                               | 1182 |
| Move Group field descriptions.....                                    | 1182 |
| Import Groups field descriptions.....                                 | 1183 |
| Resource Synchronization field descriptions.....                      | 1183 |
| Resources field descriptions.....                                     | 1183 |
| Managing resources.....   | 1186 |
| Manage resources.....   | 1186 |
| Accessing resources.....  | 1186 |
| Assigning resources to a new group.....                               | 1186 |
| Adding resources to a selected group.....                             | 1188 |
| Searching for resources.....  | 1188 |
| Filtering resources.....  | 1189 |
| New Group field descriptions.....                                     | 1190 |
| Resources field descriptions.....                                     | 1191 |
| Choose Group field descriptions.....                                  | 1194 |
| Choose Parent Group field descriptions.....                           | 1194 |
| Managing roles.....   | 1195 |
| Manage Roles.....   | 1195 |
| Types of default roles.....   | 1196 |
| Viewing user roles.....   | 1196 |
| Creating a role.....  | 1197 |
| Modifying user roles.....   | 1197 |
| Creating duplicate roles.....   | 1198 |
| Deleting user roles.....  | 1198 |
| Searching for roles.....  | 1199 |
| Filtering roles.....  | 1199 |
| Assigning users to roles.....   | 1200 |
| Removing users from roles.....  | 1200 |
| Bulk importing roles.....   | 1201 |
| Exporting roles in bulk.....  | 1202 |
| Viewing details of role import jobs.....                              | 1203 |
| Scheduling a role importing job.....                                  | 1203 |
| Viewing a role import job in Scheduler.....                           | 1204 |
| Aborting a role importing job on first error.....                     | 1205 |
| Canceling a role import job.....                                      | 1205 |
| Deleting a role importing job.....                                    | 1206 |
| Downloading error records for an unsuccessful role importing job..... | 1206 |
| Assigning permissions to a role.....                                  | 1207 |
| Removing permissions from a role.....                                 | 1208 |
| Adding groups and resources to a permission.....                      | 1208 |
| Removing groups and resources from a permission.....                  | 1209 |
| Adding attributes to a role.....                                      | 1209 |
| Removing attributes from a permission.....                            | 1210 |
| Manage Roles field descriptions.....                                  | 1211 |

|   |             |
|---|-------------|
| New Role field descriptions.....                          | 1212        |
| Edit Role field descriptions.....                         | 1215        |
| View Role field descriptions.....                         | 1217        |
| Duplicate Role field descriptions.....                    | 1218        |
| Assign Users To Roles field descriptions.....             | 1220        |
| UnAssign Roles field descriptions.....                    | 1221        |
| Select Groups and Resources field descriptions.....       | 1221        |
| Select Attributes field descriptions.....                 | 1222        |
| Import Roles field descriptions.....                      | 1223        |
| Import Roles – Job Details field descriptions.....        | 1225        |
| <b>Chapter 10: Managing network routing policies.....</b> | <b>1227</b> |
| Managing Session Manager routing.....                     | 1227        |
| Overview of Session Manager routing.....                  | 1227        |
| Prerequisites for Routing Setup.....                      | 1228        |
| Routing.....  | 1228        |
| Domains.....  | 1233        |
| Locations.....  | 1237        |
| Adaptations.....  | 1242        |
| SIP Entities.....   | 1255        |
| SIP Entity References.....                                | 1265        |
| Entity Links.....   | 1266        |
| Time Ranges.....  | 1270        |
| Routing Policies.....                                     | 1274        |
| Dial Patterns.....  | 1281        |
| Regular Expressions.....                                  | 1288        |
| Defaults.....   | 1293        |
| <b>Chapter 13: Managing System Manager Data.....</b>      | <b>1297</b> |
| Administering backup and restore.....                     | 1297        |
| Backup and Restore.....                                   | 1297        |
| Viewing list of backup files.....                         | 1297        |
| Creating a data backup on a local computer.....           | 1298        |
| Scheduling a data backup on a local computer.....         | 1298        |
| Restoring a data backup from a local machine.....         | 1299        |
| Viewing data retention rules.....                         | 1299        |
| Modifying data retention rules.....                       | 1299        |
| Accessing the Data Retention Rules service.....           | 1300        |
| Viewing loggers for a log file.....                       | 1300        |
| Assigning an appender to a logger.....                    | 1300        |
| Editing a logger in a log file.....                       | 1301        |
| Modifying an appender.....                                | 1302        |
| Removing an appender from a logger.....                   | 1302        |
| Backup And Restore field descriptions.....                | 1303        |
| Backup field descriptions.....                            | 1303        |
| Schedule Backup field descriptions.....                   | 1304        |
| Restore field descriptions.....                           | 1305        |
| Data Retention field descriptions.....                    | 1306        |
| Logging Settings field descriptions.....                  | 1306        |
| Edit Logger field descriptions.....                       | 1307        |
| Edit Appender field descriptions.....                     | 1308        |
| Attach Appender field descriptions.....                   | 1309        |

|  |      |
|--|------|
| Managing data retention rules.....                   | 1310 |
| Accessing the Data Retention Rules service.....      | 1310 |
| Data retention rules.....                            | 1310 |
| Viewing data retention rules.....                    | 1310 |
| Modifying data retention rules.....                  | 1311 |
| Data Retention field descriptions.....               | 1311 |
| Data Replication Service.....                        | 1312 |
| Data Replication Service.....                        | 1312 |
| Viewing replica groups.....                          | 1312 |
| Viewing replica nodes in a replica group.....        | 1313 |
| Repairing a replica node.....                        | 1313 |
| Repairing all replica nodes in a replica group.....  | 1314 |
| Viewing replication details for a replica node.....  | 1314 |
| Replica Groups field descriptions.....               | 1315 |
| Replica Nodes field descriptions.....                | 1315 |
| Data Replication field descriptions.....             | 1317 |
| Managing scheduled jobs.....                         | 1318 |
| Scheduler.....                                       | 1318 |
| Accessing scheduler.....                             | 1318 |
| Viewing pending jobs.....                            | 1319 |
| Viewing completed jobs.....                          | 1319 |
| Viewing details of a pending job.....                | 1319 |
| Viewing details of a completed job.....              | 1320 |
| Viewing details of a pending job.....                | 1320 |
| Viewing logs for a job.....                          | 1320 |
| Viewing completed jobs.....                          | 1321 |
| Filtering Jobs.....                                  | 1321 |
| Editing a job.....                                   | 1322 |
| Deleting a job.....                                  | 1323 |
| Disabling a job.....                                 | 1324 |
| Enabling a job.....                                  | 1324 |
| Stopping a Job.....                                  | 1325 |
| Pending Jobs field descriptions.....                 | 1325 |
| Completed Jobs field descriptions.....               | 1327 |
| Job Scheduling-View Job field descriptions.....      | 1330 |
| Job Scheduling-Edit Job field descriptions.....      | 1331 |
| Job Scheduling-On Demand Job field descriptions..... | 1332 |
| Disable Confirmation field descriptions.....         | 1333 |
| Stop Confirmation field descriptions.....            | 1334 |
| Delete Confirmation field descriptions.....          | 1335 |
| Setting service profiles for applications.....       | 1336 |
| About Service Profile Management.....                | 1336 |
| Edit global feature profiles.....                    | 1336 |
| View global feature profiles.....                    | 1337 |
| Edit Profile System Manager field descriptions.....  | 1337 |
| View Profile System Manager field descriptions.....  | 1338 |
| Edit software feature profiles.....                  | 1338 |
| View software feature profiles.....                  | 1339 |
| View Profile:Licenses field descriptions.....        | 1339 |
| Edit Profile:Licenses field descriptions.....        | 1340 |
| Edit Profile:Alarming UI field descriptions.....     | 1341 |

|   |      |
|---|------|
| View Profile:Alarming UI field descriptions.....                                    | 1341 |
| View Profile Enterprise Directory Synchronization field descriptions.....           | 1342 |
| Edit Profile Enterprise Directory Synchronization field descriptions.....           | 1344 |
| Synchronizing users with Active Directory.....                                      | 1346 |
| System Manager security authentication mechanism.....                               | 1347 |
| View Profile:IAM field descriptions.....  | 1348 |
| Edit Profile:IAM field descriptions.....  | 1355 |
| View Profile: System Manager Element Manager field descriptions.....                | 1361 |
| Edit Profile: System Manager Element Manager field descriptions.....                | 1363 |
| View Profile:Logging field descriptions.....  | 1364 |
| Edit Profile:Logging field descriptions.....  | 1365 |
| View Profile:Logging Service field descriptions.....                                | 1366 |
| Edit Profile:Logging Service field descriptions.....                                | 1367 |
| View Profile:Scheduler field descriptions.....                                      | 1368 |
| Edit Profile:Scheduler field descriptions.....                                      | 1369 |
| View Profile:SNMP field descriptions.....   | 1370 |
| Edit Common Console Profile field descriptions.....                                 | 1371 |
| View Common Console Profile field descriptions.....                                 | 1372 |
| Edit Profile: Communication System Management Configuration field descriptions..... | 1372 |
| View Profile: Communication System Management Configuration field descriptions..... | 1373 |
| Edit Profile: Role Bulk Import Profile field descriptions.....                      | 1374 |
| View Profile: Role Bulk Import Profile field descriptions.....                      | 1376 |
| Edit Profile: User Bulk Import Profile field descriptions.....                      | 1378 |
| View Profile: User Bulk Import Profile field descriptions.....                      | 1379 |
| View Profile: Agent Management field descriptions.....                              | 1381 |
| View Profile: Alarm Management field descriptions.....                              | 1383 |
| View Profile: Event processor field descriptions.....                               | 1384 |
| View Profile : Data Transport Config field descriptions.....                        | 1385 |
| View Profile: Data Transport Static Config field descriptions.....                  | 1388 |

**Chapter 14: Managing Users.....1389**

|   |      |
|---|------|
| Managing users.....                                     | 1389 |
| Manage users, public contacts and shared address.....   | 1389 |
| User Management.....                                    | 1389 |
| Users in Management Console.....                        | 1390 |
| Viewing details of a user.....                          | 1390 |
| Modifying user accounts.....                            | 1390 |
| Creating a new user profile.....                        | 1391 |
| Creating duplicate users.....                           | 1391 |
| Creating a user on communication management system..... | 1392 |
| Removing user accounts.....                             | 1392 |
| Filtering users.....                                    | 1393 |
| Searching for users.....                                | 1394 |
| Assigning roles to a user.....                          | 1394 |
| Assigning roles to multiple users.....                  | 1395 |
| Removing roles from a user.....                         | 1395 |
| Assigning groups to a user.....                         | 1396 |
| Assigning groups to multiple users.....                 | 1397 |
| Removing a user from groups.....                        | 1397 |
| Viewing deleted users.....                              | 1398 |
| Restoring a deleted user.....                           | 1398 |

|   |      |
|---|------|
| Deleting the deleted users.....                         | 1398 |
| Assigning users to roles.....                           | 1399 |
| Removing users from roles.....                          | 1399 |
| Managing addresses.....                                 | 1400 |
| Managing bulk importing and exporting.....              | 1404 |
| Managing communication profiles.....                    | 1560 |
| Managing default contact list of the user.....          | 1595 |
| Managing private contacts of a user.....                | 1602 |
| User Management field descriptions.....                 | 1615 |
| User Profile View field descriptions.....               | 1617 |
| User Profile Edit field descriptions.....               | 1623 |
| New User Profile field descriptions.....                | 1633 |
| User Profile Duplicate field descriptions.....          | 1642 |
| User Delete Confirmation field descriptions.....        | 1648 |
| Assign Roles to Multiple Users field descriptions.....  | 1648 |
| Assign Roles field descriptions.....                    | 1649 |
| Assign Groups field descriptions.....                   | 1649 |
| Assign Groups to Multiple Users field descriptions..... | 1650 |
| Deleted Users field descriptions.....                   | 1651 |
| User Restore Confirmation field descriptions.....       | 1652 |
| Change Password field descriptions.....                 | 1652 |
| Assign Users To Roles field descriptions.....           | 1653 |
| UnAssign Roles field descriptions.....                  | 1654 |
| Managing public contacts.....                           | 1655 |
| Manage public contact list.....                         | 1655 |
| Adding a new public contact.....                        | 1655 |
| Modifying the details of a public contact.....          | 1656 |
| Deleting public contacts.....                           | 1656 |
| Viewing the details of a public contact.....            | 1657 |
| Adding a postal address of a public contact.....        | 1657 |
| Modifying a postal address of a public contact.....     | 1658 |
| Deleting postal addresses of a public contact.....      | 1658 |
| Choosing a shared address for a public contact.....     | 1659 |
| Adding a contact address of a public contact.....       | 1659 |
| Modifying the details of a public contact.....          | 1660 |
| Deleting contact addresses of a public contact.....     | 1660 |
| Add Address field descriptions.....                     | 1661 |
| Choose Address field descriptions.....                  | 1661 |
| View Public Contact field descriptions.....             | 1662 |
| Edit Public Contact field descriptions.....             | 1663 |
| New Public Contact field descriptions.....              | 1665 |
| Public Contacts field descriptions.....                 | 1667 |
| Add Address field descriptions.....                     | 1668 |
| Edit Address field descriptions.....                    | 1669 |
| Managing shared addresses.....                          | 1670 |
| Manage shared address.....                              | 1670 |
| Choosing a shared address.....                          | 1670 |
| Adding a shared address.....                            | 1671 |
| Modifying a shared address.....                         | 1671 |
| Deleting a shared address.....                          | 1671 |
| Add Address field descriptions.....                     | 1672 |

|   |             |
|---|-------------|
| Shared Address field descriptions.....                    | 1673        |
| Managing presence access control lists.....               | 1673        |
| Manage Presence access control lists.....                 | 1673        |
| Viewing details of a high priority enforced ACL rule..... | 1674        |
| Modifying a high priority enforced ACL rule.....          | 1675        |
| Creating a new high priority enforced ACL rule.....       | 1675        |
| Deleting high priority enforced ACL rules.....            | 1676        |
| Viewing details of a low priority enforced ACL rule.....  | 1676        |
| Modifying a low priority enforced ACL rule.....           | 1676        |
| Creating a low priority enforced ACL rule.....            | 1677        |
| Deleting low priority enforced ACL rules.....             | 1678        |
| Viewing details of a System ACL rule.....                 | 1678        |
| Modifying a System ACL rule.....                          | 1678        |
| Creating a new System ACL rule.....                       | 1679        |
| Deleting System ACL rules.....                            | 1680        |
| Defining a new policy for Enforced User ACL rules.....    | 1680        |
| Modifying a policy for Enforced User ACL rules.....       | 1681        |
| Deleting policies for Enforced User ACL rules.....        | 1681        |
| Creating a system rule.....                               | 1682        |
| Modifying a System rule.....                              | 1682        |
| Deleting system rules.....                                | 1683        |
| Filtering presentities.....                               | 1683        |
| Searching for presentities.....                           | 1684        |
| Filtering watchers.....                                   | 1684        |
| Searching for watchers.....                               | 1685        |
| Presence ACL field descriptions.....                      | 1685        |
| New Enforced User ACL field descriptions.....             | 1689        |
| Edit Enforced User ACL field descriptions.....            | 1692        |
| View Enforced User ACL field descriptions.....            | 1694        |
| New System ACL field descriptions.....                    | 1696        |
| Edit System ACL field descriptions.....                   | 1698        |
| View System ACL field descriptions.....                   | 1700        |
| New System Rule field descriptions.....                   | 1701        |
| Edit System Rule field descriptions.....                  | 1702        |
| <b>Index.....</b>   | <b>1705</b> |

# Chapter 1: Avaya Aura System Manager overview

System Manager is a central management system that delivers a set of shared management services and a common console for System Manager and its components. System Manager includes the following shared management services:

| Service             | Description   |
|---------------------|---|
| Elements            | Provides you features offered by individual components of System Manager. Except some links that provide access to generic features provided by System Manager, most of the links provides access to features provided by different components of System Manager.   |
| Events              | Provides you features for administering alarms and logs generated by System Manager and other components of System Manager. You can view and change the status of alarms. For logs, you can view logs, harvest logs for System Manager and its components, and manage loggers and appender.   |
| Groups & Roles      | Provides you features for administering groups and roles. You can create and manage groups, roles, and permissions.   |
| Licenses            | Provides you features for administering licenses for individual components of Avaya Aura Unified Communication System.  |
| Routing             | Provides you features for managing routing applications. You can create and manage routing applications that includes Domains, Adaptations, SIP Entities, Entity Links, Time Ranges, Policies, Dial Patterns, and Regular Expressions to configure your network configuration.  |
| Security            | Provides you the features for configuring certificates  |
| System Manager Data | Provides you features for: <ul style="list-style-type: none"><li>• Backing up and restoring System Manager configuration data.</li><li>• Monitoring and scheduling jobs.</li><li>• Replicating data from remote nodes.</li><li>• Configuring data retention settings and profile for various services provided by System Manager.</li></ul> |
| Users               | Provides you the features to administer users, shared address, public contact list and system presence access control list information. You can create and manage user profiles. You can associate the user   |

| Service | Description   |
|---------|---|
|         | profiles with groups, roles, communication profiles, create a contact list, add address, and private contacts for the user. |

## Chapter 2: What is new in this release

- Avaya Aura™ System Manager 6.0 supports a new navigation pane with new navigation paths
- Synchronization of with System Manager Communication Manager 6.0
- Support for Avaya Aura™ Messaging 6.0 and Communication Manager Messaging 6.0
- Versioning of endpoint templates – support for Communication Manager 5.x, and Communication Manager 6.0
- Support for 1408, 1416, and H.323 set types
- Support for Advanced Encryption Standard (AES)
- Support for Class Of Service (COS) object and COS administration
- Support for administration of announcements and audio groups
- Support for new fields:
  - **Location** field in endpoint management – this field is applicable to all the H.323 and SIP endpoint types.
  - **Voice Mail Number** field in endpoint management and associated endpoint templates- this field is available for the SIP set types.
  - **Logged off/PSA/TTI** field on the Coverage path object
  - **Redirect to** field in Hunt groups – the **Redirect VDN** field is modified to **Redirect To** in Hunt Groups
  - **Vdn** field in Hunt groups
  - **Work State Can Be Forced** field in COR object
  - **Can Force Work State** field in COR object
- Support for increase in hunt groups to 8000 in the Hunt group object
- Support for increase in vectors to 8000 in the Vectors object
- Support for increase in Policy Routing Table to 8000 in the VDN object
- Support for the Per Button Ring Control feature in SIP endpoints
- Support for the Japanese Katakana font
- Bulk import and export of endpoint and messaging profiles in User Profile Management
- Support for log harvesting of event and debug logs
- **Device Discovery Management**- The Discovery Management feature allows you to configure System Manager to discover specific devices within the network.

What is new in this release

# Chapter 3: Log on to System Manager

---

## Logging onto the System Manager web interface

The System Manager web interface is the main interface to the Avaya Aura System Manager. You must log onto the Management Console web interface before you can perform any tasks.

 **Important:**

System Manager does not support the browser back functionality. It is not advisable to use the browser back button to navigate to the previously visited pages. Use of the back button may give unpredictable results. You must use the System Manager menu to navigate across pages.

### Prerequisites

You must have a user account to log on to the System Manager interface. Contact your system administrator if you do not have an user account.

- 
1. In the browser enter the Avaya Aura System Manager URL (`https://<SERVER_NAME>/SMGR`) and click **Enter**.
  2. In the **Username** field enter the user name.
  3. In the **Password** field enter the password.
  4. Click **Log On**.

If your user name and password:

- Match an authorized System Manager user account, System Manager displays the Avaya Aura System Manager Home page with Avaya Aura System Manager Version *version\_number*. The System Manager home page displays navigation menu in the left pane. The menu provides access to shared services using which you can perform various operations supported by System Manager. What you see and can do from there depends on your user role.

The content page in the right pane displays short cut links that provides access to the shared services.

## Log on to System Manager

- Do not match an authorized System Manager user account, System Manager displays an error message and prompts you to enter the user name and password so that you can log in again.
-

# Chapter 1: Managing elements

---

## Managing application instances

---

### Managing application instances

System Manager provides an interface to keep a track of the instances of applications running on different servers in an enterprise. You can perform the following operations:

- Add an entry for an application instance
- Modify an entry for application instance
- Delete an entry for application instance
- Assign and Remove an entry for applications

Using this service you can also

- Issue a certificate to an application instance
- Replace an existing certificate

---

### Creating a new application instance

System Manager supports Media Gateway and gateway 1.0 device types while adding an application instance.

#### Prerequisites

You must have a Trust Management type entry in the **Access point** section for the application instance.

- 
1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
  2. On the Application Management page, click **New**.

3. On the New Application Instance page, enter the appropriate details in the **Application, Port, Access Point, and Attributes** sections.
4. Click **Commit** .

When you add an application entity through RTS (Runtime Topology Service), it in turn starts a synchronization job in the background to bring all the relevant data from the application instances to the Communication System Management database. You can check the status of this synchronization job on the System Manager console by accessing **System Manager Data > Scheduler** or in the log files on the Communication System Management server.

 **Note:**

The following information applies if you are creating an instance of messaging:

- The details (FQDN or IP address) in the Node field for a messaging instance should correspond to that of MSS (Messaging Storage Server) and not MAS (Messaging Application Server).
- You have to add the System Manager or Communication System Management server details in the Trusted Server list on the Messaging box (in Messaging Administration/ Trusted Servers screen), before adding the Messaging box in the System Manager applications.
- The login credentials between the Messaging box trusted servers screen and the Session Manager application, entity, or attributes for a Messaging type of application have to match.
- The Trusted Server Name field on the Trusted Server page is mapped to the Login field in the Attributes section. Similarly the Password field on the Trusted Server page is mapped to the Password field in the Attributes section.
- You should set the **LDAP Access Allowed** field on the trusted server page to yes, to allow LDAP access to this Messaging box from the trusted server that you add.

---

## Viewing details of an application instance

- 
1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
  2. On the Application Management page, click an instance.
  3. Click **View**.
-

## Result

The View Application Instance page displays the details of the selected instance.

---

## Modifying an application instance

- 
1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
  2. On the Application Management page, click an application instance and perform one of the following steps:
    - Click **Edit**.
    - Click **View > Edit**.
  3. On the Edit Application Instance page, modify the appropriate details in the **Application, Port, Access Point, Attributes** sections.
  4. Click **Commit** to save the changes.
- 

---

## Deleting an application instance

- 
1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
  2. On the Application Management page, click an instance.
  3. Click **Delete**.
  4. On the Delete Application Confirmation page, click **Delete**.
- 

---

## Modifying an access point

- 
1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
  2. On the Application Management page, perform one of the following steps:

- Click **New**.
  - If you want to configure an access point for an existing application instance, click an instance and then click **Edit**.
  - If you want to configure an access point for an existing application instance, click an instance and click **View > Edit**.
3. Click an access point in the **Access Point** section and click **Edit**.
  4. Modify the access point information in the following mandatory fields: **Name, Access Point Type, Protocol, Host, Port, Order**.
  5. Click **Save**.
- 

---

## Assigning applications to an application instance

---

1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
  2. On the Application Management page, perform one of the following steps:
    - Select an application instance and then click **Edit**.
    - If you want to assign applications to an existing application instance in the view mode, select an instance and click **View > Edit**.
  3. Click **Assign Applications** in the Assign Applications section.
  4. On the Assign Applications page, select applications and click **Assign**.
- 

---

## Removing assigned applications

---

1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
2. On the Application Management page, perform one of the following steps:
  - If you want to remove assigned applications from an existing application instance, click an instance and then click **Edit**.

- If you want to remove assigned applications from an existing application instance, click an instance and click **View > Edit**.
3. Select applications and click **Unassign Applications** in the **Assign Applications** section.
- 

---

## Creating a new port

---

1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
  2. On the Application Management page, perform one of the following steps:
    - Click **New**.
    - If you want to configure a port for an existing application instance, click an instance and then click **Edit**.
    - If you want to configure a port for an existing application instance, click an instance and click **View > Edit**.
  3. Click **New** in the **Port** section.
  4. Enter the information about the port in the following mandatory fields: **Name**, **Protocol**, **Port**.
  5. Click **Save**.
- 

### Result

The table in the **Port Details** section displays the new port.

---

## Modifying the port information

---

1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
2. On the Application Management page, perform one of the following steps:
  - Click **New**.
  - If you want to configure a port for an existing application instance, click an instance and then click **Edit**.

- If you want to configure a port for an existing application instance, click an instance and click **View > Edit**.
3. Click **Edit** in the **Port** section.
  4. Modify the port information in the following fields: **Name, Protocol, Port, Description**.
  5. Click **Save** to save the changes to the database.
- 

---

## Deleting a port

1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
  2. On the Application Management page, perform one of the following steps:
    - Click **New**.
    - If you want to configure a port for an existing application instance, click an instance and then click **Edit**.
    - If you want to configure a port for an existing application instance, click an instance and click **View > Edit**.
  3. Click a port and click **Delete** in the **Port** section.
- 

### Result

Deletes the selected port from the table in the **Ports** section.

---

## Creating an access point

1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
2. On the Application Management page, perform one of the following steps:
  - Click **New**.
  - If you want to configure an access point for an existing application instance, click an instance and then click **Edit**.

- If you want to configure an access point for an existing application instance, click an instance and click **View > Edit**.
3. Click **New** in the **Access Point** section.
  4. Enter the information about the access point in the following mandatory fields: **Name, Access Point Type, Protocol, Host, Port, Order**.
  5. Click **Save**.
- 

---

## Deleting an access point

1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
2. On the Application Management page, perform one of the following steps:
  - Click **New**.
  - If you want to configure an access point for an existing application instance, click an instance and then click **Edit**.
  - If you want to configure an access point for an existing application instance, click an instance and click **View > Edit**.
3. Click an access point in the **Access Point** section and click **Delete**.

**Note:**

You cannot delete an access point that is of type Trust Management.

---



---

## Application Management field descriptions

Use this page to view the create, edit, view and delete instances of the application.

| Name                | Description  |
|---------------------|--|
| <b>Name</b>         | Name of the application instance.                                    |
| <b>Node</b>         | The node on which the application is running.                        |
| <b>Registration</b> | The registration status of the application instance. The values are: |

| Name               | Description   |
|--------------------|---|
|                    | <ul style="list-style-type: none"> <li>• True: Indicates a registered instance.</li> <li>• False: Indicates an unregistered instance</li> </ul> |
| <b>Description</b> | A brief description about the instance.   |

| Button                                 | Description   |
|--|---|
| <b>View</b>                            | Opens the View application page. Use this page to view the details of the selected application instance.                          |
| <b>Edit</b>                            | Opens the Edit Application page. Use this page to modify the information of the instance.   |
| <b>Delete</b>                          | Opens the Delete Application Confirmation page. Use this page to delete a selected application instance.                          |
| <b>Configure Trusted Certificates</b>  | Opens the Trusted Certificates page. Use this page to view, add and delete the trusted certificates for the application instance. |
| <b>Configure Identity Certificates</b> | Opens the Identity Certificates page. Use this page to view and replace the identity certificates for the application instance.   |
| <b>Filter: Enable</b>                  | Displays fields under select columns that you can use to set filter criteria. This is a toggle button.                            |
| <b>Filter: Disable</b>                 | Hides the column filter fields. This is a toggle button.  |
| <b>Filter: Apply</b>                   | Filters application instances based on the filter criteria.   |
| <b>Select: All</b>                     | Selects all the application instances in the table.   |
| <b>Select: None</b>                    | Clears the selection for the users that you have selected.  |
| <b>Refresh</b>                         | Refreshes the application instance information in the table.  |

---

## Application Details field descriptions

Use this page to add and edit an application instance.

### Application

| Name               | Description  |
|--------------------|--|
| <b>Name</b>        | The name of the instance.  |
| <b>Type</b>        | The type of the application to which the instance belongs.         |
| <b>Description</b> | A brief description about the instance.                            |
| <b>Node</b>        | Select the node on which you want to run the application instance. |

| Name              | Description  |
|-------------------|--|
| <b>Other Node</b> | The node on which you want to run the application instance.<br><br> <b>Note:</b><br>The page displays this field when you select <b>Other</b> from the <b>Node</b> field. |

## Port

| Name               | Description  |
|--------------------|--|
| <b>Name</b>        | The name of the port.                                |
| <b>Port</b>        | The port on the application instance is running.     |
| <b>Protocol</b>    | The protocol associated with the corresponding port. |
| <b>Description</b> | A brief description about the port.                  |

| Button        | Description   |
|---------------|---|
| <b>New</b>    | Displays fields in the <b>Port</b> section that you can use to add the port details.  |
| <b>Edit</b>   | Displays fields in the <b>Port</b> section with port information. You can modify the port details in the port mode.   |
| <b>Delete</b> | Deletes the selected configured port.   |
| <b>Save</b>   | Saves the port details.<br><br> <b>Note:</b><br>The section displays this button only when you click <b>Add</b> or <b>Edit</b> in the <b>port</b> section.   |
| <b>Cancel</b> | Cancels the operation of creating or editing an access point and hides the fields that you use to enter or modify the port information.<br><br> <b>Note:</b><br>The section displays this button only when you click <b>Add</b> or <b>Edit</b> in the <b>port</b> section. |

## Access Point

| Name                     | Description   |
|--------------------------|---|
| <b>Name</b>              | The name of the access point.   |
| <b>Access Point Type</b> | The type of the access point.<br>The options are: <ul style="list-style-type: none"> <li>• EMURL: Use this option to create a URL type access point .</li> <li>• Other</li> </ul> |

| Name            | Description  |
|-----------------|--|
| <b>Protocol</b> | The protocol that the application instance supports to communicate with other communication devices. |
| <b>Host</b>     | The name of the host on which the application instance is running.                                   |
| <b>Port</b>     | The port on which the application instance is running.   |
| <b>Order</b>    | The order in which the access points are accessed.   |

| Button        | Description   |
|---------------|---|
| <b>New</b>    | Displays fields in the <b>Access Point</b> section that you can use to add port details.                |
| <b>Edit</b>   | Displays fields in the <b>Access Point</b> section that allows you to modify the selected port details. |
| <b>Delete</b> | Deletes the selected access point.  |

These fields appear when you click **Add** or **Edit** in the **Access Point** section.

| Name                     | Description   |
|--------------------------|---|
| <b>Name</b>              | The name of the access point.   |
| <b>Access Point Type</b> | The type of the access point.<br>The options are: <ul style="list-style-type: none"> <li>• EMURL: Use this option to create a URL type access point .</li> <li>• Other</li> </ul> |
| <b>Protocol</b>          | The protocol for communicating with the application instance.   |
| <b>Host</b>              | The name of the host on which the application instance is running.  |
| <b>Port</b>              | The port on which the application instance is running.  |
| <b>Order</b>             | The order in which the access points are accessed.  |
| <b>User Name</b>         | The name of the user who can access the application instance.   |
| <b>Password</b>          | The password that authenticates the user.   |

| Button        | Description  |
|---------------|--|
| <b>Save</b>   | Saves the access point details.<br><br> <b>Note:</b><br>This button is visible only when you click <b>Add</b> and <b>Edit</b> in the <b>Access Point</b> section. |
| <b>Cancel</b> | Cancels the operation of creating or editing an access point and hides the fields that you use to enter or modify the access point information.  |

| Button | Description   |
|--------|---|
|        |  <b>Note:</b><br>This button is available only when you click <b>Add</b> and <b>Edit</b> in the <b>Access Point</b> section. |

## Attributes

This section provides information about attributes fields that you can configure for the selected application.

| Name                                      | Description  |
|---|--|
| <b>Login</b>                              | Login name to be used for connecting to the application instance.<br><br> <b>Note:</b><br>craft, craft2, dadmin, inads, init, rasaccess, sroot, and tsc are the restricted logins when you configure a Communication Manager.<br><br> <b>Note:</b><br>Do not use this login to connect to CM from any other application or to connect to the Communication Manager SAT terminal using CLI. |
| <b>Password</b>                           | Password which authenticates the SSH/ Telnet login name on the application instance. This field is not required for ASG login.   |
| <b>Is SSH Connection</b>                  | Use this check box to specify whether the SSH connection should be used to connect to the application instance. By default this is selected. If you clear the check box, the connection with the application instance is made using Telnet.  |
| <b>Port</b>                               | The port on which the service provided by the application instance is running. The default SSH port is 5022.   |
| <b>Alternate IP Address</b>               | Alternate IP address of the application instance. This is the IP address of the standby server in case of duplex servers.  |
| <b>RSA SSH Fingerprint (Primary IP)</b>   | The RSA SSH key of the CM Server. In case of Duplex servers, RSA SSH Key is the key of the Active server.  |
| <b>RSA SSH Fingerprint (Alternate IP)</b> | The DSA SSH Key of the CM Server used only in case of Duplex servers. This is the key of the Standby server.   |
| <b>Is ASG Enabled</b>                     | Use this check box to enable ASG. If you select the <b>Is ASG enabled</b> check box, then you should enter the ASG key. Password is not required.  |
| <b>ASG Key</b>                            | The ASG key used to authenticate the ASG login. You do not have to enter any value in this field if non-ASG login is used.   |
| <b>Location</b>                           | The location of the application instance.  |

The following fields provides information about attributes related to messaging.

| Name                           | Description   |
|--------------------------------|---|
| <b>Login</b>                   | Name as given in the Trusted Server Name field of the Trusted Servers page on the Messaging Box for this server.  |
| <b>Password</b>                | Password for the login name as given in the Password field of the Trusted Servers page on the Messaging Box for this server.  |
| <b>Confirm Password</b>        | You should retype the password for confirmation.  |
| <b>Messaging Type</b>          | The type of the Messaging box. The following are the types of messaging: <ul style="list-style-type: none"> <li>• MM: for Modular Messaging systems</li> <li>• CMM: for Communication Manager Embedded Messaging systems</li> </ul> |
| <b>Version</b>                 | The version of the Messaging Box. Supported versions are 5.0 and above.   |
| <b>Secured LDAP Connection</b> | Use this check box to specify whether Secure LDAP connection is to be used. Select this check box to use secure LDAP connection, else LDAP will be used.  |
| <b>Port</b>                    | The port on which the LDAP or secure LDAP service provided by the application instance is running. For LDAP the port is 389 and for secure LDAP the port is 636.  |
| <b>Location</b>                | The location of the application instance.   |

### SNMP Attributes

You set some basic parameters for specific devices or a range of devices in the SNMP Attributes section. You can choose either SNMP protocol V1 or V3. Based on your selection of SNMP protocol, you can then set certain basic SNMP parameters.

| Name                   | Description  |
|------------------------|--|
| <b>Version</b>         | Specifies the SNMP protocol type.  |
| <b>Read Community</b>  | The read community of the device.. Only applicable for SNMP protocol V1.                                 |
| <b>Write Community</b> | The write community of the device. Only applicable for SNMP protocol V1.                                 |
| <b>Retries</b>         | The number of times an application polls a device without receiving a response before timing out.        |
| <b>Timeout</b>         | The number of milliseconds an application polls a device without receiving a response before timing out. |
| <b>Device Type</b>     | Specifies the type of the device   |

## Assign Applications

| Name               | Description   |
|--------------------|---|
| <b>Name</b>        | The name of the application instance.               |
| <b>Type</b>        | The type of application.                            |
| <b>Description</b> | A brief description about the application instance. |

| Button                       | Description   |
|------------------------------|---|
| <b>Assign Applications</b>   | Opens the Assign Applications page. Use the page to assign an application instance to another application instance. |
| <b>Unassign Applications</b> | Removes an assigned application.  |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Creates or modifies an instance by saving the instance information to the database.<br><br> <b>Note:</b><br>This button is visible only when you click <b>New</b> and <b>Edit</b> on the Application Management page. |
| <b>Cancel</b> | Closes the page without saving the information and takes you back to the <b>Application Management</b> page.   |

## Certificate Details

| Name                   | Description   |
|------------------------|---|
| <b>Subject Details</b> | Details of the certificate holder.                      |
| <b>Valid From</b>      | The date and time from which the certificate is valid.  |
| <b>Valid To</b>        | The date and time until which the certificate is valid. |
| <b>Key Size</b>        | The size of the key in bits or bytes for encryption.    |
| <b>Issuer Name</b>     | The name of the issuer of the certificate.              |
| <b>Finger Print</b>    | The finger print that authenticates the certificate.    |

| Button                    | Description   |
|---------------------------|---|
| <b>Issue Certificates</b> | Adds the application as a trusted application.                  |
| <b>Add Untrusted</b>      | Adds the application as a non-trusted application.              |
| <b>Cancel</b>             | Cancel the operation of issuing certificate to the application. |

## Delete Application Confirmation field descriptions

Use this page to delete the selected application instance.

| Name                | Description  |
|---------------------|--|
| <b>Name</b>         | Name of the application instance.  |
| <b>Node</b>         | The node on which the application is running.  |
| <b>Registration</b> | The registration status of the application instance. The values are: <ul style="list-style-type: none"> <li>• True: Indicates a registered instance.</li> <li>• False: Indicates an unregistered instance</li> </ul> |
| <b>Description</b>  | A brief description about the instance.  |

| Button        | Description                                      |
|---------------|--|
| <b>Delete</b> | Deletes the selected application instance.       |
| <b>Cancel</b> | Closes the Delete Application Confirmation page. |

## Assign Applications field descriptions

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use the check box to select application instances. |
| <b>Name</b>             | The name of the application instance.              |
| <b>Type</b>             | The type of the application.                       |
| <b>Description</b>      | A brief description about the application.         |

| Button        | Description   |
|---------------|---|
| <b>Assign</b> | Assigns the selected application instance to another application instance.          |
| <b>Cancel</b> | Cancel the assignment operation and takes you back to the Application details page. |

## Import Applications field descriptions

Use this page to bulk import applications data from a valid XML file.

## File Selection

| Name               | Description  |
|--------------------|--|
| <b>Select File</b> | The path and name of the XML file from which you want to import the applications data. |

| Button        | Description   |
|---------------|---|
| <b>Browse</b> | Opens a dialog box that you can use to select the file from which you want to import the applications data. |

## General

| Name                                       | Description   |
|--|---|
| <b>Select Error Configuration</b>          | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Abort on First Error:</b> If you select this option, system aborts importing the applications data when the import application operation encounters the first error in the import file containing the applications data.</li> <li>• <b>Continue Processing other records:</b> If you select this option, the system imports the data of next application if the data of previous application failed to import.</li> </ul>   |
| <b>If a matching record already exists</b> | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Skip:</b> Skips a matching record that already exists in the system during an import operation.</li> <li>• <b>Replace:</b> Re-imports or replaces all the data for an application. This is essentially the ability to replace an application along with the other data related to the application.</li> <li>• <b>Merge:</b> Imports the application data at an even greater degree of granularity. Using this option you can simultaneously perform both the add and update operation of applications data.</li> <li>• <b>Delete:</b> Deletes the applications along with their data from the database that match the records in the input XML file.</li> </ul> |

## Job Schedule

| Name                | Description   |
|---------------------|---|
| <b>Schedule Job</b> | <p>The options for configuring the schedule of the job:</p> <ul style="list-style-type: none"> <li>• <b>Run immediately:</b> Use this option if you want to run the import job immediately.</li> <li>• <b>Schedule later:</b> Use this option to run the job at the specified date and time.</li> </ul> |

| Name             | Description  |
|------------------|--|
| <b>Date</b>      | Date when you want to run the import applications job. The date format is mm dd yyyy. You can use the calendar icon to choose a date. This field is available when you select the <b>Schedule later</b> option for scheduling a job. |
| <b>Time</b>      | Time of running the import applications job. The time format is hh:mm:ss and 12 (AM or PM) or 24 hour format. This field is available when you select the <b>Schedule later</b> option for scheduling a job.                         |
| <b>Time Zone</b> | Time zone of your region. This field is available when you select the <b>Schedule later</b> option for scheduling a job.   |

| Button        | Description   |
|---------------|---|
| <b>Import</b> | Imports or schedules the import operation based on the option you selected. |

### Manage Jobs

| Name                       | Description   |
|----------------------------|---|
| <b>Check box</b>           | Use this check box to select a job.   |
| <b>Scheduled Time</b>      | The time and date of scheduling the job   |
| <b>Status</b>              | The current status of the job. The following are the different status of the job: <ol style="list-style-type: none"> <li>1. PENDING EXECUTION: The job is in queue.</li> <li>2. RUNNING: The job execution is in progress.</li> <li>3. SUCCESSFUL: The job execution is completed.</li> <li>4. INTERRUPTED: The job execution is cancelled.</li> <li>5. PARTIAL FAILURE: The job execution has partially failed.</li> <li>6. FAILED: The job execution has failed.</li> </ol> |
| <b>Job Name</b>            | A link to the Scheduler user interface. You can cancel the job from the Scheduler user interface too.   |
| <b>% Complete</b>          | The job completion status in percentage.  |
| <b>Application Records</b> | The total user records in the input file.   |
| <b>Error</b>               | Number of user records in the input file that failed to import.   |

| Button          | Description                            |
|-----------------|--|
| <b>View Job</b> | Shows the details of the selected job. |

| Button              | Description  |
|---------------------|--|
| <b>Cancel Job</b>   | Cancels the import operation for the selected job. You can cancel a job that is in progress or queued for import.  |
| <b>Delete Job</b>   | Deletes the selected job.  |
| <b>Refresh</b>      | Refreshes the job information in the table.  |
| <b>Show</b>         | Provides you an option to view all the jobs on the same page. If the table displaying scheduled jobs are spanning multiple pages, select <b>All</b> to view all the jobs on a single page. |
| <b>Select: All</b>  | Selects all the jobs in the table.   |
| <b>Select: None</b> | Clears the check box selections.   |
| <b>Previous</b>     | Displays jobs in the previous page.  |
| <b>Next</b>         | Displays jobs in the next page.  |
| <b>Done</b>         | Takes you back to the <b>User Management</b> page.   |

---

## Import Status field descriptions

The Import Status page displays the detailed status of the selected import job.

| Name             | Description  |
|------------------|--|
| <b>End</b>       | End date and time of the job.  |
| <b>Status</b>    | Status of the job.   |
| <b>File</b>      | Name of the file that is used to import the application records.     |
| <b>Count</b>     | Total number of application records in the input file.               |
| <b>Success</b>   | Total number of applications records that are successfully imported. |
| <b>Fail</b>      | Total number of application records that failed to import.           |
| <b>Completed</b> | Displays the percentage completion of the import.                    |

| Name                 | Description                                       |
|----------------------|---|
| <b>Line Number</b>   | Line number in the file where the error occurred. |
| <b>Login Name</b>    | The login name through which job was executed.    |
| <b>Error Message</b> | A brief description about the error message       |

| Button      | Description                                     |
|-------------|---|
| <b>Done</b> | Takes you back to the Import Applications page. |

---

## Managing certificates

---

### About Trust Management

Trust Management provisions certificates to applications enabling them to have a secure inter-element communication. It provides Identity and Trusted (root) certificates with which mutually authenticated TLS sessions can be established. You can perform the following operations for an application instance using the Trust Management service:

- View trusted and identity certificates
- Add and remove trusted certificates
- Replace identity certificates

---

### Setting SCEP enrollment password

Use this functionality to generate the simple certificate enrollment password (SCEP) for adopting products. The adopting products require the SCEP password to request certificates from Trust Management.

- 
1. On the System Manager console, click **Security > Trust Management > Enrollment Password**.
  2. On the Enrollment Password page, select the expiration of password in hours in the **Password expires in** field.
  3. Click **Generate**.

 **Note:**

The password field displays the generated password.

4. Click **Done**.

 **Note:**

When you click **Generate**, the time displayed next to the **Time remaining** label is updated by the value selected in the **Password expires in** field.

---

**Related topics:**

[Enrollment Password field descriptions](#) on page 42

---

## Adding trusted certificates

You need to import the certificates that you want to add as trusted certificate in the trust store of the application. The following are the four methods of importing a trusted certificate in the trust store for an application instance:

1. Import from existing
2. Import from file
3. Import as PEM Certificate
4. Import using TLS

You can add a trusted certificate from a list of an existing certificates, a file, a remote location using TLS connection and by copying the content from a PEM file.

- 
1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
  2. On the Application Management page, select an application and click **More Actions > Configure Trusted Certificates**.
  3. On the Trusted Certificates page, click **Add**.
  4. On the **Add Trusted Certificate** page, select store type from the **Store Type** field and perform one of the following steps:
    - To import certificates from existing certificates:
      - i. Click **Import from existing** .
      - ii. Select the certificate from the Global Trusted Certificate section.
      - iii. Click **Commit**.
    - To import certificates from a file:
      - i. Click **Import from file** .
      - ii. Enter the name of the file. You can also click **Browse** to select a file.
      - iii. Click **Retrieve Certificate**.
      - iv. Click **Commit**.
    - To import certificates in the PEM format:
      - i. Locate the PEM certificate.
      - ii. Open the certificate in the Notepad application.

- iii. Select all the contents in the file.
- iv. Perform a copy operation.
- v. Click **Import as PEM Certificate** .
- vi. Perform a paste operation in the box provided at the bottom of the page.



**Note:**

You may include the start and end tags: -----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----.

- vii. Click **Commit**.
- To import using TLS:
    - i. Click **Import using TLS** .
    - ii. Enter the IP Address of the computer in the **IP Address** field.
    - iii. Enter the port of the computer in the **Port** field.
    - iv. Click **Retrieve Certificate**.
    - v. Click **Commit**.

---

**Related topics:**

[Add Trusted Certificate field descriptions](#) on page 43

---

## Viewing trusted certificates

### Prerequisites

You must have permission to view certificates of an application instance.

1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
2. On the Manage Elements page, select an application and click **More Actions > Configure Trusted Certificates**.
3. On the Trusted Certificates page, click **View**.

---

### Result

The **View Trust Certificate** page displays the details of the selected certificate.

**Related topics:**

[View Trust Certificate field descriptions](#) on page 45

---

## Removing trusted certificates

---

1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
  2. On the Manage Elements page, click **More Actions > Configure Trusted Certificates**.
  3. On the Trusted Certificates page, select the certificates and click **Remove**.
- 

**Result**

Trust Management removes the certificates from the list of trusted certificates for the application instance.

---

## Viewing identity certificates

---

1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
  2. On the Application Management page, click **More Actions > Configure Identity Certificates**.
- 

**Result**

The Identity Certificate page displays the identity certificates.

**Related topics:**

[Identity Certificates field descriptions](#) on page 46

---

## Replacing an identity certificate

1. On the System Manager console, click **Elements > Inventory > Manage Elements** in the left navigation pane.
2. On the Application Management page, click **More Actions > Configure Identity Certificates**.
3. On the Identity Certificate page, click **Replace**.
4. On the Replace Identity Certificate, perform one of the following steps:
  - click **Replace this Certificate with Internal CA Signed Certificate** and do the following:
    - Enter common name, org unit, organization, country in the respective fields.
    - Select key size/type from the respective field.
    - Click **Commit** to replace the identity certificate with the internal CA signed certificate.
  - Click **Import third party PCKS # 12 file** and do the following:
    - Enter the file name in the **Please select a file** field.
    - Enter the password in the **Password** field.
    - Click **Retrieve Certificate** . The Certificate Details section displays the details of the certificate.
    - Click **Commit** to replace the certificate with the imported third party certificate.

---

### Related topics:

[Replace Identity Certificate field descriptions](#) on page 47

---

## Enrollment Password field descriptions

Use this page to generate a simple certificate enrollment password (SCEP).

| Name                     | Description   |
|--------------------------|---|
| <b>Existing Password</b> | The current simple certificate enrollment password (SCEP) that the external SCEP clients use to request certificates. |

| Name                       | Description  |
|----------------------------|--|
| <b>Time Remaining</b>      | Displays the time in hours and minutes remaining for expiration of the current password.   |
| <b>Password expires in</b> | The duration for which the existing password is valid (in hours).  |
| <b>Password</b>            | The password that the external SCEP clients use to request a certificate. Trust Manager generates this password when you click <b>Generate</b> . |

| Button          | Description   |
|-----------------|---|
| <b>Generate</b> | Generates a random password.  |
| <b>Done</b>     | Updates the <b>Existing Password</b> and <b>Time Remaining</b> fields |

---

## Trusted Certificates field descriptions

Use this page to view and delete the trusted certificates listed on the page. You can also use this page to add more certificates in the existing list of trusted certificates

| Name                    | Description  |
|-------------------------|--|
| <b>Certificate Name</b> | The name of the trusted certificate.                   |
| <b>Store Type</b>       | The type of the store associated with the certificate. |
| <b>Subject Name</b>     | The name of the certificate holder.                    |

| Button         | Description  |
|----------------|--|
| <b>View</b>    | Open the View Trust Certificate page. Use this page to view the certificate details.                     |
| <b>Add</b>     | Open the Adds Trusted Certificate page. use this page to import certificates from the selected resource. |
| <b>Remove</b>  | Removes the selected certificate from the list of trusted certificates.                                  |
| <b>Exports</b> | Exports the selected certificate from the list of trusted certificates.                                  |

---

## Add Trusted Certificate field descriptions

Use this page to add a trusted certificate.

| Name                             | Description   |
|----------------------------------|---|
| <b>Store Type</b>                | The type of the store based on inbound and outbound connection. The options are: <ul style="list-style-type: none"> <li>• All</li> <li>• TM_INBOUND_TLS</li> <li>• TM_OUTBOUND_TLS</li> <li>• TM_INBOUND_TLS_PEM</li> </ul> |
| <b>Import from existing</b>      | Use this option to import the certificate from your local machine.  |
| <b>Import from file</b>          | Use this option to import the certificates from a file. The file format is .cer.  |
| <b>Import as PEM Certificate</b> | Use this option to import the certificate in .pem format.   |
| <b>Import using TLS</b>          | Use this option to import a certificate if the application instance requires to contact the certificate provider to obtain the certificate.   |

**Global Trusted Certificate:**

The page displays the following fields when you select the **Import from existing** option.

| Name                    | Description  |
|-------------------------|--|
| <b>Certificate Name</b> | The fully qualified domain name of the certificate.  |
| <b>Subject Name</b>     | The fully qualified domain name of the certificate holder.   |
| <b>Valid To</b>         | The date until which the certificate is valid.   |
| <b>Filter: Enable</b>   | Displays fields under select columns that you can use to set filter criteria. This is a toggle button. |
| <b>Filter: Disable</b>  | Hides the column filter fields without resetting the filter criteria. This is a toggle button.         |
| <b>Filter: Clear</b>    | Clears the filter criteria.  |
| <b>Filter: Apply</b>    | Filters certificates based on the filter criteria.   |
| <b>Select: All</b>      | Select all the certificates in the table.  |
| <b>Select: None</b>     | Clears all the check box selections.   |
| <b>Refresh</b>          | Refreshes the certificates information .   |

The page displays these fields when you select the **Import from file** option.

| Name/Button                 | Description                              |
|-----------------------------|--|
| <b>Please select a file</b> | The file that contains the certificates. |

| Name/Button                 | Description  |
|-----------------------------|--|
| <b>Browse</b>               | Opens the choose file dialog box. Use this dialog box to choose the file from which you want to import the certificates. |
| <b>Retrieve Certificate</b> | Retrieves the certificate from the file and displays the details of the certificate in the Certificate Details section.  |

#### Certificate Details:

The page displays these fields when you click **Retrieve**.

| Name                   | Description   |
|------------------------|---|
| <b>Subject Details</b> | Details of the certificate holder.                      |
| <b>Valid From</b>      | The date and time from which the certificate is valid.  |
| <b>Valid To</b>        | The date and time until which the certificate is valid. |
| <b>Key Size</b>        | The size of the key in bits for encryption.             |
| <b>Issuer Name</b>     | The name of the issuer of the certificate.              |
| <b>Finger Print</b>    | The finger print that authenticates the certificate.    |

The page displays these fields when you select the **Import using TLS** option.

| Field/Button                | Description   |
|-----------------------------|---|
| <b>IP Address</b>           | IP address of the certificate provider that is to be contacted for retrieving the certificate.            |
| <b>Port</b>                 | Port of the server to be used for obtaining the certificate.  |
| <b>Retrieve Certificate</b> | Retrieves the certificate and displays the details of the certificate in the Certificate Details section. |

#### Related topics:

[Adding trusted certificates](#) on page 39

---

## View Trust Certificate field descriptions

Use this page to view details of a selected certificate.

| Name                   | Description   |
|------------------------|---|
| <b>Subject Details</b> | Details of the certificate holder.                      |
| <b>Valid From</b>      | The date and time from which the certificate is valid.  |
| <b>Valid To</b>        | The date and time until which the certificate is valid. |
| <b>Key Size</b>        | The size of the key in bits for encryption.             |

| Name                | Description  |
|---------------------|--|
| <b>Issuer Name</b>  | The name of the issuer of the certificate.           |
| <b>Finger Print</b> | The finger print that authenticates the certificate. |

| Button      | Description  |
|-------------|--|
| <b>Done</b> | Closes the page and takes you back to the Trusted Certificates page. |

---

## Delete Trusted Certificate Confirmation field descriptions

Use this page to delete a trusted certificate from the list of trusted certificate maintained by the application instance.

| Name                    | Description  |
|-------------------------|--|
| <b>Certificate Name</b> | The name of the trusted certificate.                   |
| <b>Store Type</b>       | The type of the store associated with the certificate. |
| <b>Subject Name</b>     | The name of the certificate holder.                    |

| Button        | Description  |
|---------------|--|
| <b>Delete</b> | Deletes the trusted certificate from the corresponding store.                  |
| <b>Cancel</b> | Cancel the delete operation and takes you back to the Add Trusted Certificate. |

---

## Identity Certificates field descriptions

Use this page to view the identity certificates for the application instance.

| Name                       | Description   |
|----------------------------|---|
| <b>Service Name</b>        | The name of the service that uses the identity certificate. |
| <b>Common Name</b>         | Common name to identify the service.                        |
| <b>Valid To</b>            | The date until which the certificate is valid.              |
| <b>Service Description</b> | A brief description about the service.                      |

| Button         | Description   |
|----------------|---|
| <b>Replace</b> | Opens the Replace Identity Certificate page. Use this page to replace a selected identity certificate with a new certificate. |

| Button | Description  |
|--------|--|
| Cancel | Closes the Identity Certificates page and takes you back to the Application Management page. |

## Replace Identity Certificate field descriptions

Use this page to replace an identity certificate.

### Certificate Details section

| Name            | Description   |
|-----------------|---|
| Subject Details | Details of the certificate holder.                      |
| Valid From      | The date and time from which the certificate is valid.  |
| Valid To        | The date and time until which the certificate is valid. |
| Key Size        | The size of the key in bits for encryption.             |
| Issuer Name     | The name of the issuer of the certificate.              |
| Finger Print    | The finger print that authenticates the certificate.    |

| Name   | Description  |
|--|--|
| Replace this Certificate with Internal CA Signed Certificate | Use this option to replace the current certificate with internal CA signed certificate.            |
| Import third party PCKS #12 file                             | Use this option if you like to replace the identity certificate with imported third PCKS #12 file. |

The page displays following fields when you select **Replace this Certificate with Internal CA Signed Certificate** option.

| Name              | Description   |
|-------------------|---|
| Common Name (CN): | The common name of the certificate holder.            |
| Org Unit (OU):    | The name of the organizational unit.                  |
| Organization (O): | The name of the organization                          |
| Country (C):      | The country where the organization is located.        |
| Key Size/Type:    | The size of the key in bits or bytes for encryption . |

The page displays following fields when you select **Import third party PCKS #12 file** option.

| Name/Button                 | Description   |
|-----------------------------|---|
| <b>Please Select a file</b> | The full path of the PKCS #12 file where you have saved the certificate.  |
| <b>Password</b>             | The password that is used to encrypt the certificate.   |
| <b>Browse</b>               | Opens the file dialog box to navigate to the PKCS #12 file.   |
| <b>Retrieve Certificate</b> | Retrieves the details of the imported certificate and displays in the following <b>Certificate Details</b> section. |

| Name/Button    | Description  |
|----------------|--|
| <b>Commit</b>  | Replaces the current identity certificate with the selected certificate. |
| <b>Exports</b> | Exports the Identity Certificates.                                       |
| <b>Cancel</b>  | Cancels the certificate replacement operation.                           |

**Related topics:**

[Replacing an identity certificate](#) on page 42

## System Manager- Communication Manager capabilities Overview

System Manager provides a common, central administration of some of the existing IP Telephony products. System Manager helps you consolidate key capabilities of the current suite of Integrated Management administration products with other Avaya Management tools on a common software platform. System Manager helps you administer Avaya Aura™ Communication Manager, Communication Manager Messaging, and Modular Messaging. System Manager features include:

- Endpoint Management
- Template Management
- Mailbox Management
- Discovery Management
- Element Cut Through to native administration screens

### Managing Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Feature Management**. It also allows you to directly add, edit, view or delete these objects through **Feature Management**.

## **Endpoint Management**

System Manager allows you to create and manage endpoints. Endpoint Management provides support for Communication Manager endpoint objects and helps you add, change, remove and view endpoint data.

## **Templates**

Using templates, you can specify specific parameters of an endpoint or a subscriber once and then reuse that template for subsequent add endpoint or subscriber tasks. The system provides default templates, but additionally you can also add your own custom templates.

There are two categories of templates: default templates and user-defined templates. You cannot edit or delete the default templates. However, you can modify or remove user-defined templates any time.

## **Subscriber Management**

System Manager lets you manage subscriber data. Subscriber Management provides support for Communication Manager Messaging and Modular Messaging objects. You can add, change, remove, and view subscriber data.

Using System Manager Communication Manager capabilities you can:

- Add Communication Manager (for endpoints) and Modular Messaging (for subscribers) to the list of managed elements.
- Create templates to simplify endpoint and subscriber management.
- Administer endpoints, subscribers, and create user profiles (with Communication Profiles).
- Associate the user profiles with the required endpoints and subscribers.



# Chapter 2: Managing endpoints

---

## Endpoints

---

### Endpoint Management

System Manager allows you to create and manage endpoints using the **Manage Endpoints** option. You can also view, edit, and delete endpoints. It provides support for the following set types:

| Set Type         |  |
|------------------|--|
| IP/SIP Set types | 9610SIP/9620SIP/9630SIP/9640SIP/<br>9650SIP<br>9610/9620/9630/9640/9650<br>1603/1608/1616/16CC<br>9600SIP<br>4620SIP<br>4620SIPCC<br>4610/4620/4621/4622/4625/4630<br>4602+<br>4612CL<br>H.323 |
| DCP Set types    | 2402/2410/2420<br>6402/6402D/6408/6408+/6408D/6408D+/<br>6416D+/6424D+<br>8403B/8405B/8405B+/8405D/8405D+/<br>8410B/8410D/8411B/8411D/8434D<br>1408<br>1416                                    |
| Analog Set types | 2500   |
| BRI Set types    | WCBRI  |

 **Note:**

The set types supported varies based on the Communication Manager versions managed.

---

## Adding an endpoint

1. From the navigation pane, click **Elements > Endpoints > Manage Endpoints**.
2. Choose a Communication Manager from the list.
3. Click **Show List**.  
The system displays the available Endpoints list on the Communication Manager you selected.
4. Click **New**.
5. Select the template based on the set type you want to add.  
The system displays all the sections on the Add Endpoint page.
6. Complete the Add Endpoint page and click **Commit** to add the endpoint.  
You must complete the mandatory fields (marked with an asterisk symbol) under the **General options, Feature Options, Site Data, Data Module/Analog Adjunct, Abbreviated Call Dialing, Enhanced Call Fwd, Button Assignment** sections before adding an endpoint.



**Note:**

To add an endpoint with a non-supported set type, add the endpoint using Element Cut Through. For alias endpoints, you can choose the corresponding Alias set type from the **Template** field. System Manager automatically creates a template for the Alias set types based on the “aliased-to” set type. Alias endpoint templates have names beginning with “Alias”. Before the Alias endpoint type Template appears in the pull-down menu, you have to create an alias set type on the managed Communication Manager. You can then use the template to add an endpoint.

---

**Related topics:**

[Endpoint / Template field descriptions](#) on page 57

---

## Using Native Name

To enter the native name, you must use the Input Method Editor (IME) application. The IME application lets you enter characters in multiple languages such as Japanese, Korean, Russian, Arabic and Chinese without requiring a special keyboard. However, you must enable the IME application manually. Otherwise, the keyboard input remains in the default language.

The IME icon appears in the Windows system tray and indicates the language you are currently using. For example, if you are using English, the IME icon in the system tray displays **EN**. If you are using French, the IME icon in the system tray displays **FR**.

- 
1. Click the IME icon in the Windows system tray.  
The system displays a menu with the languages installed on your PC.
  2. Select the language you want to use.
  3. Type the native name in Site Administration Communication System Management.
- 

---

## Editing an endpoint

- 
1. From the navigation pane, click **Elements > Endpoints > Manage Endpoints**.
  2. Select a Communication Manager from the list.
  3. Click **Show List**.
  4. From the corresponding Endpoint list, select the endpoint you want to edit.
  5. Click **Edit** or **View > Edit**.
  6. Edit the required fields in the Edit Endpoint page.
  7. Click **Commit** to save the changes.
- 

### Related topics:

[Endpoint / Template field descriptions](#) on page 57

---

## Viewing an endpoint

- 
1. From the navigation pane, click **Elements > Endpoints > Manage Endpoints**.
  2. Select a Communication Manager from the list.
  3. Click **Show List**.
  4. From the list of endpoints, select the endpoint you want to view.
  5. Click **View** to view the attributes of the endpoint you have chosen.



**Note:**

You cannot edit the fields in the View Endpoint page. To go to the Edit Endpoint page, click **Edit**.

---

**Related topics:**

[Endpoint / Template field descriptions](#) on page 57

---

## Deleting an endpoint

1. From the navigation pane, click **Elements > Endpoints > Manage Endpoints**.
2. Choose a Communication Manager from the list.
3. Click **Show List**.
4. From the Endpoint list, select the endpoint(s) you want to delete.
5. Click **Delete**.

The system displays a confirmation message alerting you to a user associated with the endpoint. The system flags these user-associated endpoints in yellow color.



**Note:**

You cannot delete an endpoint associated with a user through endpoint management. You can delete the user associated endpoints only through User Profile Management.

---

## Editing endpoint extensions

1. From the navigation pane, click **Elements > Endpoints > Manage Endpoints**.
2. Select a Communication Manager from the list.
3. Click **Show List**.
4. From the Endpoint list, select the endpoint for which you want to edit the extension.
5. Click **More Actions > Edit Endpoint Extension**.
6. Complete the Edit Endpoint Extension page and click **Commit** to save the new extension.

 **Note:**

You can use the **Edit Endpoint Extension** option to change the endpoint extension. You can also edit the **Message Lamp Ext** and **Emergency Location Ext** fields through **Edit Endpoint Extension**. Use the **Edit** option to modify the other attributes.

---

**Related topics:**

[Edit Endpoint Extension field descriptions](#) on page 77

---

## Bulk adding endpoints

1. From the navigation pane, click **Elements > Endpoints > Manage Endpoints**.
2. Choose a Communication Manager from the list.
3. Click **Show List**.
4. Click **More Actions > Bulk Add Endpoints**.
5. Complete the Bulk Add Endpoint page and click **Commit** to bulk add the endpoints. The **Endpoint Name Prefix** field gives the common prefix which appears for all the endpoints you bulk add. You can enter any prefix name of your choice in this field.

 **Note:**

In the **Enter Extensions** field you can enter the extensions which you want to use. You must enter the extensions in serial order and also check for the availability of an extension before you use it.

---

**Related topics:**

[Bulk Add Endpoint field descriptions](#) on page 78

---

## Bulk editing endpoints

1. From the navigation pane, click **Elements > Endpoints > Manage Endpoints**.
2. Choose a Communication Manager from the list.
3. Click **Show List**.
4. From the Endpoint list select the endpoint(s) you want to bulk edit.

5. Click **More Actions > Bulk Edit Endpoints**.
6. Complete the Bulk Edit Endpoint page and click **Commit** to bulk edit the endpoints. The **Endpoint Name Prefix** field gives the common prefix that appears for all the endpoints you bulk add or edit. You can enter any prefix name of your choice in this field.

---

**Related topics:**

[Bulk Edit Endpoint field descriptions](#) on page 79

---

## Endpoint List

Endpoint List displays all the endpoints under the Communication Manager(s) you select. You can perform an advanced search on the endpoint list using the search criteria. You can also apply filters and sort each of the columns in the Endpoint List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name             | Description  |
|------------------|--|
| <b>Name</b>      | Specifies the name of the endpoint.  |
| <b>Extension</b> | Specifies the extension of the endpoint.   |
| <b>Port</b>      | Specifies the port of the endpoint.  |
| <b>Set Type</b>  | Specifies the set type of the endpoint.  |
| <b>COS</b>       | Specifies the COS for the endpoint.  |
| <b>COR</b>       | Specifies the COR for the endpoint.  |
| <b>User</b>      | If an endpoint is associated with a user, the system displays the name of the user in this column. |
| <b>System</b>    | Specifies the Communication Manager of the endpoint.   |

---

## Filtering endpoints

1. From the navigation pane, click **Elements > Endpoints > Manage Endpoints**.
2. Select a Communication Manager from the list.
3. Click **Show List**.
4. Click **Filter: Enable** in the Endpoint List.

5. Filter the endpoints according to one or multiple columns.
6. Click **Apply**.  
To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

 **Note:**

The table displays only those endpoints that match the filter criteria.

---

---

## Using Advanced Search

1. From the navigation pane, click **Elements > Endpoints > Manage Endpoints**.
2. Select a Communication Manager from the list.
3. Click **Show List**.
4. Click **Advanced Search** in the Endpoint list .
5. In the Criteria section, do the following:
  - a. Select the search criterion from the first drop-down field.
  - b. Select the operator from the second drop-down field.
  - c. Enter the search value in the third field.

If you want to add a search condition, click **+** and repeat the sub steps listed in step 5.

If you want to delete a search condition, click **-** . This button is available if there is more than one search condition.

---

---

## Add station Template

### Endpoint / Template field descriptions

You can use these fields to perform endpoint / template tasks. This page has the exclusive fields that occur for endpoints and templates apart from the **General options**, **Feature Options**, **Site Data**, **Data Module/Analog Adjunct**, **Abbreviated Call Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections.

### Field description for Endpoints

| Name            | Description   |
|-----------------|---|
| <b>System</b>   | Specifies the Communication Manager that the endpoint is assigned to.   |
| <b>Template</b> | Specifies all the templates that correspond to the set type of the endpoint.  |
| <b>Set Type</b> | Specifies the set type or the model number of the endpoint.   |
| <b>Name</b>     | Specifies the name associated with an endpoint. The name you enter displays on called telephones that have display capabilities. Some messaging applications, such as Communication Manager Messaging recommend that you enter the user's name (last name first) and their extension to identify the telephone. The name entered is also used for the integrated directory. |

### Field description for Templates

| Name                 | Description   |
|----------------------|---|
| <b>Set Type</b>      | Specifies the set type or the model of the endpoint template.                                     |
| <b>Template Name</b> | Specifies the name of the endpoint template. You can enter the name of your choice in this field. |

### Extension

The extension for this station.

For a virtual extension, a valid physical extension or a blank can be entered. Blank allows an incoming call to the virtual extension to be redirected to the virtual extension “busy” or “all” coverage path.

### Port

The port assigned to the station.

| Valid Entry | Usage   |
|-------------|---|
| 01 to 64    | First and second numbers are the cabinet number   |
| A to E      | Third character is the carrier  |
| 01 to 20    | Fourth and fifth characters are the slot number   |
| 01 to 32    | Sixth and seventh characters are the circuit number   |
| x or X      | Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) stations, as well as for SBS Extensions. |
| IP          | Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have an IP set. This is automatically entered for certain   |

| Valid Entry | Usage  |
|-------------|--|
|             | IP station set types, but you can enter for a DCP set with softphone permissions. This changes to the s00000 type when the set registers.  |
| xxxVmpp     | Specifies the media gateway. <ul style="list-style-type: none"> <li>• xxx is the gateway number, which is in the range 001 to 250.</li> <li>• m is the module number, which is in the range 1 to 9.</li> <li>• pp is the port number, which is in the range 01 to 32.</li> </ul> |

## General Options

This section lets you set the general fields for a station.

### COS

The Class of Service (COS) number used to select allowed features.

### COR

Class of Restriction (COR) number with the desired restriction.

### Coverage Path 1 or Coverage Path 2

The coverage-path number or time-of-day table number assigned to the station.



#### Note:

If Modified Misoperation is active, a Coverage Path must be assigned to all stations on Communication Manager.

#### Related topics:

[Misoperation Alerting](#) on page 607

### TN

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

### Security Code

The security code required by users for specific system features and functions, including the following: Personal Station Access, Redirection of Calls Coverage Off-Net, Leave Word Calling, Extended Call Forwarding, Station Lock, Message Retrieval, Terminal Self-Administration, and Demand Printing. The required security code length is administered system-wide.

#### Related topics:

[Minimum Station Security Code Length](#) on page 853

### Emergency Location Ext

The Emergency Location Extension for this station. This extension identifies the street address or nearby location when an emergency call is made. Defaults to the telephone's extension. Accepts up to eight digits.



**Note:**

On the ARS Digit Analysis Table in Communication Manager, 911 must be administered to be call type emer or alrt for the E911 Emergency feature to work properly.

**Related topics:**

[Remote Softphone Emergency Calls](#) on page 63

**Message Lamp Ext**

The extension of the station tracked with the message waiting lamp.

**Lock Messages**

Controls access to voice messages by other users.

| Valid Entry | Usage   |
|-------------|---|
| y           | Restricts other users from reading or canceling the voice messages, or retrieving messages using Voice Message Retrieval. |
| n           | Allows other users to read, cancel, or retrieve messages.   |

**Feature Options**

This section lets you set features unique to a particular voice terminal type.

**Location**

This field appears only when the **Multiple Locations** field is set to y and the **Type** field is set to H.323 or SIP station types.

| Valid entry | Usage  |
|-------------|--|
| 1 to 250    | (Depending on your server configuration, see <i>Avaya Aura™ Communication Manager System Capacities Table</i> , 03-300511.) Assigns the location number to a particular station. Allows IP telephones and softphones connected through a VPN to be associated with the branch an employee is assigned to. This field is one way to associate a location with a station. For the other ways and for a list of features that use location, see the Location sections in <i>Avaya Aura™ Communication Manager Feature Description and Implementation</i> , 555-245-205. |
| blank       | Indicates that the existing location algorithm applies. By default, the value is blank.  |

**Active Station Ringing**

Defines how calls ring to the telephone when it is off-hook without affecting how calls ring at this telephone when the telephone is on-hook.

| Valid Entry | Usage  |
|-------------|--|
| continuous  | All calls to this telephone ring continuously.                         |
| single      | Calls to this telephone receive one ring cycle and then ring silently. |

| Valid Entry    | Usage   |
|----------------|---|
| if-busy-single | Calls to this telephone ring continuously when the telephone is off-hook and idle. Calls to this telephone receive one ring cycle and then ring silently when the telephone is off-hook and active. |
| silent         | All calls to this station ring silently.  |

### Auto Answer

In EAS environments, the auto answer setting for the Agent LoginID can override a station's setting when an agent logs in.

| Valid Entry | Usage  |
|-------------|--|
| all         | All ACD and non-ACD calls terminated to an idle station cut through immediately. Does not allow automatic hands-free answer for intercom calls. With non-ACD calls, the set is also rung while the call is cut through. The ring can be prevented by activating the ringer-off feature button when the <b>Allow Ringer-off with Auto-Answer</b> is enabled for the system.                       |
| acd         | Only ACD split /skill calls and direct agent calls to auto answer. Non-ACD calls terminated to a station ring audibly. For analog stations, the station is off-hook and idle, only the ACD split/skill calls and direct agent calls auto answer; non-ACD calls receive busy treatment. If the station is active on an ACD call and a non-ACD call arrives, the Agent receives call-waiting tone. |
| none        | All calls terminated to this station receive an audible ringing treatment.   |
| icom        | Allows a telephone user to answer an intercom call from the same intercom group without pressing the <b>intercom</b> button.   |

### Related topics:

[Allow Ringer-off with Auto-Answer](#) on page 619

### MWI Served User Type

Controls the auditing or interrogation of a served user's message waiting indicator (MWI).

| Valid Entries | Usage  |
|---------------|--|
| fp-mwi        | The station is a served user of an fp-mwi message center.  |
| qsig-mwi      | The station is a served user of a qsig-mwi message center.   |
| blank         | The served user's MWI is not audited or if the user is not a served user of either an fp-mwi or qsig-mwi message center. |

### Coverage After Forwarding

Governs whether an unanswered forwarded call is provided coverage treatment.

| Valid Entry | Usage   |
|-------------|---|
| y           | Coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters. |

| Valid Entry | Usage  |
|-------------|--|
| n           | No coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters. |
| s(system)   | Administered system-wide coverage parameters determine treatment.  |

**Related topics:**

[Coverage After Forwarding](#) on page 932

**Per Station CPN - Send Calling Number**

Determines Calling Party Number (CPN) information sent on outgoing calls from this station.

| Valid Entries | Usage  |
|---------------|--|
| y             | All outgoing calls from the station deliver the CPN information as “Presentation Allowed.”                                     |
| n             | No CPN information is sent for the call.   |
| r             | Outgoing non-DCS network calls from the station delivers the Calling Party Number information as “Presentation Restricted.”    |
| blank         | The sending of CPN information for calls is controlled by administration on the outgoing trunk group the calls are carried on. |

**Display Language**

| Valid Entry   | Usage  |
|---|--|
| english<br>french<br>italian<br>spanish<br>user-defined | The language that displays on stations.<br>Time of day is displayed in 24-hour format (00:00 - 23:59) for all languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.).   |
| unicode   | Displays English messages in a 24-hour format . If no Unicode file is installed, displays messages in English by default.<br><br> <b>Note:</b><br>Unicode display is only available for Unicode-supported telephones. Currently, 4610SW, 4620SW, 4621SW, 4622SW, Sage, Spark, and 9600-series telephones (Avaya one-X Deskphone Edition SIP R2 or later) support Unicode display. Unicode is also an option for DP1020 (aka 2420J) and SP1020 (Toshiba SIP Phone) telephones when enabled for the system. |

**Personalized Ringing Pattern**

Defines the personalized ringing pattern for the station. Personalized Ringing allows users of some telephones to have one of 8 ringing patterns for incoming calls. For virtual stations, this field dictates the ringing pattern on its mapped-to physical telephone.

L = 530 Hz, M = 750 Hz, and H = 1060 Hz

| Valid Entries | Usage                  |
|---------------|------------------------|
| 1             | MMM (standard ringing) |
| 2             | HHH                    |
| 3             | LLL                    |
| 4             | LHH                    |
| 5             | HHL                    |
| 6             | HLL                    |
| 7             | HLH                    |
| 8             | LHL                    |

### **Hunt-to Station**

The extension the system should hunt to for this telephone when the telephone is busy. A station hunting chain can be created by assigning a hunt-to station to a series of telephones.

### **Remote Softphone Emergency Calls**

Tells Communication Manager how to handle emergency calls from the IP telephone.

#### **Caution:**

An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. Please be advised that an Avaya IP endpoint cannot dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. Do not use an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations. Please contact your Avaya representative if you have questions about emergency calls from IP telephones.

Available only if the station is an IP Softphone or a remote office station.

| Valid Entry | Usage   |
|-------------|---|
| as-on-local | <p>If the emergency location extension that corresponds to this station's IP address is not administered (left blank), the value as-on-local sends the station emergency location extension to the Public Safety Answering Point (PSAP).</p> <p>If the administrator populates the IP address mapping with emergency numbers, the value as-on-local functions as follows:</p> <ul style="list-style-type: none"> <li>• If the station emergency location extension is the same as the IP address mapping emergency location extension, the value as-on-local sends the extension to the Public Safety Answering Point (PSAP).</li> <li>• If the station emergency location extension is different from the IP address mapping emergency location extension, the value as-on-</li> </ul> |

| Valid Entry | Usage   |
|-------------|---|
|             | local sends the IP address mapping extension to the Public Safety Answering Point (PSAP).   |
| block       | Prevents the completion of emergency calls. Use this entry for users who move around but always have a circuit-switched telephone nearby, and for users who are farther away from the server than an adjacent area code served by the same 911 Tandem office. When users attempt to dial an emergency call from an IP Telephone and the call is blocked, they can dial 911 from a nearby circuit-switched telephone instead.  |
| cesid       | Allows Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP. The end user enters the emergency information into the IP Softphone.<br>Use this entry for IP Softphones with road warrior service that are near enough to the server that an emergency call routed over the it's trunk reaches the PSAP that covers the server or switch. If the server uses ISDN trunks for emergency calls, the digit string is the telephone number, provided that the number is a local direct-dial number with the local area code, at the physical location of the IP Softphone. If the server uses CAMA trunks for emergency calls, the end user enters a specific digit string for each IP Softphone location, based on advice from the local emergency response personnel. |
| option      | Allows the user to select the option (extension, block, or cesid) that the user selected during registration and the IP Softphone reported. This entry is used for extensions that can be swapped back and forth between IP Softphones and a telephone with a fixed location.<br>The user chooses between block and cesid on the softphone. A DCP or IP telephone in the office automatically selects the extension.  |

**Related topics:**

[Emergency Location Ext](#) on page 59

[IP Softphone](#) on page 71

[Emergency Location Extension](#) on page 674

[Remote Office Phone](#) on page 901

**Service Link Mode**

Determines the duration of the service link connection. The service link is the combined hardware and software multimedia connection between an Enhanced mode complex's H.320 DVC system and a server running Avaya Communication Manager that terminates the H.320 protocol. When the user receives or makes a call during a multimedia or IP Softphone or IP Telephone session, a "service link" is established.

| Valid Entry | Usage  |
|-------------|--|
| as-needed   | Used for most multimedia, IP Softphone, or IP Telephone users. Setting the Service Link Mode to as-needed leaves the service link connected for 10 seconds after the user ends a call so that they can immediately |

| Valid Entry | Usage   |
|-------------|---|
|             | place or take another call. After 10 seconds the link is dropped and a new link would have to be established to place or take another call.   |
| permanent   | Used for busy call center agents and other users who are constantly placing or receiving multimedia, IP Softphone, or IP Telephone calls. In permanent mode, the service link stays up for the duration of the multimedia, IP Softphone, or IP Telephone application session. |

### Loss Group

| Valid Entry | Usage   |
|-------------|---|
| 1 to 17     | Determines which administered two-party row in the loss plan applies to each station. Does not appear for stations that do not use loss — such as x-mobile stations and MASI terminals. |

### Speakerphone

Controls the behavior of speakerphones.

| Valid Entry | Usage   |
|-------------|---|
| 1-way       | Indicates that the speakerphone listen-only.  |
| 2-way       | Indicates that the speakerphone is both talk and listen.  |
| grp-listen  | Group Listen allows a telephone user to talk and listen to another party with the handset or headset while the telephone's two-way speakerphone is in the listen-only mode. Others in the room can listen, but cannot speak to the other party through the speakerphone. The person talking on the handset acts as the spokesperson for the group. Group Listen provides reduced background noise and improves clarity during a conference call when a group needs to discuss what is being communicated to another party.<br>Available only with 6400-series and 2420/2410 telephones. |
| none        | Not administered for a speakerphone.  |

### LWC Reception

Indicates where Leave Word Calling (LWC) messages are stored.

| Valid Entry | Usage   |
|-------------|---|
| audix       | LWC messages are stored on the voice messaging system.                          |
| none        | LWC messages are not be stored.   |
| spe         | LWC messages are stored in the system or on the switch processor element (spe). |

### Related topics:

[AUDIX Name](#) on page 662

**Survivable COR**

Sets a level of restriction for stations to be used with the survivable dial plan to limit certain users to only to certain types of calls. You can list the restriction levels in order from the most restrictive to least restrictive. Each level assumes the calling ability of the ones above it. This field is used by PIM module of the Integrated Management to communicate with the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for Standard Local Survivability (SLS) on the H.248 gateways.

Available for all analog and IP station types.

| Valid Entries | Usage  |
|---------------|--|
| emergency     | This station can only be used to place emergency calls.  |
| internal      | This station can only make intra-switch calls. This is the default.  |
| local         | This station can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables.                                      |
| toll          | This station can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables.                                  |
| unrestricted  | This station can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users. |

**Related topics:**

[Survivable ARS Analysis Table](#) on page 919

**Time of Day Lock Table**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 5      | Assigns the station to a Time of Day (TOD) Lock/Unlock table. The assigned table must be administered and active. |
| blank       | Indicates no TOD Lock/Unlock feature is active. This is the default.  |

**Survivable GK Node Name**

Any valid previously-administered IP node name. Identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the H.248 gateways. When a valid IP node name is entered into this field, Communication Manager adds the IP address of this gateway to the bottom of the Alternate Gatekeeper List for this IP network region. As H.323 IP stations register with Communication Manager, this list is sent down in the registration confirm message. This allows the IP station to use the IP address of this Survivable Gatekeeper as the call controller of last resort.

If blank, there are no external gatekeeper nodes within a customer's network. This is the default value.

Available only if the station type is an H.323 station for the 46xx or 96xx models.

**Related topics:**

[Name](#) on page 700

[Type](#) on page 909

**Media Complex Ext**

When used with Multi-media Call Handling, indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to place either a voice or a data call, and voice conversion, coverage, and forwarding apply as if the call were made to the 1-number.

| Valid Entry                | Usage  |
|----------------------------|--|
| A valid BRI data extension | For MMCH, enter the extension of the data module that is part of this multimedia complex.  |
| H.323 station extension    | For 4600 series IP Telephones, enter the corresponding H.323 station. For IP Softphone, enter the corresponding H.323 station. If you enter a value in this field, you can register this station for either a road-warrior or telecommuter/Avaya IP Agent application. |
| blank                      | Leave this field blank for single-connect IP applications.   |

**AUDIX Name**

The voice messaging system associated with the station. Must contain a user-defined adjunct name that was previously administered.

**Related topics:**

[Name](#) on page 700

**Call Appearance Display Format**

Specifies the display format for the station. Bridged call appearances are not affected by this field. Use this field to Available only on telephones that support downloadable call appearance buttons, such as the 2420 and 4620 telephones.

 **Note:**

This field sets the administered display value only for an individual station.

| Valid Entry       | Usage  |
|-------------------|--|
| loc-param-default | The system uses the administered system-wide default value. This is the default.                                 |
| inter-location    | The system displays the complete extension on downloadable call appearance buttons.                              |
| intra-location    | The system displays a shortened or abbreviated version of the extension on downloadable call appearance buttons. |

**Related topics:**

[Display Parameters](#) on page 536

**IP Phone Group ID**

Available only for H.323 station types.

| Valid Entry       | Usage                                 |
|-------------------|---------------------------------------|
| 0 to 999<br>blank | The Group ID number for this station. |

**Always Use**

Enables or disables the following emergency call handling settings:

- A softphone can register no matter what emergency call handling settings the user has entered into the softphone. If a softphone dials 911, the administered **Emergency Location Extension** is used. The softphone's user-entered settings are ignored.
- If an IP telephone dials 911, the administered **Emergency Location Extension** is used.
- If a call center agent dials 911, the physical station extension is displayed, overriding the administered **LoginID for ISDN Display** .

Does not apply to SCCAN wireless telephones, or to extensions administered as type h.323.

**Related topics:**

[Emergency Location Ext](#) on page 59

**Audible Message Waiting**

Enables or disables an audible message waiting tone indicating the user has a waiting message consisting of a stutter dial tone when the user goes off-hook.

This field does *not* control the Message Waiting lamp.

Available only if **Audible Message Waiting** is enabled for the system.

**Related topics:**

[Audible Message Waiting](#) on page 944

**Auto Select Any Idle Appearance**

Enables or disables automatic selection of any idle appearance for transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being transferred or conferenced has. If that attempt fails, Communication Manager selects the first idle appearance.

**Bridged Call Alerting**

Controls how the user is alerted to incoming calls on a bridged appearance.

| Valid Entry | Usage   |
|-------------|---|
| y           | The bridged appearance rings when a call arrives at the primary telephone.  |
| n           | The bridged appearance flashes but does not ring when a call arrives at the primary telephone. This is the default. |

| Valid Entry | Usage  |
|-------------|--|
|             | If disabled and <b>Per Button Ring Control</b> is also disabled, audible ringing is suppressed for incoming calls on bridged appearances of another telephone's primary extension. |

**Related topics:**

[Per Button Ring Control](#) on page 72

**Bridged Idle Line Preference**

Specifies whether the selected line for incoming bridged calls is always an idle line.

| Valid Entry | Usage   |
|-------------|---|
| y           | The user connects to an idle call appearance instead of the ringing call. |
| n           | The user connects to the ringing call appearance.                         |

**CDR Privacy**

Enables or disables Call Privacy for each station. Allows digits in the called number field of an outgoing call record to be blanked on a per-station basis. The number of blocked digits is administered system-wide as CDR parameters.

**Related topics:**

[Privacy — Digits to Hide](#) on page 473

**Conf/Trans On Primary Appearance**

Enables or disables the forced use of a primary appearance when the held call to be conferenced or transferred is a bridge. This is regardless of the administered value for **Auto Select Any Idle Appearance** .

**Related topics:**

[Auto Select Any Idle Appearance](#) on page 68

**Coverage Msg Retrieval**

Allows or denies users in the telephone's Coverage Path to retrieve Leave Word Calling (LWC) messages for this telephone. Applies only if the telephone is enabled for LWC Reception.

**IP Video**

Enables or disables IP video capability for this signaling group. Available only if the signaling group type h.323 and sip.

**Data Restriction**

Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Cannot be assigned if **Auto Answer** is administered as all or acd. If enabled, whisper page to this station is denied.

**Related topics:**

[Auto Answer](#) on page 61

**Direct IP-IP Audio Connections**

Allows or denies direct audio connections between IP endpoints that saves on bandwidth resources and improves sound quality of voice over IP transmissions.

**Display Client Redirection**

Enables or disables the display of redirection information for a call originating from a station with Client Room Class of Service and terminating to this station. When disabled, only the client name and extension or room display. Available only if Hospitality is enabled for the system.

 **Note:**

This field must be enabled for stations administered for any type of voice messaging that needs display information.

**Related topics:**

[Hospitality \(Basic\)](#) on page 946

[Hospitality \(G3V3 Enhancements\)](#) on page 946

**Select Last Used Appearance**

| Valid Entry | Usage   |
|-------------|---|
| y           | Indicates a station's line selection is not to be moved from the currently selected line button to a different, non-alerting line button. The line selection on an on-hook station only moves from the last used line button to a line button with an audibly alerting call. If there are no alerting calls, the line selection remains on the button last used for a call. |
| n           | The line selection on an on-hook station with no alerting calls can be moved to a different line button that might be serving a different extension.  |

**Survivable Trunk Dest**

Designates certain telephones as not being allowed to receive incoming trunk calls when the Media Gateway is in survivable mode. This field is used by the PIM module of the Integrated Management to successfully interrogate the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for SLS on the H.248 gateways.

Available for all analog and IP station types.

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows this station to be an incoming trunk destination while the Media Gateway is running in survivability mode. This is the default. |
| n           | Prevents this station from receiving incoming trunk calls when in survivable mode.   |

**H.320 Conversion**

Enables or disables the conversion of H.320 compliant calls made to this telephone to voice-only. Because the system can handle only a limited number of conversion calls, the number of telephones with H.320 conversion should be limited.

**Idle Appearance Preference**

Indicates which call appearance is selected when the user lifts the handset and there is an incoming call.

| Valid Entry | Usage   |
|-------------|---|
| y           | The user connects to an idle call appearance instead of the ringing call.                       |
| n           | The Alerting Appearance Preference is set and the user connects to the ringing call appearance. |

**IP Audio Hairpinning**

Enables or disables hairpinning for H.323 or SIP Enablement Services (SES) trunk groups. H.323 and SES-enabled endpoints are connected through the IP circuit pack without going through the time division multiplexing (TDM) bus. Available only if **Group Type** is h.323 or sip.

**Related topics:**

[Group Type](#) on page 860

**IP Softphone**

Indicates whether or not this extension is either a PC-based multifunction station or part of a telecommuter complex with a call-back audio connection.

Available only for DCP station types and IP Telephones.

**LWC Activation**

Activates or deactivates the Leave Word Calling (LWC) feature. LWC allows internal telephone users on this extension to leave short pre-programmed messages for other internal users.

LWC should be used if:

- The system has hospitality and the guest-room telephones require LWC messages indicating that wakeup calls failed
- LWC messages are stored in a voice-messaging system

**LWC Log External Calls**

Determines whether or not unanswered external call logs are available to end users. When external calls are not answered, Communication Manager keeps a record of up to 15 calls provided information on the caller identification is available. Each record consists of the latest call attempt date and time.

**Multimedia Early Answer**

Enables or disables multimedia early answer on a station-by-station basis.

The station should be enabled for this feature if the station receives coverage calls for multimedia complexes, but is not multimedia-capable. This ensures that calls are converted and the talk path is established before ringing at this station.

**Mute Button Enabled**

Enables or disables the mute button on the station.

**Per Button Ring Control**

Enables or disables per button ring control by the station user.

| Valid Entries | Usage   |
|---------------|---|
| y             | Allows users to select ring behavior individually for each call-appr, brdg-appr, or abrdg-appr on the station and to enable Automatic Abbreviated and Delayed ring transition for each call-appr on the station. Prevents the system from automatically moving the line selection to a silently alerting call unless that call was audibly ringing earlier. |
| n             | Calls on <b>call-appr</b> buttons always ring the station and calls on <b>brdg-appr</b> or <b>abrdg-appr</b> buttons always ring or not ring based on the <b>Bridged Call Alerting</b> value. Allows the system to move line selection to a silently alerting call if there is no call audibly ringing the station.   |

**Related topics:**

[Bridged Call Alerting](#) on page 68

**Precedence Call Waiting**

Activates or deactivates Precedence Call Waiting for this station.

**Redirect Notification**

Enables or disables redirection notification that gives a half ring at this telephone when calls to this extension are redirected through Call Forwarding or Call Coverage. Must be enabled if LWC messages are stored on a voice-messaging system.

**Related topics:**

[LWC Reception](#) on page 65

**Restrict Last Appearance**

| Valid Entries | Usage   |
|---------------|---|
| y             | Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only. |
| n             | Last idle call appearance is used for incoming priority calls and outgoing call originations.                 |

**EMU Login Allowed**

Enables or disables using the station as a visited station by an Enterprise Mobility User (EMU).

**Bridged Appearance Origination Restriction**

Restricts or allows call origination on the bridged appearance.

| Valid Entry | Usage   |
|-------------|---|
| y           | Call origination on the bridged appearance is restricted.   |
| n           | Call origination on the bridged appearance is allowed. This is normal behavior, and is the default. |

**Voice Mail Number**

The complete Voice Mail Dial Up number. Accepts up to 17 digits.

**Site Data**

This section lets you set information about the Room, Floor, Jack, Cable, Mounting, and Building.

**Room**

| Valid Entry               | Usage  |
|---------------------------|--|
| <i>Telephone location</i> | Identifies the telephone location. Accepts up to 10 characters.  |
| <i>Guest room number</i>  | Identifies the guest room number if this station is one of several to be assigned a guest room and the <b>Display Room Information in Call Display</b> is enabled for the system. Accepts up to five digits. |

**Related topics:**

[Display Room Information in Call Display](#) on page 642

**Floor**

A valid floor location.

**Jack**

Alpha-numeric identification of the jack used for this station.

**Cable**

Identifies the cable that connects the telephone jack to the system.

**Mounting**

Indicates whether the station mounting is d(esk) or w(all).

**Building**

A valid building location.

**Related topics:**

[Site Data](#) on page 877

**Set Color**

Indicates the set color. Valid entries include the following colors: beige, black, blue, brown, burg (burgundy), gray, green, ivory, orng (orange), red, teak, wal (walnut), white, and yel (yellow).

**Cord Length**

The length of the cord attached to the receiver. This is a free-form entry, and can be in any measurement units.

**Headset**

Indicates whether or not the telephone has a headset.

**Speaker**

Indicates whether or not the station is equipped with a speaker.

**Abbreviated Call Dialing**

This section lets you create abbreviated dialing lists for a specific station, and provide lists of stored numbers that can be accessed to place local, long-distance, and international calls; allows you to activate features or access remote computer equipment and select enhanced, personal, system or group lists.

**Abbreviated Dialing List 1, List 2, List 3**

Assigns up to three abbreviated dialing lists to each telephone.

| Valid Entry | Usage   |
|-------------|---|
| enhanced    | Allows the telephone user to access the enhanced system abbreviated dialing list.   |
| group       | Allows the telephone user to access the specified group abbreviated dialing list. Requires administration of a group number.                |
| personal    | Allows the telephone user to access and program their personal abbreviated dialing list. Requires administration of a personal list number. |
| system      | Allows the telephone user to access the system abbreviated dialing list.  |

**Personal List**

Establishes a personal dialing list for telephone or data module users. The personal list must first be assigned to the telephone by the System Administrator before the telephone user can add entries in the list. Users access the lists in order to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Example command: `change abbreviated-dialing personal`

**Abbreviated Dialing Enhanced List**

Establishes system-wide or personal lists for speed dialing.

The Enhanced Abbreviated Dialing List can be accessed by users to place local, long-distance, and international calls; to activate or deactivate features; or to access remote computer equipment.

 **Note:**

Dialing must be enabled in the license file before the Enhanced List can be programmed.

Example command: `display abbreviated-dialing enhanced`

**Related topics:**

[Abbreviated Dialing Enhanced List](#) on page 942

**Group List**

Implements the Abbreviated Dialing Group List. The System Administrator controls the Group Lists. Up to 100 numbers can be entered for every group list. Users can access this list to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Example command: `change abbreviated-dialing group`

**Enhanced Call Fwd**

This section allows you to specify the destination extension for the different types of call forwards.

**Forwarded Destination**

A destination extension for both internal and external calls for each of the three types of enhanced call forwarding (Unconditional, Busy, and No Reply). Accepts up to 18 digits. The first digit can be an asterisk \*.

Requires administration to indicate whether the specific destination is active (enabled) or inactive (disabled).

**SAC/CF Override**

Allows the user of a station with a **Team** button administered, who is monitoring another station, to directly reach the monitored station by pushing the **Team** button. This overrides any currently active rerouting, such as Send All Calls and Call Forwarding, on the monitored station.

| Valid Entries | Usage  |
|---------------|--|
| Ask           | The system asks if the user wants to follow the rerouting or override it. When the user has the option to decide whether rerouting should take place or not, a message is sent to the station that displays the active rerouting and the number of the forwarded to station. |
| No            | Cannot override rerouting. The station does not have the ability to override the rerouting of a monitored station.   |

| Valid Entries | Usage   |
|---------------|---|
| Yes           | Can override rerouting. The station has the ability to override the rerouting the monitored station has set, as long as one incoming call appearance is free. |

**Button Assignment**

This section lets you assign features to the buttons on a phone. You can assign the main buttons for your station by choosing an option from the list down box for each button.

**Group Membership**

This section describes the different groups that an extension can be a member of. You should select the station you want to group and then choose the group from the drop-down box, before clicking **Commit**.

**Understanding groups**

Your voice system uses groups for a number of different purposes. This topic describes the different groups that an extension can be a member of. However, your voice system may include other types of groups as well (for example, trunk groups). For information on those groups, see the Administrator’s Guide to Communication Manager Software.

Your voice system may have any of the following types of groups set up:

| Type                  | Description   |
|-----------------------|---|
| group page            | Group page is a feature that allows you to make an announcement to a pre-programmed group of phone users. The announcement is heard through the speakerphone built into some sets. Users will hear the announcement if their set is idle. Users cannot respond to the announcement. |
| coverage answer group | A coverage answer group lets up to 8 phones ring simultaneously when a call is redirected to the group.   |
| coverage path         | A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call. For more information on coverage paths, see "Creating Coverage Paths" in the Administrator’s Guide to Communication Manager Software.                             |
| hunt group            | A hunt group is a group of extensions that receive calls according to the call distribution method you choose. When a call is made to a certain phone number, the system connects the call to an extension in the group. Use hunt groups when you want more                         |

|                             |   |
|-----------------------------|---|
|                             | <p>than one person to be able to answer calls to the same number.</p> <p>For more information on hunt groups, see "Managing Hunt Groups" in the Administrator's Guide to Communication Manager Software.</p>  |
| intercom group              | <p>An intercom group is a group of extensions that can call each other using the intercom feature. With the intercom feature, you can allow one user to call another user in a predefined group just by pressing a couple of buttons.</p> <p>For more information on intercom groups, see "Using Phones as Intercoms" in the Administrator's Guide to Communication Manager Software.</p> |
| pickup group                | <p>A pickup group is a group of extensions in which one person may pick up another person's calls.</p> <p>For more information on pickup groups, see "Adding Call Pickup" in the Administrator's Guide to Communication Manager Software.</p>   |
| terminating extension group | <p>A Terminating Extension Group (TEG) allows an incoming call to ring as many as 4 phones at one time. Any user in the group can answer the call.</p> <p>For more information on terminating extension groups, see "Assigning a Terminating Extension Group" in the Administrator's Guide to Communication Manager Software.</p>   |

---

## Edit Endpoint Extension field descriptions

Use this page to change the extension of an endpoint.

| Field                               | Description  |
|-------------------------------------|--|
| <b>System</b>                       | Specifies the list of Communication Managers. Select one of the options. |
| <b>Extension</b>                    | Extension of the device you want to change.                              |
| <b>New Extension</b>                | New extension you want to provide for the device.                        |
| <b>Emergency location extension</b> | Existing emergency location extension of your device.                    |

| Field                                   | Description  |
|---|--|
| <b>New emergency location extension</b> | New existing emergency location extension you want to provide. |
| <b>Message lamp extension</b>           | Existing message lamp extension of your device.                |
| <b>New message lamp extension</b>       | New message lamp extension you want to provide.                |

| Button          | Description                                |
|-----------------|--|
| <b>Commit</b>   | Saves the new extension.                   |
| <b>Schedule</b> | Saves the extension at the scheduled time. |
| <b>Reset</b>    | Clears all the entries.                    |
| <b>Cancel</b>   | Takes you back to the previous page.       |

---

## Bulk Add Endpoint field descriptions

| Field                       | Description   |
|-----------------------------|---|
| <b>Template</b>             | The template you choose for the endpoints.  |
| <b>Station name prefix</b>  | Specifies the prefix name that appears for each of the endpoints you add. You can enter a prefix name of your choice in this field. |
| <b>System</b>               | Specifies the list of the Communication Managers.   |
| <b>Available extensions</b> | The list of extensions that are available.  |
| <b>Enter extensions</b>     | The extensions that you want to use. You can enter your preferred extensions in this field.   |

| Button          | Description                                  |
|-----------------|--|
| <b>Commit</b>   | Bulk adds the endpoints.                     |
| <b>Schedule</b> | Bulk adds the station at the scheduled time. |
| <b>Clear</b>    | Undoes all the entries.                      |
| <b>Cancel</b>   | Takes you to the previous page.              |

---

## Bulk Edit Endpoint field descriptions

| Name                       | Description  |
|----------------------------|--|
| <b>Template</b>            | Specifies the endpoint template. You can choose the template which you want to bulk edit.  |
| <b>Station Name Prefix</b> | Specifies the prefix name which appears before all the endpoints that you bulk edit. You can enter a prefix name of your choice. |

| Button          | Description                                     |
|-----------------|---|
| <b>Commit</b>   | Bulk edits the endpoints.                       |
| <b>Schedule</b> | Bulk edits the endpoints at the specified time. |
| <b>Clear</b>    | Undoes the entries.                             |
| <b>Cancel</b>   | Takes you to the previous page.                 |



# Chapter 3: Managing features

---

## Communication Manager objects

---

### Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Feature Management**. It also allows you to directly add, edit, view or delete these objects through **Feature Management**. These objects are:

| <b>Group</b>       | <b>Communication Manager Object</b>  |
|--------------------|--|
| <b>Call Center</b> | Announcements<br>Audio Group<br>Vector<br>Vector Directory Number  |
| <b>Coverage</b>    | Coverage Answer Group<br>Coverage Path<br>Coverage Time of Day   |
| <b>Groups</b>      | Group Page<br>Hunt Group<br>Intercom Group<br>Pickup Group<br>Terminating Group Extension  |
| <b>Network</b>     | Automatic Alternate Routing<br>Automatic Route Selection<br>IP Interfaces<br>IP Network Regions<br>Node Names<br>Route Pattern<br>Signaling Groups |
| <b>Parameters</b>  | System Parameter CDR Option<br>System Parameter Customers Option<br>System Parameter Security<br>System Parameter Special Applications             |
| <b>System</b>      | Class of Restriction   |

|  |  |
|--|--|
|  | Class of Service<br>Dialplan Analysis<br>Dialplan Parameters<br>Feature Access Codes<br>Locations<br>Uniform Dial Plan |
|--|--|

 **Note:**

You cannot add, edit or delete Audio Groups, Announcements, Subscribers and COS objects through Element Cut Through.

**Related topics:**

[Adding Communication Manager objects](#) on page 82

[Editing Communication Manager objects](#) on page 83

[Viewing Communication Manager objects](#) on page 83

[Deleting Communication Manager objects](#) on page 84

[Filtering Communication Manager objects](#) on page 84

---

## Adding Communication Manager objects

1. From the navigation pane, click **Elements > Feature Management**.
2. Select the Communication Manager object to which you want to add.
3. From the Communication Manager list, select a Communication Manager.
4. Click **Show List**.
5. Click **New**.
6. Select the Communication Manager again from the list of Communication Managers.

 **Note:**

Enter the qualifier number in the **Enter Qualifier** field (if applicable).

7. Click **Add**.  
The system displays the Element Cut Through screen where you can enter the attributes of the Communication Manager object you want to add.
  8. Click **Enter** to add the Communication Manager object.  
To return to the Communication Manager screen click **Cancel**.
-

---

## Editing Communication Manager objects

- 
1. From the navigation pane, click **Elements > Feature Management**.
  2. Select the Communication Manager object you want to edit.
  3. Select a Communication Manager from the Communication Manager list.
  4. Click **Show List**.
  5. From the group list, select the device you want to edit.
  6. Click **Edit**.  
The system displays the Element Cut Through screen where you can edit the attributes of the device you have chosen.
  7. To save the changes and go back to the Communication Manager screen, click **Enter**.  
To undo the changes and return to the Communication Manager screen, click **Cancel**.
- 

---

## Viewing Communication Manager objects

- 
1. From the navigation pane, click **Elements > Feature Management**.
  2. Select the Communication Manager object you want to view.
  3. From the list of Communication Managers, select an option.
  4. Click **Show List**.
  5. From the group list, select the object you want to view.
  6. Click **View**.  
You can view the attributes of the object you have selected in the Element Cut Through screen.
  7. To return to the Communication Manager screen, click **Cancel**.
-

---

## Deleting Communication Manager objects

- 
1. From the navigation pane, click **Elements > Feature Management**.
  2. Select the Communication Manager object you want to delete.
  3. Select a Communication Manager from the list of Communication Managers.
  4. Click **Show List**.
  5. Select the object or objects you want to delete from this group.
  6. Click **Delete**.
  7. Confirm to delete the Communication Manager object(s).
- 

---

## Filtering Communication Manager objects

- 
1. From the navigation pane, click **Elements > Feature Management**.
  2. Select the Communication Manager object you want to filter.
  3. Select one of the Communication Managers from the Communication Manager list.
  4. Click **Show List**.
  5. Click **Filter: Enable** in the group List.
  6. Filter the Communication Manager objects according to one or multiple columns.
  7. Click **Apply**.  
To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

 **Note:**

The table displays only those devices that match the filter criteria.

---

---

## Announcements

---

### What is an announcement?

An announcement is a recorded message a caller hears while the call is in a queue. An announcement is often used in conjunction with music. Announcements are recorded on special circuit packs (TN750, TN750B, TN750C, or TN2501AP) on your Communication Manager system.

The three types of announcements are:

- delay announcement — explains the reason for the delay and encourages the caller to wait
- forced announcement — explains an emergency or service problem. Use when you anticipate a large number of calls about a specific issue
- information announcement — gives the caller instructions on how to proceed, information about the number called, or information that the caller wants

Announcements are most effective when they are:

- short, courteous, and to-the-point
- spaced close together when a caller on hold hears silence
- spaced farther apart when music or ringing is played on hold
- played for calls waiting in queue

Music on Hold is a package of professionally-recorded music available from Avaya.

---

### Announcement List

Announcement List displays the property of an announcement. You can navigate through **Elements > Feature Management > Call Center > Announcements** to view this list.

| Name             | Description   |
|------------------|---|
| <b>Name</b>      | Specifies the filename of the audio file. The filename can be up to 27 characters and must be alphanumeric. |
| <b>Extension</b> | Valid extension number for the announcement. Extension numbers may not include punctuation.                 |

| Name               | Description   |
|--------------------|---|
| <b>Group/Board</b> | This field indicates whether the announcement's audio file exists on the VAL board. Type the group number in the format gggV9 for media gateway vVAL, where ggg is the gateway number of the media gateway (up to 250).   |
| <b>Type</b>        | Specifies the type of the announcement. Possible values include: <ul style="list-style-type: none"> <li>• <b>Integ-mus</b> – integrated music type</li> <li>• <b>Integ-rep</b> – integrated repeating type</li> <li>• <b>Integrated</b> – stored internally on a special integrated announcement circuit pack. Use this for general announcements and VDN of Origin Announcements.</li> </ul>   |
| <b>Protected</b>   | Use this field to set the protection mode for an integrated announcement. When you set this field to <b>y</b> , the recording is protected and cannot be deleted or changed through a telephone session or FTP. When you set this field to <b>n</b> , you can change or delete the recording if you have the corresponding console permissions.   |
| <b>Rate</b>        | If the VAL board is administered on the circuit packs form, then 64 (64Kbps) automatically appears in the Rate field.   |
| <b>COR</b>         | The Class of Restriction associated with this announcement.   |
| <b>TN</b>          | Specifies the tenant partition number of the announcement. Valid entries include 1 to 100.  |
| <b>Queue</b>       | Specifies the announcement queuing or barge-in. Possible values include: <ul style="list-style-type: none"> <li>• <b>no</b> (default)- indicates that the announcement does not play if a port is not available.</li> <li>• <b>yes</b> indicates that the request queues when all ports on the circuit pack are busy. The announcement plays when a port becomes available. This setting is recommended for most call center applications.</li> <li>• <b>bargain</b> indicates that you can connect callers to the announcement at any time while it is playing. With n or y, the caller is always connected to the beginning of the announcement.</li> </ul> |
| <b>Size</b>        | The size of the audio files in kilobytes.   |
| <b>Timestamp</b>   | The date and time the audio file was created or modified. This changes each time the audio file is put on the VAL board using FTP.  |
| <b>System</b>      | Specifies the name of the Communication Manager associated with the announcement.   |

---

## Adding an announcement

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. Select **New**.
  5. Complete the Add Announcement page and click **Commit**.
- 

**Related topics:**

[Announcements field descriptions](#) on page 93

---

## Editing an announcement

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. From the Announcement list, select the announcement you want to edit.
  5. Click **Edit** or **View > Edit**.
  6. Edit the required fields on the Edit Announcement page.
  7. Click **Commit** to save the changes.
- 

**Related topics:**

[Announcements field descriptions](#) on page 93

---

## Viewing an announcement

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. Select the announcement you want to view.
  5. Click **View**.  
You can view the properties of the announcement in the View Announcements page.
- 

### Related topics:

[Announcements field descriptions](#) on page 93

---

## Deleting an announcement

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. From the Announcement list, select the announcement(s) you want to delete.
  5. Click **Delete**.
  6. Confirm to delete the announcement(s).
- 

---

## Saving an announcement

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
  2. Select one of the Communication Managers from the Communication Managers list.

3. Click **Show List**.
4. Select the announcements you want to save from the Announcements list.
5. Click **More Actions > Save**.  
This action internally edits and updates the announcements in the Communication Manager.

---

**Related topics:**

[Announcements field descriptions](#) on page 93

---

## Backing up announcements

1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
2. Select one of the Communication Managers from the Communication Managers list.
3. Click **Show List**.
4. Select the announcement(s) you want to backup.
5. Click **More Actions > Backup** to back up your announcements.

---

**Related topics:**

[Announcements field descriptions](#) on page 93

---

## Backing up all announcements

1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
2. Select one of the Communication Managers from the Communication Managers list.
3. Click **Show List**.
4. Click **More Actions > Backup All** to back up all the announcements.

---

## Downloading announcements

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. Click **More Actions > Download**.
  5. Select the files you want to download from the Backedup Announcements list.
  6. Click **Download** to download the backed up announcements.

---

**Related topics:**

[Announcements field descriptions](#) on page 93

---

## Restoring announcements

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. Click **More Actions > Restore**.
  5. Select a Communication Manager from the Communication Manager list.
  6. Select the option(s) from the Restore Options section.
  7. If you want to restore from client, select the **Restore from Client** checkbox.
  8. Select the announcements you want to restore from the Backedup Announcement List.
  9. Click **Restore** to restore your announcement and announcement property files from your application to a VAL / Virtual VAL board you select.

---

**Related topics:**

[Announcements field descriptions](#) on page 93

---

## Restoring all announcements

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. Click **More Actions > Restore All**.
- 

---

## Moving an announcement

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. Click **More Actions > Move**.
  5. Select the destination where you want to move the announcement.
  6. Click **Now** to move the announcements from one VAL board to another within the same voice system.
- 

### Related topics:

[Announcements field descriptions](#) on page 93

---

## Broadcasting announcements

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.

4. Select the announcements you want to broadcast from the Announcement list.
5. Click **More Actions** > **Broadcast**.
6. Select the destination VAL source.
7. Click **Now** to broadcast the announcement files to various VAL boards on a voice system.

---

**Related topics:**

[Announcements field descriptions](#) on page 93

---

## File Transfer Settings in announcements

1. From the navigation pane, click **Elements** > **Feature Management** > **Call Center** > **Announcements**.
2. Select one of the Communication Managers from the Communication Managers list.
3. Click **Show List**.
4. Select an announcement from the Announcement list.
5. Click **More Actions** > **File Transfer Settings**.
6. Select a VAL board from the VAL Board and Media Gateway list.
7. Click **Done**.

---

**Related topics:**

[Announcements field descriptions](#) on page 93

---

## List Usage Extension in announcements

1. From the navigation pane, click **Elements** > **Feature Management** > **Call Center** > **Announcements**.
2. Select one of the Communication Managers from the Communication Managers list.
3. Click **Show List**.
4. Select an announcement from the Announcement list.
5. Click **More Actions** > **List Usage Extension**.

You can view the details of the announcement through the List Usage for Extension list.

6. Click **Done**.

---

**Related topics:**

[Announcements field descriptions](#) on page 93

---

## Filtering the Announcements list

1. From the navigation pane, click **Elements > Feature Management > Call Center > Announcements**.
2. Click **Filter: Enable** in the Announcement list.
3. Filter the list according to one or multiple columns.
4. Click **Apply**.  
To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.



**Note:**

The table displays only those options that match the filter criteria.

---

## Announcements field descriptions

| Name               | Description   |
|--------------------|---|
| <b>Name</b>        | Specifies the filename of the audio file. The filename can be up to 27 characters and must be alphanumeric.   |
| <b>Extension</b>   | Valid extension number for the announcement. Extension numbers may not include punctuation.   |
| <b>Group/Board</b> | This field indicates whether the announcement's audio file exists on the VAL board. Type the group number in the format <i>gggV9</i> for media gateway vVAL, where <i>ggg</i> is the gateway number of the media gateway (up to 250). |

| Name             | Description   |
|------------------|---|
| <b>Type</b>      | Specifies the type of the announcement. Possible values include: <ul style="list-style-type: none"> <li>• <b>Integ-mus</b> – integrated music type</li> <li>• <b>Integ-rep</b> – integrated repeating type</li> <li>• <b>Integrated</b> – stored internally on a special integrated announcement circuit pack. Use this for general announcements and VDN of Origin Announcements.</li> </ul>   |
| <b>Protected</b> | Use this field to set the protection mode for an integrated announcement. When you set this field to <b>y</b> , the recording is protected and cannot be deleted or changed through a telephone session or FTP. When you set this field to <b>n</b> , you can change or delete the recording if you have the corresponding console permissions.   |
| <b>Rate</b>      | The recording rate speed for announcements. If the VAL board is administered on the circuit packs form, then 64 (64Kbps) automatically appears in this field.   |
| <b>COR</b>       | The Class of Restriction associated with this announcement.   |
| <b>TN</b>        | Specifies the tenant partition number of the announcement. Valid entries include 1 to 100.  |
| <b>Queue</b>     | Specifies the announcement queuing or barge-in. Possible values include: <ul style="list-style-type: none"> <li>• <b>no</b> (default)- indicates that the announcement does not play if a port is not available.</li> <li>• <b>yes</b> indicates that the request queues when all ports on the circuit pack are busy. The announcement plays when a port becomes available. This setting is recommended for most call center applications.</li> <li>• <b>bargain</b> indicates that you can connect callers to the announcement at any time while it is playing. With n or y, the caller is always connected to the beginning of the announcement.</li> </ul> |
| <b>Size</b>      | The size of the audio file in kilobytes.  |
| <b>Timestamp</b> | The date and time the audio file was created or modified. This changes each time the audio file is uploaded.  |
| <b>System</b>    | Specifies the name of the Communication Manager associated with the announcement.   |

### Audio File Information

| Name                        | Description  |
|-----------------------------|--|
| <b>Use Unused Wave File</b> | Select this checkbox to use an audio file that has not been used yet.                        |
| <b>Upload Audio File</b>    | You can upload an audio file through this option by browsing to the file you want to upload. |

## More Actions in Audio Groups field description

| Name  | Description   |
|---|---|
| <b>File Name</b>  | Specifies the filename of the audio file. The filename can be up to 27 characters and must be alphanumeric.   |
| <b>File Size</b>  | The size of the audio file in kilobytes.  |
| <b>Backup Announcement Properties</b>                                   | Backs up the announcement property  |
| <b>Backup Wave Files</b>  | Backs up the WAVE files only  |
| <b>Backup Both (Announcement Properties with associated wave file)</b>  | Backs up both the announcement property and the WAVE file for the announcement.   |
| <b>Restore Announcement Properties</b>                                  | Restores only your announcement properties  |
| <b>Restore Wave Files</b>   | Restores only the wave files present for the announcement.  |
| <b>Restore Both (Announcement Properties with associated wave file)</b> | Restores both the announcement property and the wave file for the announcement.   |
| <b>VAL Board</b>  | Specifies the group number of the VAL board. Type the group number in the format gggV9 for media gateway vVAL, where <i>ggg</i> is the gateway number of the media gateway (up to 250).<br>Type the board format as: cabinet(01-64): carrier(A-E): slot(01-20). For example, 03A10. |
| <b>Type</b>   | Specifies whether the Announcement is a VAL Announcement or a Media Gateway (MG) Announcement.  |
| <b>Transfer Mode</b>  | Type of transfer used to backup or restore or upload audio files. Possible values are FTP, SFTP, and, SCP.  |
| <b>Used By</b>  | Specifies the object in which the extension is used. For example Endpoint, Announcement etc.  |
| <b>Object info</b>  | Specifies the details of the object.  |
| <b>Used as</b>  | Specifies how the extension is used in the object.  |

| Button          | Description                                |
|-----------------|--|
| <b>Commit</b>   | Completes the action you initiate.         |
| <b>Schedule</b> | Performs the action at the chosen time.    |
| <b>Reset</b>    | Clears the action and resets the field.    |
| <b>Clear</b>    | Clears all the entries.                    |
| <b>Edit</b>     | Allows you to edit the fields in the page. |

| Button          | Description   |
|-----------------|---|
| <b>Done</b>     | Completes your current action and takes you to the subsequent page. |
| <b>Cancel</b>   | Cancels your current action and takes you to the previous page.     |
| <b>Download</b> | Downloads the audio files or announcement files.                    |
| <b>Now</b>      | Performs the action you initiate real time.                         |
| <b>Restore</b>  | Restores your announcements on the voice system you select.         |

---

## Audio Groups

---

### What is an audio group?

An audio group is a logical container that holds VAL sources. An audio group can hold several VAL Sources which can be VAL Boards or media gateways.

---

### Adding an audio group

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Audio Groups**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. Click **New**.
  5. Complete the Add Audio Groups page and click **Commit**.
- 

**Related topics:**

[Audio Groups field descriptions](#) on page 99

---

## Editing an audio group

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Audio Groups**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. Select the audio group you want to edit.
  5. Click **Edit** or **View > Edit**.
  6. Edit the required fields and click **Commit** to save the changes.

---

### Related topics:

[Audio Groups field descriptions](#) on page 99

---

## Viewing an audio group

- 
1. From the navigation pane, click **Elements > Feature Management > Call Center > Audio Groups**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. Select the audio group you want to view.
  5. Click **View** to view the properties of the audio group.

---

### Related topics:

[Audio Groups field descriptions](#) on page 99

---

## Deleting an audio group

- 
1. From the navigation pane, click **Elements** > **Feature Management** > **Call Center** > **Audio Groups**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. Select the audio group(s) you want to delete from the list.
  5. Click **Delete**.
  6. Confirm to delete the audio group(s).
- 

---

## More actions in audio groups

- 
1. From the navigation pane, click **Elements** > **Feature Management** > **Call Center** > **Audio Groups**.
  2. Select one of the Communication Managers from the Communication Managers list.
  3. Click **Show List**.
  4. Select an option from the Audio Groups list.
  5. Click **More Actions**.
  6. Do one of the following:
    - Click **Backup** to back up the audio groups you selected on a voice system.
    - Click **Download** to download the audio groups you selected.
    - Click **Restore** to restore the audio groups on a voice system you select.
- 

### Related topics:

[Audio Groups field descriptions](#) on page 99

## Audio Groups field descriptions

| Name                | Description  |
|---------------------|--|
| <b>System</b>       | Specifies the device type. In this case, the Communication Manager you choose. |
| <b>Group Number</b> | Specifies the audio group number.  |
| <b>Group Name</b>   | Specifies the name of the audio group.   |

### Members List

| Name               | Description  |
|--------------------|--|
| <b>Group/Board</b> | This field indicates whether the announcement's audio file exists on the VAL board. Type the group number in the format gggV9 for media gateway vVAL, where <i>ggg</i> is the gateway number of the media gateway (up to 250). |
| <b>Is Member</b>   | Specifies whether the VAL board or the Media gateway shown is a member in the audio group.   |



#### Note:

You can filter the Members list according to one or multiple columns using the **Filter: Enable** option in the list.

### More Actions in Announcements- field descriptions

| Name   | Description   |
|--|---|
| <b>CM</b>  | Specifies the Communication Manager you have chosen.                            |
| <b>Backup Announcement Properties</b>                                  | Backs up the announcement property.   |
| <b>Backup Wave Files</b>   | Backs up the waves files only.  |
| <b>Backup Both (Announcement Properties with associated wave file)</b> | Backs up both the announcement property and the wave file for the announcement. |
| <b>File Name</b>   | Name of the audio group.  |
| <b>File Size</b>   | Specifies the size of the audio file in kilobytes.                              |
| <b>Restore Announcement Properties</b>                                 | Restores only your announcement properties.                                     |
| <b>Restore Wave Files</b>  | Restores only the wave files present for the announcement.                      |

| Name  | Description   |
|---|---|
| <b>Restore Both (Announcement properties with Associated wave file)</b> | Restores both the announcement property and the wave file for the announcement. |
| <b>Restore from client</b>  | Select this checkbox if you want to restore from the client machine.            |

| Button          | Description   |
|-----------------|---|
| <b>Commit</b>   | Performs the action you initiate.                                   |
| <b>Schedule</b> | Performs the action at the specified time.                          |
| <b>Reset</b>    | Clears the action and resets the fields.                            |
| <b>Clear</b>    | Clears all the entries.   |
| <b>Done</b>     | Completes your current action and takes you to the subsequent page. |
| <b>Cancel</b>   | Cancel your current action and takes you to the previous page.      |
| <b>Restore</b>  | Restores your announcements on the voice system you select.         |
| <b>Backup</b>   | Backs up the audio files that you select.                           |
| <b>Download</b> | Downloads the audio files or announcement files.                    |
| <b>Now</b>      | Performs the action you initiate real time.                         |

---

## Messaging Class of Service

A Class of Service (COS) is a set of messaging capabilities that you define and assign to subscribers. The Class of Service page lists the current name and number of the different Classes of Service. You can only view the COS names and numbers on this screen; you cannot use this screen to change the COS names or numbers.

---

## Viewing Class of Service

1. From the navigation pane, click **Elements > Feature Management > Messaging > Class of Service**.
2. Choose one or more messaging systems from the Messaging Systems list.

3. Click **Show List**.
  4. Click the respective column heading to sort the Class of Service by **Name** (in alphabetical order) or by **Class No.** (by numeric order).  
This is a read-only list.
- 

---

## Class of Service List field descriptions

| Name                    | Description  |
|-------------------------|--|
| <b>Class No</b>         | Specifies the number of each class of service.                           |
| <b>Name</b>             | Specifies the name of the class of service.                              |
| <b>Last Modified</b>    | Specifies the time and date when the class of service was last modified. |
| <b>Messaging System</b> | Specifies the type of messaging system.                                  |

---

## Subscribers

---

### Subscriber Management

System Manager lets you perform selected messaging system administration activities. You can add, view, edit, and delete subscribers through System Manager. Apart from subscriber management, you can also administer mailboxes and modify mailbox settings for a messaging system.

System Manager supports:

- Communication Manager versions 5.0 and later
- Avaya Aura™ Messaging versions 5.0 and later
- Communication Manager Messaging version 5.2 (with LDAP support) and later

---

## Adding a Subscriber

1. From the navigation pane, click **Elements > Feature Management > Messaging > Subscriber**.
2. From the list of messaging systems, select one or more of the messaging systems.
3. Click **Show List**.
4. Click **New**.
5. Complete the **Basic Information, Subscriber Directory, Mailbox Features, Secondary Extensions, Miscellaneous** sections.
6. Complete the Add Subscriber page and click **Commit** to add the subscriber.



If you select more than one Modular Messaging or Communication Manager Messaging from the list of messaging systems, and then click **New**, the system displays the Add Subscriber page with the first Modular Messaging or Communication Manager Messaging in context.

---

### Related topics:

- [Subscribers \(CMM\) field descriptions](#) on page 105
- [Subscribers \(MM\) field descriptions](#) on page 107

---

## Editing a Subscriber

1. From the navigation pane, click **Elements > Feature Management > Messaging > Subscriber**.
  2. From the list of messaging systems, select one of the messaging systems.
  3. Click **Show List**.
  4. From the subscriber list choose the subscriber you want to edit.
  5. Click **Edit** or **View > Edit**.
  6. Edit the required fields in the Edit Subscriber page.
  7. Click **Commit** to save the changes.
-

**Related topics:**

[Subscribers \(CMM\) field descriptions](#) on page 105

[Subscribers \(MM\) field descriptions](#) on page 107

---

## Viewing a Subscriber

1. From the navigation pane, click **Elements > Feature Management > Messaging**.
2. Click **Subscriber**.
3. From the list of messaging systems, select one of the messaging systems.
4. Click **Show List**.
5. From the subscriber list, select the subscriber you want to view.
6. Click **View**.

**Note:**

You cannot edit any field in the View Subscriber page.

---

**Related topics:**

[Subscribers \(CMM\) field descriptions](#) on page 105

[Subscribers \(MM\) field descriptions](#) on page 107

---

## Deleting a Subscriber

1. Click **Elements > Feature Management > Messaging**.
2. Click **Subscriber**.
3. From the Messaging Systems list, select one of the messaging systems.
4. Click **Show List**.
5. From the subscriber list, select the subscriber or subscribers you want to delete.
6. Click **Delete**.  
The system displays a confirmation page for deleting the subscriber.
7. Confirm to delete the subscriber or subscribers.



**Note:**

You cannot delete a subscriber associated with a user through mailbox management. You can delete the user associated subscribers only through User Profile Management.

## Subscriber List

Subscriber list displays all the subscribers under a messaging version (Communication Manager Messaging or Modular Messaging). You can apply filters to each column in the Subscriber List. You can also sort the subscribers according to each of the column in the Subscriber List. When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name                    | Description  |
|-------------------------|--|
| <b>Name</b>             | Specifies the name of the subscriber.  |
| <b>Mailbox Number</b>   | Specifies the subscriber's mailbox number.   |
| <b>Email Handle</b>     | Specifies the subscriber's e-mail handle.  |
| <b>Telephone Number</b> | Specifies the telephone number of the mailbox.   |
| <b>Last Modified</b>    | Specifies the time and date when the subscriber's details were last modified.                            |
| <b>User</b>             | If a subscriber is associated with a user, then the system displays the name of the user in this column. |
| <b>System</b>           | Specifies the subscriber's messaging system.   |

## Filtering Subscribers

1. From the navigation pane, click **Elements > Feature Management > Messaging > Subscriber**.
2. Select one of the supported messaging versions from the list.
3. Click **Show List**.
4. Click the **Filter: Enable** option in the Subscriber List.
5. Filter the subscribers according to one or multiple columns.
6. Click **Apply**.

To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

**Note:**

The table displays only those subscribers that match the filter criteria.

---

## Subscribers (CMM) field descriptions

| Field                   | Description   |
|-------------------------|---|
| <b>System</b>           | Specifies the messaging system of the subscriber you want to add.                               |
| <b>Template</b>         | Specifies the template for this subscriber. You can choose any template from the drop-down box. |
| <b>Type</b>             | Specifies the messaging type of your subscriber.  |
| <b>Software Version</b> | Specifies the messaging version of the subscriber.  |
| <b>Save as Template</b> | Saves your current settings as a template.  |

### Basic Information

| Field               | Description   |
|---------------------|---|
| <b>Last Name</b>    | Specifies the last name of the subscriber.  |
| <b>First Name</b>   | Specifies the first name of the subscriber.   |
| <b>Extension</b>    | Specifies a number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must: <ul style="list-style-type: none"> <li>• Be within the range of Extension Numbers assigned to your system.</li> <li>• Not be assigned to another local subscriber.</li> <li>• Be a valid length on the local machine.</li> </ul> |
| <b>Password</b>     | The default password that a user has to use to login to his/her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank   |
| <b>COS</b>          | The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.   |
| <b>Community ID</b> | Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.   |

| Field                | Description  |
|----------------------|--|
| <b>Switch Number</b> | <p>Specifies the number of the switch on which this subscriber's extension is administered. You can enter "0" through "99", or leave this field blank.</p> <ul style="list-style-type: none"> <li>• Leave this field blank if the host switch number should be used.</li> <li>• Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.</li> </ul> |
| <b>Account Code</b>  | <p>Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.</p>   |

### Subscriber Directory

| Field               | Description   |
|---------------------|---|
| <b>Email Handle</b> | <p>Specifies the name that appears before the machine name and domain in the subscriber's e-mail address.</p> |
| <b>Common Name</b>  | <p>Specifies the display name of the subscriber.</p>  |

### Mailbox Features

| Field                     | Description   |
|---------------------------|---|
| <b>Covering Extension</b> | <p>Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.</p> |

### Secondary Extensions

| Field                      | Description   |
|----------------------------|---|
| <b>Secondary extension</b> | <p>Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension.</p> |

### Miscellaneous

| Field         | Description   |
|---------------|---|
| <b>Misc 1</b> | <p>Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.</p> |
| <b>Misc 2</b> | <p>Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.</p> |

| Field         | Description  |
|---------------|--|
| <b>Misc 3</b> | Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 4</b> | Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |

| Button                  | Description   |
|-------------------------|---|
| <b>Commit</b>           | Adds the subscriber to the messaging system.              |
| <b>Schedule</b>         | Adds the subscriber at the specified time.                |
| <b>Save as Template</b> | Saves the settings as a template.                         |
| <b>Reset</b>            | Clears all the changes.                                   |
| <b>Edit</b>             | Allows you to edit the fields.                            |
| <b>Done</b>             | Completes your action and takes you to the previous page. |
| <b>Cancel</b>           | Takes you to the previous page.                           |

---

## Subscribers (MM) field descriptions

| Field                   | Description  |
|-------------------------|--|
| <b>System</b>           | Specifies the messaging system of the subscriber you want to add. You can choose this option from the drop-down box. |
| <b>Type</b>             | Specifies the messaging type of your subscriber.   |
| <b>Template</b>         | Specifies the messaging template of a subscriber. You can choose an option from the drop-down box.                   |
| <b>Software Version</b> | Specifies the message version of the subscriber.   |
| <b>Save as Template</b> | Saves your current settings as a template.   |

### Basic Information

| Field                  | Description  |
|------------------------|--|
| <b>Last Name</b>       | Specifies the last name of the subscriber.   |
| <b>First Name</b>      | Specifies the first name of the subscriber.  |
| <b>Numeric Address</b> | Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number. |
| <b>PBX Extension</b>   | The primary telephone extension of the subscriber.   |

| Field               | Description   |
|---------------------|---|
| <b>COS</b>          | The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box. |
| <b>Community ID</b> | Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.                         |
| <b>Password</b>     | Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.                                     |

### Subscriber Directory

| Field                        | Description   |
|------------------------------|---|
| <b>Email Handle</b>          | Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.   |
| <b>Telephone Number</b>      | The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses (()) and (()). |
| <b>Common Name</b>           | Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.   |
| <b>ASCII Version of Name</b> | If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.   |

### Subscriber Security

| Field                     | Description   |
|---------------------------|---|
| <b>Expire Password</b>    | Specifies whether your password expires or not. You can choose one of the following: <ul style="list-style-type: none"> <li>• <b>yes</b>: for password to expire</li> <li>• <b>no</b>: if you do not want your password to expire</li> </ul>  |
| <b>Is Mailbox Locked?</b> | Specifies whether you want your mailbox to be locked. A subscriber mailbox can become locked after two unsuccessful login attempts. You can choose one of the following: <ul style="list-style-type: none"> <li>• <b>no</b>: to unlock your mailbox</li> <li>• <b>yes</b>: to lock your mailbox and prevent access to it</li> </ul> |

## Mailbox Features

| Field                             | Description  |
|-----------------------------------|--|
| <b>Backup Operator Mailbox</b>    | Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.  |
| <b>Personal Operator Schedule</b> | Specifies when to route calls to the backup operator mailbox. The default value for this field is <b>Always Active</b> .   |
| <b>TUI Message Order</b>          | Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: <ul style="list-style-type: none"> <li>• <b>urgent first then newest</b>: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received.</li> <li>• <b>oldest messages first</b>: to direct the system to play messages in the order they were received.</li> <li>• <b>urgent first then oldest</b>: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received.</li> <li>• <b>newest messages first</b>: to direct the system to play messages in the reverse order of how they were received.</li> </ul> |
| <b>Intercom Paging</b>            | Specifies the intercom paging settings for a subscriber. You can choose one of the following: <ul style="list-style-type: none"> <li>• <b>paging is off</b>: to disable intercom paging for this subscriber.</li> <li>• <b>paging is manual</b>: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber.</li> <li>• <b>paging is automatic</b>: if the TUI automatically allows callers to page the subscriber.</li> </ul>   |
| <b>Voicemail Enabled</b>          | Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: <ul style="list-style-type: none"> <li>• <b>yes</b>: to allow the subscriber to create, forward, and receive messages.</li> <li>• <b>no</b>: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.</li> </ul>   |

## Secondary Extensions

| Field                      | Description   |
|----------------------------|---|
| <b>Secondary extension</b> | Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers. |

## Miscellaneous

| Field         | Description  |
|---------------|--|
| <b>Misc 1</b> | Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 2</b> | Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 3</b> | Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 4</b> | Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |

| Button                  | Description   |
|-------------------------|---|
| <b>Commit</b>           | Adds the subscriber to the messaging system.                      |
| <b>Schedule</b>         | Adds the subscriber at the specified time.                        |
| <b>Save as Template</b> | Saves the settings as a template.                                 |
| <b>Reset</b>            | Clears all your changes.  |
| <b>Edit</b>             | Allows you to edit all the fields.                                |
| <b>Done</b>             | Completes your current action and takes you to the previous page. |
| <b>Cancel</b>           | Takes you to the previous page.                                   |

---

## Class of service

---

### Class of Service

Class of Service (COS) allows you to administer permissions for call processing features that require dial code or feature button access. COS determines the features that can be activated

by or on behalf of endpoints. Using System Manager you can view and modify the Class of Service data.

---

## Editing Class of Service data

- 
1. Click **Elements > Feature Management > System > Class of Service**.
  2. Select a Communication Manager from the list.
  3. Click **Show List**.
  4. Select the Class of Service that you want to edit.
  5. Click **Edit** or **View > Edit**.
  6. Edit the required fields and click **Commit** to save the changes.

---

### Related topics:

[Class of Service field descriptions](#) on page 112

---

## Viewing Class of Service data

- 
1. From the navigation pane, click **Elements > Feature Management > System > Class of Service**.
  2. Select a Communication Manager from the list.
  3. Click **Show List**.
  4. Select the Class of Service you want to view.
  5. Click **View** to view the Class of Service data.

---

### Related topics:

[Class of Service field descriptions](#) on page 112

---

## Filtering the Class of Service list

1. From the navigation pane, click **Elements > Feature Management > System > Class of Service**.
2. Select a Communication Manager from the list.
3. Click **Show List**.
4. Click **Filter: Enable** in the Class of Service list.
5. Filter the list according to one or multiple columns.
6. Click **Apply**.  
To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.



**Note:**

The table displays only those options that match the filter criteria.

---



---

## Class of Service field descriptions

| Name          | Description   |
|---------------|---|
| <b>System</b> | Specifies the name of the Communication Manager associated with the Class of Service. |
| <b>Number</b> | Specifies the Class of Service number.  |

### General options

| Name                             | Description   |
|----------------------------------|---|
| <b>Ad-hoc video conferencing</b> | Enables Ad-hoc Video Conferencing, so that up to six users can participate in a video conference call.  |
| <b>Automatic Callback</b>        | Allows users to request Automatic Callback.   |
| <b>Automatic Exclusion</b>       | Allows a user to activate automatically Exclusion when they go off hook on an endpoint that has an assigned Exclusion button.   |
| <b>Buttonless Auto Exclusion</b> | Allows bridged appearances to operate in the exclusion mode regardless of the existence of an administered exclusion button. Currently this feature is only administrable on a per-endpoint basis |

| Name                                 | Description   |
|--------------------------------------|---|
|                                      | by administering a feature exclusion button. This feature relaxes the requirement to use a feature button.  |
| <b>Call Forwarding Busy / DA</b>     | Allows users to forward calls to any extension when the dialed extension is busy or does not answer.  |
| <b>Call Forwarding Enhanced</b>      | Allows users to designate different preferred destinations for forwarding calls that originate from internal and external callers.  |
| <b>Call Forwarding All Calls</b>     | Allows users to forward all calls to any extension.   |
| <b>Client Room</b>                   | Allows users to access Check-In, Check-Out, Room Change/ Swap, and Maid status functions. In addition, Client Room is required at consoles or telephones that are to receive message waiting notification. You can administer class of service for Client Room only when you have Hospitality Services and a Property Management System interface.  |
| <b>Conference Tones</b>              | This feature provides the conference tone as long as three or more calls are in a conference call.<br>If you enable these tones for countries other than Italy, Belgium, United Kingdom, or Australia, the tones will be equivalent to no tone (silence) unless the tone is independently administered or customized on the Tone Generation screen.   |
| <b>Console Permissions</b>           | Allows multi-appearance telephone users to control the same features that the attendant controls. You might assign this permission to front-desk personnel in a hotel or motel, or to a call center supervisor. With console permission, a user can: <ul style="list-style-type: none"> <li>• Activate Automatic Wakeup for another extension</li> <li>• Activate and deactivate controlled restrictions for another extension or group of extensions</li> <li>• Activate and deactivate Do Not Disturb for another extension or group of extensions</li> <li>• Activate Call Forwarding for another extension</li> <li>• Add and remove agent skills</li> <li>• Record integrated announcements</li> </ul> |
| <b>Contact Closure Activation</b>    | Allows a user to open and close a contact closure relay.  |
| <b>Data Privacy</b>                  | Isolates a data call from call waiting or other interruptions.  |
| <b>Extended Forwarding All</b>       | Allows a user to administer call forwarding (for all calls) from a remote location.   |
| <b>Extended Forwarding Busy / DA</b> | Allows this user to administer call forwarding (when the dialed extension is busy or does not answer) from a remote location.   |

| Name                                 | Description  |
|--------------------------------------|--|
| <b>Intra-Switch CDR</b>              | Administers extensions for which Intra-Switch CDR is enabled.  |
| <b>Masking CPN / Name Override</b>   | Allows users to override the MCSNIC capability (that is, masking the display of calling party information and replacing it with a hard-coded, system-wide text string, Info Restricted).   |
| <b>Off-Hook Alert</b>                | To enable this option, either the Hospitality (Basic) or Emergency Access to Attendant field must be enabled in your license file. When enabled, these fields display as y on the System- Parameters Customer-Options screen.  |
| <b>Personal Station Access (PSA)</b> | Allows users to associate a telephone to their extension with their programmed services, using a feature access code. This field must be set to n for virtual telephones. This field must be set to y at a user's home endpoint in order for that user to use the Enterprise Mobility User (EMU) feature at other endpoints. |
| <b>Priority Calling</b>              | Allows users to dial a feature access code to originate a priority call. Such calls ring differently and override send all calls, if active.   |
| <b>Priority IP Video</b>             | Allows priority video calling, where video calls have an increased likelihood of receiving bandwidth and can also be allocated a larger maximum bandwidth per call.  |
| <b>QSIG Call Offer Originations</b>  | Allows users to invoke QSIG Call Offer services.   |
| <b>Restrict Call Fwd-Off Net</b>     | Restricts users from forwarding calls to the public network. For security reasons, this should be enabled for all classes of service except the ones you use for very special circumstances.   |
| <b>Trk-To-Trk Transfer Override</b>  | Users with this COS override any system and/or COR-to-COR calling party restrictions that would otherwise prohibit the trunk-to-trunk transfer operation for users with this COS.  |
| <b>VIP Caller</b>                    | Enables automatic priority calling when assigned to the originator of a call. A call from a VIP phone is always a priority call without the use of a feature button or FAC.  |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Saves the changes you make.                                   |
| <b>Reset</b>  | Undoes the changes you made.                                  |
| <b>Edit</b>   | Takes you to the Edit Class of Service data page.             |
| <b>Done</b>   | Performs the action you initiate.                             |
| <b>Cancel</b> | Cancel the current action and takes you to the previous page. |

# Chapter 4: Managing inventory

---

## Discovery Management

---

### Discovery Management

The Discovery Management feature allows you to configure System Manager to discover specific devices within the network. This feature also lets you manage the SNMP access parameters used for the discovery process.

Device Discovery detects or discovers your network, including subnets and nodes. Device Discovery exclusively uses Simple Network Management Protocol (SNMP) to discover your network.

Device Discovery in System Manager includes:

- Configuring SNMP access parameters, Communication Manager access parameters and subnets
- Discovering the devices
- Populating the devices discovered in the Network Device Inventory list

---

### SNMP Access list

The SNMP Access list can be used to configure the basic SNMP parameters for specific devices or for a range of devices. **Discovery Management** recognizes SNMP V1 and V3 protocols. For both these protocols access parameters also include timeout and retry values.

| Name                   | Description  |
|------------------------|--|
| <b>Type</b>            | Specifies the SNMP protocol type. Value can either be V1 or V3.          |
| <b>Read Community</b>  | The read community of the device. Only applicable for SNMP V1 protocol.  |
| <b>Write Community</b> | The write community of the device. Only applicable for SNMP V1 protocol. |

| Name                | Description  |
|---------------------|--|
| <b>User</b>         | User name as defined in the application. Applicable for SNMP V3 protocol only.   |
| <b>Auth Type</b>    | The authentication protocol used to authenticate the source of traffic from SNMP V3 protocol users. Possible values are: <ul style="list-style-type: none"> <li>• <b>MD5 (default)</b></li> <li>• <b>SHA</b></li> </ul> Authorization Type is applicable only for SNMP V3 protocol.  |
| <b>Priv Type</b>    | The encryption policy for SNMP V3 users. Possible values are: <ul style="list-style-type: none"> <li>• <b>DES</b> - Use DES encryption for SNMP based communication.</li> <li>• <b>AES</b> - Use AES encryption for SNMP based communication</li> <li>• <b>No Privacy</b> - Do not encrypt traffic for this user</li> </ul> Privacy Type is applicable only for SNMP V3 users. |
| <b>Timeout (ms)</b> | The number of milliseconds discovery waits for the response from the device being polled.  |
| <b>Retries</b>      | The number of times discovery polls a device without receiving a response before timing out.   |
| <b>Description</b>  | Describes the SNMP Access profile.   |

---

## Setting the order in the SNMP Access list

You can set the order in which you want to list the SNMP Access profiles in the SNMP Access list. While polling a device, the SNMP Access profiles are used according to this list.

- 
1. From the navigation pane, click **Elements > Inventory > Discovery Management > Configuration**.
  2. Select the SNMP Access profile you want to move up or move down.
  3. Do one of the following:
    - Click **Move Up** if you want to set the SNMP Access profile one step ahead in the list.
    - Click **Move Down** if you want to set the SNMP Access profile one step down in the list.
- 

### Related topics:

[SNMP Access list](#) on page 115

---

## Adding an SNMP Access profile

- 
1. From the navigation pane, click **Elements > Inventory > Discovery Management > Configuration**.
  2. Click **New**.
  3. Select the SNMP protocol type from the **Type** field.
  4. Complete the Add SNMP Access Configuration page and click **Commit**.
- 

### Related topics:

[SNMP Access field descriptions](#) on page 118

---

## Editing an SNMP Access profile

- 
1. From the navigation pane, click **Elements > Inventory > Discovery Management > Configuration**.
  2. Select the SNMP Access profile which you want to edit.
  3. Click **Edit**.
  4. Edit the required fields on the Edit SNMP Access Configuration page.
  5. Click **Commit** to save the changes.
- 

### Related topics:

[SNMP Access field descriptions](#) on page 118

---

## Deleting an SNMP Access profile

- 
1. From the navigation pane, click **Elements > Inventory > Discovery Management**.
  2. Click **Configuration**.
  3. From the SNMP Access Configuration list, select the SNMP Access profile or profiles you want to delete.

4. Click **Delete**.
5. Confirm to delete the SNMP Access profile(s).

## SNMP Access field descriptions

### For SNMP protocol V3

| Name                                   | Description  |
|--|--|
| <b>Type</b>                            | Specifies the SNMP protocol type. Value can be either V1 or V3.  |
| <b>User</b>                            | User name as defined in the application.   |
| <b>Authentication Type</b>             | <p>The authentication protocol used to authenticate the source of traffic from SNMP V3 users. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>MD5 (default)</b></li> <li>• <b>SHA</b></li> </ul> <p>Authorization Type is applicable only for SNMP V3 protocol.</p>   |
| <b>Authentication Password</b>         | The password used to authenticate the user. Passwords must consist of at least eight characters.   |
| <b>Confirm Authentication Password</b> | You must re-type the SNMP V3 protocol authentication password for confirmation.  |
| <b>Privacy Type</b>                    | <p>The encryption policy for an SNMP V3 user. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>DES</b>- Use DES encryption for SNMP based communication.</li> <li>• <b>AES</b>- Use AES encryption for SNMP based communication.</li> <li>• <b>No Privacy</b> - Do not encrypt traffic for this user.</li> </ul> <p>Privacy Type is only required for an SNMP V3 user.</p> |
| <b>Privacy Password</b>                | The password used to enable DES or AES encryption, if you select DES as the Privacy Type. DES Passwords must consist of at least eight characters.   |
| <b>Confirm Privacy Password</b>        | You must re-type the privacy password in this field for confirmation.  |
| <b>Timeout (ms)</b>                    | The number of milliseconds discovery waits for the response from the device being polled.  |
| <b>Retries</b>                         | The number of times discovery polls a device without receiving a response before timing out.   |

## For SNMP protocol V1

| Field                  | Description  |
|------------------------|--|
| <b>Type</b>            | Specifies the SNMP protocol type. Value can be either V1 or V3.                              |
| <b>Read Community</b>  | The read community of the device. Only applicable for SNMP V1 protocol.                      |
| <b>Write Community</b> | The write community of the device. Only applicable for SNMP V1 protocol.                     |
| <b>Timeout (ms)</b>    | The number of milliseconds discovery waits for the response from the device being polled.    |
| <b>Retries</b>         | The number of times discovery polls a device without receiving a response before timing out. |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Adds or edits the SNMP Access profile (whichever applicable). |
| <b>Reset</b>  | Undoes your action.   |
| <b>Cancel</b> | Takes you to the previous page.                               |

---

## Subnet(s) list

The Subnet(s) list gives the list of subnets that are manually added.

| Name               | Description  |
|--------------------|--|
| <b>Subnet IP</b>   | IP address of the subnet.  |
| <b>Subnet Mask</b> | Specifies the IP subnet mask   |
| <b>Use SNMP V3</b> | Specifies whether you want to only use SNMP V3 protocol. Select the checkbox to only use SNMP V3 protocol. |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Adds or edits the subnet.                                       |
| <b>Reset</b>  | Undoes all the entries.   |
| <b>Cancel</b> | Cancels your current action and takes you to the previous page. |

## Adding a subnet

---

1. From the navigation pane, click **Elements > Inventory > Discovery Management > Configuration**.
  2. Click **New**.
  3. Complete the Add Subnet Configuration page and click **Commit**.
- 

**Related topics:**

[Subnet\(s\) list](#) on page 119

---

## Editing a subnet

---

1. Click **Elements > Inventory > Discovery Management > Configuration**.
  2. Select the subnet you want to edit.
  3. Click **Edit**.
  4. Edit the required fields on the Edit Subnet Configuration page.
  5. Click **Commit** to save the changes.
- 

**Related topics:**

[Subnet\(s\) list](#) on page 119

---

## Deleting a subnet

---

1. From the navigation pane, click **Elements > Inventory > Discovery Management**.
2. Click **Configuration**.
3. On the Configuration screen, select the subnet(s) you want to delete.

4. Click **Delete**.
  5. Confirm to delete the subnet(s).
- 

---

## CM Access list

The CM Access list specifies the Communication Manager login parameters to connect to the Communication Manager servers in your network.

| Name                  | Description  |
|-----------------------|--|
| <b>IP address</b>     | IP address of the Communication Manager.   |
| <b>Port</b>           | Login port of the Communication Manager.   |
| <b>Login</b>          | Login name as configured on the Communication Manager server.  |
| <b>Use ASG Key</b>    | Indicates the use of ASG encryption.   |
| <b>Use SSH</b>        | Indicates the use of SSH protocol.   |
| <b>Global profile</b> | Specifies the default parameters that can be used to configure a Communication Manager server in the Entities application in System Manager. |

---

## Filtering Subnet(s) and CM Access lists

1. From the navigation pane, click **Elements > Inventory > Discovery Management > Configuration**.
2. Click **Filter: Enable** in the Subnet(s) list or the CM Access list.
3. Filter the subnets or the CM access profiles according to one or multiple columns.
4. Click **Apply**.  
To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.



**Note:**

The table displays only those options that match the filter criteria.

---

---

## Adding a Communication Manager Access profile

- 
1. From the navigation pane, click **Elements > Inventory > Discovery Management > Configuration**.
  2. Click **New**.
  3. Complete the Add CM Access details page and click **Commit**.
- 

**Related topics:**

[CM Access profile field descriptions](#) on page 123

---

## Editing a Communication Manager Access profile

- 
1. From the navigation pane, click **Elements > Inventory > Discovery Management > Configuration**.
  2. Select the Communication Manager Access profile you want to edit.
  3. Click **Edit**.
  4. Edit the required fields on the Edit CM Access details page.
  5. Click **Commit** to save the changes.
- 

**Related topics:**

[CM Access profile field descriptions](#) on page 123

---

## Deleting a Communication Manager Access profile

- 
1. From the navigation pane, click **Elements > Inventory > Discovery Management > Configuration**.
  2. Select the Communication Manager Access profile you want to delete.

3. Click **Delete**.
4. Confirm to delete the Communication Manager Access profile.

---

## CM Access profile field descriptions

| Name                    | Description   |
|-------------------------|---|
| <b>IP Address</b>       | IP address of the Communication Manager.  |
| <b>Port</b>             | Login port of the Communication Manager.  |
| <b>Login</b>            | Login name as configured on the Communication Manager server.   |
| <b>Password</b>         | Password for logging in.  |
| <b>Confirm Password</b> | Re-enter password for confirmation.   |
| <b>Use ASG Key</b>      | Indicates the use of ASG encryption.  |
| <b>ASG key</b>          | Specifies the ASG password or key for login. ASG key is a 20 character octal code.  |
| <b>Use SSH</b>          | Indicates the use of SSH protocol.  |
| <b>Global Profile</b>   | Specifies the default parameters that can be used to configure a Communication Manager server in the Entities application in System Manager. You can select this checkbox only once. This checkbox is disabled once you configure the Global Profile. |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Adds or edits the Communication Manager Access profile.        |
| <b>Reset</b>  | Undoes the current action.                                     |
| <b>Cancel</b> | Cancels the current action and takes you to the previous page. |

---

## Discovery

---

### Device Discovery

The **Discovery** tab in **Discovery Management** allows you to configure the subnets and device types to be discovered. You must select the subnet as well as the device type before starting the discovery process.

---

## Discovering devices

1. From the navigation pane, click **Elements** > **Inventory** > **Discovery Management**.
2. Click **Discovery**.
3. Select the subnet and then the device type from the Network Subnet(s) list and the Device Type(s) list respectively.
4. Click **Now** to start the discovery process.



**Note:**

To schedule the discovery process at a later time, click **Schedule**.



**Note:**

To restart the discovery process, select the **Clear previous results** check box. When you select this checkbox, the discovered devices are removed only from the inventory list and not from the Entities application.

---

**Related topics:**

[Discovering Devices field descriptions](#) on page 125

---

## Filtering Network Subnet(s)

1. From the navigation pane, click **Elements** > **Inventory** > **Discovery Management** > **Discovery**.
2. Click **Filter: Enable** in the Network Subnet(s) list.
3. Filter the network subnet(s) according to one or multiple columns.
4. Click **Apply**.  
To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.



**Note:**

The table displays only those options that match the filter criteria.

---

## Discovering Devices field descriptions

### Select Network Subnet list

| Name                        | Description  |
|-----------------------------|--|
| <b>Subnet IP</b>            | IP address of the subnet.  |
| <b>Subnet Mask</b>          | Specifies the subnet mask.   |
| <b>Use SNMP V3</b>          | Specifies whether you want to only use SNMP V3 protocol. Select the checkbox to only use the SNMP V3 protocol.   |
| <b>Discovery Status</b>     | <p>Provides information about the current discovery status. Possible values include:</p> <ul style="list-style-type: none"> <li>• <b>Pending</b></li> <li>• <b>In Progress</b></li> <li>• <b>In Progress: preparing for discovery</b></li> <li>• <b>In Progress: probing network elements</b></li> <li>• <b>In progress: saving discovered elements</b></li> <li>• <b>In progress: collecting inventory information</b></li> <li>• <b>In progress: saving inventory information</b></li> <li>• <b>Failed</b></li> <li>• <b>Idle</b></li> </ul> |
| <b>Last Discovered Time</b> | Latest time when the discovery was carried out.  |

### Select Device Type list

| Name               | Description                       |
|--------------------|-----------------------------------|
| <b>Device Type</b> | Specifies the type of the device. |
| <b>Description</b> | Describes the device type.        |

---

## Discovered Inventory

---

### Discovered Inventory

The **Discovered Inventory** tab displays a list of all the inventory components or items that are discovered. After the discovery is complete, the system lists the discovered devices. You can either choose the **Tree** View or the **List** View for viewing all the discovered devices.

---

### Network Device Inventory list

The Network Device Inventory list displays all the inventory components or items that are discovered. This list also displays some of the properties of the devices discovered. You can sort this list according to any of the columns in the list.

There are two default views of the Network Device Inventory list: List View and Tree View.

- The List View lists every entity that is discovered. In this view, each entity appears as a separate row.
- The Tree View displays the inventory items in groups. The inventory items are grouped by the device type.

**Related topics:**

[Network Device Inventory list field description](#) on page 128

---

### Viewing the Network Device Inventory list

1. From the navigation pane, click **Elements > Inventory > Discovered Inventory**. The system displays the **Network Device Inventory** list, which gives the details of the devices discovered.



**Note:**

This is a read-only list.

2. Click an IP address in the inventory list to view more information about the device.

When you click an IP address in the list, the system displays a window which gives more information about the inventory items for that IP address. This information varies according to the device you choose.

---

**Related topics:**

[Network Device Inventory list field description](#) on page 128

---

## Filtering the Inventory list

1. From the navigation pane, click **Elements > Inventory > Discovered Inventory**.
2. Click **Filter: Enable** in the Discovered Inventory list.
3. Filter the list according to one or multiple columns.
4. Click **Apply**.  
To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

**Note:**

The table displays only those options that match the filter criteria.

---

---

## Using Advanced Search in Discovered Inventory

1. From the navigation pane, click **Elements > Inventory > Discovered Inventory**.
2. Click **Advanced Search** in the Discovered Inventory list.
3. In the Criteria section, do the following:
  - a. Select the search criterion from the first drop-down field.
  - b. Select the operator from the second drop-down field.
  - c. Enter the search value in the third field.

If you want to add a search condition, click **+** and repeat the sub steps listed in step 3.

If you want to delete a search condition, click - . This button is available if there is more than one search condition.

---

## Network Device Inventory list field description

| Name                    | Description  |
|-------------------------|--|
| <b>Family</b>           | Specifies the device family type. Possible values include Communication Manager, Media Gateway and Switches; Application and Element Managers. |
| <b>IP</b>               | IP address of the device.  |
| <b>Name</b>             | Name of the device.  |
| <b>Type</b>             | Specifies the type of the device.  |
| <b>Module ID</b>        | Module ID of the device.   |
| <b>Location</b>         | Location of the device.  |
| <b>Serial No</b>        | Serial number of the hardware.   |
| <b>Software Release</b> | Software release of the device.  |
| <b>Hardware Version</b> | Hardware version of the device.  |

---

## Synchronization of Data

---

### Synchronizing Communication Manager and Messaging data

Managed elements have alternative ways of administering data. To ensure uniformity in the database when a variety of tools are used, you can use the synchronization menu. You can synchronize both Communication Manager and messaging data through this menu.

#### Initializing Synchronization

Initializing synchronization allows you to synchronize data in the System Manager database with each managed Communication Manager system. When you add a Communication Manager into the system, System Manager automatically initiates an initialization task to get all the Communication Manager data that is required, and stores it in the System Manager database.

## Incremental Synchronization

Incremental synchronization with selected devices allows you to incrementally synchronize data in the System Manager database with each managed Communication Manager system. This synchronization updates the changed data in the database in Communication Manager since synchronization was last run.

## Scheduled Synchronization with Communication Manager

You can create and schedule synchronization jobs using System Manager. You can schedule a synchronization job to run at a fixed time and repeat it periodically. System Manager provides a default incremental synchronization every 24 hours. You can modify this to your convenience.

## On demand Synchronization

System Manager allows you to synchronize data with the Communication Manager on demand. Administrators can initiate this at any time. On-demand synchronization can either be initialization synchronization or an incremental synchronization.

## Synchronizing messaging data

You can also synchronize messaging data in System Manager with the Communication Manager Messaging and Modular Messaging systems.



### Note:

You must add a new Communication Manager or a messaging entity through Application Management before you perform synchronization.

### Related topics:

[Initializing Synchronization](#) on page 129

[Incremental Synchronization](#) on page 130

[Saving Communication Manager translations](#) on page 130

---

## Initializing Synchronization

1. From the navigation pane, click **Elements > Inventory > Synchronization > Communication System**.
  2. Select the Communication Managers you want to synchronize.
  3. Select **Initialize data for selected devices**.
  4. Click **Now** to perform the initializing synchronization or do one of the following:
    - a. Click **Schedule** to perform the synchronization at a specified time.
    - b. Click **Cancel** to cancel the synchronization.
-

---

## Incremental Synchronization

---

1. From the navigation pane, click **Elements > Inventory > Synchronization > Communication System**.
2. Select the Communication Managers you want to synchronize.
3. Select **Incremental Sync data for selected devices**.
4. Click **Now** to perform the incremental synchronization or do one of the following:
  - a. Click **Schedule** to perform the synchronization at a specified time.
  - b. Click **Cancel** to cancel the synchronization.

 **Note:**

While scheduling incremental synchronization, you must set the logging levels on Communication Manager using the **change logging-levels** option. Select the **both** option for the **Log Data Values** field.

---

---

## Synchronizing Messaging Data

---

1. From the navigation pane, click **Elements > Inventory > Synchronization > Messaging System**.
  2. Select the messaging systems you want to synchronize
  3. Click **Now** to perform the synchronization or do one of the following:
    - a. Click **Schedule** to perform the synchronization at a specified time.
    - b. Click **Cancel** to cancel the synchronization.
- 

---

## Saving Communication Manager translations

---

1. From the navigation pane, click **Elements > Inventory > Synchronization > Communication System**.
2. Select a Communication Manager from the list.

3. Select **Save Translations for selected devices**.
  4. Click **Now** to save the System Manager administration changes in Communication Manager.  
Click **Schedule** to save the translations at a specified time.
- 

---

## Element Cut Through

---

### Element Cut Through User Reference

The Element Cut Through provides you an interface to all Communication Manager SAT screens.

Click **Elements > Inventory > Synchronization > Communication System** to launch the Element Cut Through screen.



**Warning:**

If you login to System Manager as an administrator, you do not require separate login credentials to launch Element Cut Through.

If you are a custom user, you need explicit login credentials to launch Element Cut Through.

a

Once you launch Element Cut Through you can enter the SAT commands in the **command** field, similar to the SAT native administration command line. Element Cut Through also provides direct access to any field on a Communication Manager administration form, excluding “list / display” forms when selecting a field.

When you launch the Element Cut Through from the Communication Manager Web pages, the voice system IP address and port information are passed to the Element Cut Through from the Communication Manager Web pages.

#### **IP Connectivity**

The Element Cut Through only supports IP connectivity. It does not support direct serial port connection and modem/data module connectivity. Element Cut Through only supports IP connectivity to supported voice systems through SSH, but not through telnet.

#### **Element Cut Through help system**

The Element Cut Through Help System is a part of the *Administering Avaya Aura™ Communication Manager*.

## Element Cut Through commands

The system saves a history of the last 20 commands you entered. Access this command history through a pull-down menu on the command field. Some of the common commands are:

- Add Station Next
- Change Station
- Remove Station
- List Station
- List Cor
- List Coverage Path
- List ARS Analysis
- Display Dialplan Analysis
- List Hunt-Group
- List History

## Buttons

- **Enter** sends completed forms to the voice system
- **Refresh** refreshes the screen
- **Cancel** cancels a command
- **Clear field** undoes all the entries in a command page
- **Help** displays the action command words for the user to enter
- **Previous page** retrieves the previous page of data from the voice system and is mainly used to move between pages in a form
- **Next page** displays the next page of data from the voice system or moves between pages in a form
- **More actions** displays the other actions which you can perform

## Using Help

- Administration Help: launches the entire Element Cut Through Help System. Use Search and Index features for key-word searches.
- Page and field-level Help: Each Element Cut Through screen has a context-sensitive Help topic launched from the **Help** button on each page.
- Print from your browser: You can print Help topics from the print button accessible from the Help GUI. Or, click the topic and use your browser print button.

### **Note:**

The **info** field at the bottom of the screen displays the action a user can perform next. This field also acts as a status bar.

**Note:**

To exit the Element Cut Through screen all users must click **Done**.

---

## System Basics

### Logging into the System

You must log in before you can administer your system. If you are performing remote administration, you must establish a remote administration link and possibly assign the remote administration extension to a hunt group before you log in. The members of this hunt group are the extensions of the data modules available to connect to the system administration terminal. For information about setting up remote administration, contact your Avaya technical support representative. When not using the system, log off for security purposes.

#### Logging in for remote administration

---

1. Dial the Uniform Call Distribution (UCD) group extension number.

**Note:**

The UCD group extension number is assigned when you set up remote administration.

- If you are off-premises, use the Direct Inward Dialing (DID) number, a Listed Directory Number (LDN) (you must use a telephone), or the trunk number dedicated to remote administration.
- If you are on-premises, use an extension number.

If you dialed a DID number, dedicated trunk number, or extension, you receive data tone or visually receive answer confirmation.

If an LDN was dialed, the attendant will answer.

- i. Ask to be transferred to the UCD group extension number.

You receive data tone or visually receive answer confirmation.

- ii. Transfer the voice call to your data terminal.

The Login prompt displays.

2. Complete the steps for Logging into the System.

For information about setting up remote administration, contact your Avaya technical support representative.

See also Enhancing System Security. For a complete description of the Security Violation Notification feature, see Security Violation Notification in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

---

## Accessing the Avaya S8XXX Server

To administer an Avaya S8XXX Server, you must be able to access it. Personal computers and services laptop computers equipped with an SSH client (PuTTY) or Avaya Site Administrator (ASA), and a Web browser are the primary support access for system initialization, aftermarket additions, and continuing maintenance.

You can access an Avaya S8XXX Server in one of three ways:

- directly
- remotely over the customer's local area network (LAN)
- over a modem for Communication Manager Release 5.2 or earlier

A direct connection and over the customer's LAN are the preferred methods. Remote access over a modem is for Avaya maintenance access only.

### Accessing the Avaya S8XXX Server Directly — connected to the services port Prerequisites

Enable IP forwarding to access System Platform through the services port.

---

1. Open the MS Internet Explorer browser.  
Microsoft Internet Explorer version 7.0 is supported.
  2. In the **Location/Address** field, type the IP address of the Communication Manager server.
  3. Press `Enter`.
  4. When prompted, log in to administer the Avaya S8XXX Server and the features of Communication Manager.
- 

### Enabling IP forwarding to access System Platform through the services port

To access System Platform Web Console through the services port, you must enable IP forwarding on System Domain (Dom-0) . You can set the IP forwarding status as enabled or disabled during installation of System Platform. If you disable IP forwarding during installation and later want to enable it, perform the following procedure. For security reasons, always disable IP forwarding after finishing your task.

---

1. To enable IP forwarding:

- a. Start an SSH session.
  - b. Log in to System Domain (Domain-0) as admin.
  - c. In the command line, type `service_port_access enable` and press **Enter**.
2. For security reasons, always disable IP forwarding after finishing your task. Perform the following tasks to disable IP forwarding:
    - a. Start an SSH session.
    - b. Log in to System Domain (Domain-0) as admin.
    - c. In the command line, type `ip_forwarding disable` and press **Enter**.

---

### Accessing the Avaya S8XXX Server Directly — connected to the customer network

---

1. Open the MS Internet Explorer browser.  
Microsoft Internet Explorer version 7.0 is supported.
2. In the **Location/Address** field, type the active server name or IP address.
3. Press `Enter`.
4. When prompted, log in to administer the Avaya S8XXX Server and the features of Avaya Communication Manager.  
You can also connect directly to an individual server using its name or IP address.

---

### Accessing the Avaya S8XXX Server remotely over the network

You can access the Avaya S8XXX Server from any computer connected through the LAN. To access either server, use the IP address assigned to the server you want to access. You can also use the active server address to connect automatically to the server that is active. Once connected, you can administer the server using three tools:

- Web interface for server-specific administration and call processing features.
- Avaya Site Administration for Communication Manager (Only available on the active Communication Manager server).
- An SSH client, like PuTTY, and a configured IP address for the Communication Manager server.

## Using Avaya Site Administration

Avaya Site Administration features a graphical user interface (GUI) that provides access to SAT commands as well as wizard-like screens that provide simplified administration for frequently used features. You can perform most of your day-to-day administration tasks from this interface such as adding or removing users and telephony devices. You can also schedule tasks to run at a non-peak usage time.

This software must be installed on a computer running a compatible Microsoft Windows operating system. Once installed, it can be launched from a desktop icon.

### Installing Avaya Site Administration

#### Prerequisites

If you do not have ASA on your computer, make sure your personal computer (PC) or laptop first meets the following minimum requirements:

**Table 1: Site Administration: Microsoft Windows client computer requirements**

| Component            | Required   | Comments  |
|----------------------|--|---|
| Operating System     | Microsoft Windows XP Professional with Service Pack 3,<br>Microsoft Windows 2003 Standard Edition server with Service Pack 2,<br>Microsoft Windows 2003 Enterprise Edition server with Service Pack 2,<br>Microsoft Windows Vista Business (32-bit and 64-bit editions) with Service Pack 2,<br>Microsoft Windows Vista Enterprise (32-bit and 64-bit editions) with Service Pack 2,<br>Microsoft Windows 7,<br>Microsoft Windows 2008 Standard Edition server with Service Pack 2, or<br>Microsoft Windows 2008 Enterprise Edition server with Service Pack 2 |   |
| Processor            | latest Intel or AMD-based processors   |   |
| Hard Drive           | 1 GB   | Required to install all of the client components.                               |
| Memory               | 512 MB RAM   |   |
| Monitor              | SVGA 1024 X 768 display  |   |
| Network Connectivity | TCP/IP 10/100 Network Card   |   |
| Modem                | 56 Kbps Modem  | May be required for remote access to the computer.                              |
| Other Software       | Internet Explorer 6.0 with Service Pack 1 or Service Pack 2, Internet Explorer 7.0 Service Pack 1, or Internet Explorer 8.0, Mozilla Firefox 3.0 or 3.5 and Java Runtime Environment 1.6.0_16.   | Required to access the Integrated Management Launch Page and Web-based clients. |

Install ASA on your computer using the Avaya Site Administration CD. Place the ASA CD in the CD-ROM drive and follow the installation instructions in the install wizard.

ASA supports a terminal emulation mode, which is directly equivalent to using SAT commands on a dumb terminal or through an SSH session. ASA also supports a whole range of other features, including the graphically enhanced interface (GEDI) and Data Import. For more information see the Help, Guided Tour, and Show Me accessed from the ASA Help menu.

## Starting Avaya Site Administration

---

1. Start up ASA by double-clicking the ASA icon, or click **Start >Programs > Avaya Site Administration**.
2. In the **Target System** field, use the pull-down menu to select the desired system.
3. Click **Start GEDI**.  
You now are connected to the desired system.

## Configuring Avaya Site Administration

When Avaya Site Administration is initially installed on a client machine, it needs to be configured to communicate with Communication Manager on the Avaya S8XXX Server.

When you initially run ASA, you are prompted to create a new entry for the switch connection. You are also prompted to create a new voice mail system if desired.

## Logging in with Access Security Gateway

Access Security Gateway (ASG) is an authentication interface used to protect the system administration and maintenance ports and logins associated with Avaya Communication Manager. ASG uses a challenge and response protocol to validate the user and reduce unauthorized access.

You can administer ASG authentication on either a port type or login ID. If you set ASG authentication for a specific port, it restricts access to that port for all logins. If you set ASG authentication for a specific login ID, it restricts access to that login, even when the port is not administered to support ASG.

Authentication is successful only when Avaya Communication Manager and the ASG communicate with a compatible key. You must maintain consistency between the Access Security Gateway Key and the secret key assigned to the Communication Manager login. For more information about ASG, see Using Access Security Gateway (ASG).

Before you can log into the system with ASG authentication, you need an Access Security Gateway Key, and you need to know your personal identification number (ASG). The Access Security Gateway Key must be pre-programmed with the same secret key (such as, ASG Key, ASG Passkey, or ASG Mobile) assigned to the Avaya Communication Manager login.

Verify that the **Access Security Gateway (ASG)** field on the System-Parameters Customer Options (Optional Features) screen is set to y. If not, contact your Avaya representative.

## Logging in with ASG

---

1. Enter your login ID.  
The system displays the challenge number (for example, 555-1234) and system Product ID number (for example, 1000000000). The Product ID provides Avaya Services with the specific identifier of your Avaya MultiVantage communications application.
2. Press **ON** to turn on your Access Security Gateway Key.
3. Type your PIN.
4. Press **ON**.  
The Access Security Gateway Key displays an 8 digits challenge prompt.
5. At the challenge prompt on the Access Security Gateway Key, type the challenge number without the "-" character (for example, 5551234) from your screen.
6. Press **ON**.  
The Access Security Gateway Key displays a response number (for example, 999-1234).
7. At the response prompt on your terminal, type the ASG response number without the "-" character (for example, 9991234).
8. Press `Enter`.  
The Command prompt displays.

 **Note:**

If you make 3 invalid login attempts, the system terminates the session. For more information, see the appropriate maintenance book for your system.

---

## Login messages

Two messages may be displayed to users at the time of login.

- The `Issue of the Day` message appears prior to a successful login. In general, use the `Issue of the Day` to display warnings to users about unauthorized access. The client that is used to access the system can affect when, how, and if the user sees the `Issue of the Day` message.
- The `Message of the Day (MOTD)` appears immediately after a user has successfully logged in. In general, use the `Message of the Day` to inform legitimate users about information such as upcoming outages and impending disk-full conditions.

### Using the system default Issue of the Day

The Communication Manager file `/etc/issue.avaya` contains sample text that may be used for the `Issue of the Day` message.

- 
1. Log into the Communication Manager server.
  2. At the CLI enter the following commands:
    - `cp /etc/issue.avaya /etc/issue`
    - `cp /etc/issue.avaya /etc/issue.net`
- 

### Setting Issue of the Day and Message of the Day

For more detailed information on setting login messages and interaction with individual access services, see the *Communication Manager Administrator Logins* White Paper on <http://support.avaya.com>.

In general, to administer the Issue of the Day and the Message of the Day, use `/bin/vi` or `/usr/share/emacs` to perform the following edits:

1. Configure `etc/pam.d/mv-auth` to include issue PAM module.
2. Edit `/etc/issue` and `/etc/issue.net` (if using telnet) to include the text for the Issue of the Day.
3. Edit `etc/motd` to include the text for the Message of the Day.

The following strings is not permitted in a Message of the Day (case sensitive). When searching for strings, white space and case are ignored.

- `[513]` used by FPM, CMSA, VAM
- `513]` used by connect2
- `]` used by MSA
- `Software Version` used by ASA
- `Login:`
- `Password:`
- `Challenge:`
- `ogin`
- `ogin:`
- `incorrect login`
- `assword`
- `hallenge`
- `SAT`
- `SAT` cannot be executed on a standby server

## Logging off the System

For security, log off any time you leave your terminal. If you use terminal emulation software to administer Communication Manager, log off the system and exit the emulation application before switching to another software package.

### Logging off the System-Instructions

---

1. Type `logoff`.

2. Press `Enter`.

If the Facility Test Call or Remote Access features are administered, **Alarm origination** is disabled, or if you have busied out resources or active minor or major alarms, a security screen displays. You might want to take appropriate action (for example, disable these features or address any alarms) before you log off.

If none of the above special circumstances exist, the system logs you off.

3. At the **Proceed with Logoff** prompt, type `y` to log off.

If you log off with alarm origination disabled and the system generates an alarm, Avaya support services will not receive any notification of the alarm. For more information about alarms, see the maintenance book for your system.

---

## Administering User Profiles and Logins

Authentication, Authorization and Accounting (AAA) Services allows you to store and maintain administrator account (login) information on a central server. Login authentication and access authorization is administered on the central server.

For details on administering user profiles and logins, see AAA Services in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, and *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

## Establishing Daylight Savings Rules

Avaya Communication Manager allows you to set the daylight savings time rules so that features, such as time-of-day routing and call detail recording (CDR), adjust automatically to daylight savings time. The correct date and time ensure that CDR records are correct. You can set daylight savings time rules to transition to and from daylight savings time outside of normal business hours, so the number of affected CDR records is small.

You can set up 15 customized daylight savings time rules. This allows Communication Manager administrators with servers in several different time zones to set up a rule for each.

A daylight savings time rule specifies the exact time when you want to transition to and from daylight savings time. It also specifies the increment at which to transition (for example, 1 hour).

## Establishing Daylight Savings Rules - Instructions

---

1. Type `change daylight-savings-rules`.
2. Press `Enter`.

Rule 1 applies to all time zones in the U.S. and begins on the first Sunday on or after March 8 at 2:00 a.m. with a 01:00 increment. Daylight Savings Time stops on the first Sunday on or after November 1 at 2:00 a.m., also with a 01:00 increment (used as a decrement when switching back to Standard time. This is the default.

The increment is added to standard time at the specified start time and the clock time shifts by that increment (for example, for 01:59:00 to 01:59:59 the clock time shows 01:59 and at 02:00 the clock shows 03:00).

On the stop date, the increment is subtracted from the specified stop time (for example, for 01:59:00 to 01:59:59 the clock time shows 01:59 and at 02:00 the clock shows 01:00).

### **Note:**

You cannot delete a daylight savings rule if it is in use on either the Locations or Date and Time screens. However, you can change any rule except rule 0 (zero).

The Daylight Savings Rules screen appears.

3. To add a Daylight Savings Time rule, complete the **Start** and **Stop** fields with the day, month, date, and time you want the system clock to transition to Daylight Savings Time and back to standard time.
4. Press `Enter` to save your changes.

### **Note:**

Whenever you change the time of day, the time zone, or daylight savings rules, you must reboot the server for the changes to take effect. See the documentation for your system for information on rebooting the server.

---

## Displaying daylight savings time rules

---

1. Type `display daylight-savings-rules`.
  2. Press **Enter**.  
The Daylight Savings Rules screen appears. Verify the information you entered is correct.
-

## Setting Time of Day Clock Synchronization

Time of Day Clock Synchronization enables a server to synchronize its internal clock to UTC time provided by Internet time servers. Avaya uses the LINUX platform system clock connected to an Internet time server to provide time synchronization. The interface for these systems is web-based.

## Setting the system date and time

The system date and time is entered through System Platform. For information on how to set up the date and time, see the Configuring date and time section.

### Related topics:

[Configuring date and time](#)

## Displaying the system date and time

- 
1. Type `display time`.
  2. Press `Enter`.  
The Date and Time screen displays. Verify the information you entered is correct.
- 

### Related topics

See Establishing Daylight Savings Rules for more information about setting system time.

For additional information, see *Avaya Call Center Release 4.0 Automatic Call Distribution (ACD) Guide, 07-600779*.

## Using the Bulletin Board

Avaya Communication Manager allows you to post information to a bulletin board. You can also display and print messages from other Avaya server administrators and Avaya personnel using the bulletin board. Anyone with the appropriate permissions can use the bulletin board for messages. Only one user can post or change a message at a time.

Whenever you log in, the system alerts you if you have any messages on the bulletin board and the date of the latest message. Also, if Avaya personnel post high-priority messages while you are logged in, you receive notification the next time you enter a command. This notification disappears after you enter another command and reoccurs at login until deleted by Avaya personnel.

You maintain the bulletin board by deleting messages you have already read. You cannot delete high-priority messages. If the bulletin board is at 80% or more capacity, a message

appears at login indicating how much of its capacity is currently used (for example, 84%). If the bulletin board reaches maximum capacity, new messages overwrite the oldest messages.

 **Note:**

The bulletin board does not lose information during a system reset at level 1. If you save translations, the information can be restored if a system reset occurs at levels 3, 4, or 5.

## Displaying messages

---

1. Type `display bulletin-board`.
  2. Press `Enter`.  
The Bulletin Board screen displays.
- 

## Posting a message

In our example, we post a message to the bulletin board about a problem with a new trunk group, and an Avaya representative replies to our message.

- 
1. Type `change bulletin-board`.
  2. Press `Enter`.  
The Bulletin Board screen displays.

There are three pages of message space within the bulletin board. The first page has 19 lines, but you can only enter text on lines 11-19. The first 10 lines on page 1 are for high-priority messages from Avaya personnel and are noted with an asterisk (\*). The second and third pages each have 20 lines, and you can enter text on any line. The system automatically enters the date the message was posted or last changed to the right of each message line.

3. Type your message.  
You can enter up to 40 characters of text per line. You also can enter one blank line. If you enter more than one blank line, the system consolidates them and displays only one. The system also deletes any blank line if it is line one of any page. You cannot indent text on the bulletin board. The **Tab** key moves the cursor to the next line.
  4. Press `Enter` to save your changes.
- 

## Deleting messages

---

1. Type `change bulletin-board`.
2. Press `Enter`.

The Bulletin Board screen appears.

3. Enter a space as the first character on each line of the message you want to delete.
  4. Press `Enter`.
  5. Press `Enter` to save your changes.
- 

## Save translations

Use `save translation` to commit the active server translations (volatile) in memory to a file (non-volatile). It either completes or fails. For Linux platforms, the translation file is copied to the standby server by a `filesync` process.

All translation data is kept in volatile system memory or on the hard drive during normal operation. In the event of a power outage or certain system failures, data in memory is lost. `save translation` stores on disk the translation data currently in memory.

When a SAT user issues `save translation` on a duplicated system, translations are saved on both the active and standby servers. If an update of the standby server is already in progress, subsequent `save translation` commands fail with the message `save translations has a command conflict`.

`save translation` will not run and an error message appears when:

- translation data is being changed by an administration command.
- translations are locked by use of the Communication Manager Web interface Pre-Upgrade Step.

Run `save translation` as part of scheduled background maintenance or on demand.

For information on the `save translation` command and the command syntax descriptions, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

## Perform Backups

Information on performing backups to your system can be found in the *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300432.

---

## System Planning

Communication Manager consists of hardware to perform call processing, and the software to make it run. You use the administration interface to let the system know what hardware you have, where it is located, and what you want the software to do with it. You can find out which

circuit packs are in the system and which ports are available by entering the command `list configuration all`. There are variations on this command that display different types of configuration information. Use the help function to experiment, and see which command works for you.

## System Configuration

### Planning Your System

The System Configuration screen shows all the boards on your system that are available for connecting telephones. You can see the board number, board type, circuit-pack type, and status.

At a very basic level, Communication Manager consists of hardware to perform call processing, and the software to make it run. You use the administration interface to let the system know what hardware you have, where it is located, and what you want the software to do with it.

You can find out which circuit packs are in the system and which ports are available by entering the command `list configuration all`. There are variations on this command that display different types of configuration information. Use the help function to experiment, and see which command works for you.

To view a list of port boards on your system: Type `list configuration port-network`. Press `Enter`.

The System Configuration screen shows all the boards on your system that are available for connecting telephones, trunks, data modules and other equipment. You can see the board number, board type, circuit-pack type, and status of each board's ports. The `u` entries on this screen indicate unused ports that are available for you to administer. These might also appear as `p` or `t`, depending on settings in your system.

You will find many places in the administration interface where you are asked to enter a port or slot. The port or slot is actually an address that describes the physical location of the equipment you are using. A port address is made up of four parts:

- cabinet** the main housing for all the server equipment. Cabinets are numbered starting with 01.
- carrier** the rack within the cabinet that holds a row of circuit packs. Each carrier within a cabinet has a letter, A to E.
- slot** the space in the carrier that holds an individual circuit pack. Slots are numbered 01-16.
- port** the wire that is connected to an individual piece of equipment (such as a telephone or data module). The number of ports on a circuit pack varies depending on the type.

So, if you have a single-carrier cabinet, the circuit pack in slot 06 would have the address 01A06. If you want to attach a telephone to the 3rd port on this board, the port address is 01A0603 (01=cabinet, A=carrier, 06=slot, 03=port).

## Viewing a list of port boards

- 
1. Go to the administration interface.
  2. Enter `list configuration port-network`.

The System Configuration screen shows all the boards on your system that are available for connecting telephones, trunks, data modules and other equipment. You can see the board number, board type, circuit-pack type, and status of each board's ports. The u entries on this screen indicate unused ports that are available for you to administer. These entries might also appear as p or t, depending on settings in your system.

---

## Understanding equipment addressing

### Where addressing is used

You will find many places in the administration interface where you are asked to enter a port or slot. The port or slot is actually an address that describes the physical location of the equipment you are using.

### Address format

A port address is made up of four parts:

- cabinet — the main housing for all the server equipment. Cabinets are numbered starting with 01.
- carrier — the rack within the cabinet that holds a row of circuit packs. Each carrier within a cabinet has a letter, A to E.
- slot — the space in the carrier that holds an individual circuit pack. Slots are numbered 01-16.
- port — the wire that is connected to an individual piece of equipment (such as a telephone or data module). The number of ports on a circuit pack varies depending on the type.

### Example

So, if you have a single-carrier cabinet, the circuit pack in slot 06 would have the address 01A06. If you want to attach a telephone to the 3rd port on this board, the port address is 01A0603 (01=cabinet, A=carrier, 06=slot, 03=port).

## Dial plan

### Understanding the Dial Plan

#### What the dial plan does

Your dial plan tells your system how to interpret dialed digits. For example, if you dial 9 on your system to access an outside line, it is actually the dial plan that tells the system to find an external trunk when a dialed string begins with a 9.

The dial plan also tells the system how many digits to expect for certain calls. For example, the dial plan might indicate that all internal extensions are 4-digit numbers that start with 1 or 2. Let us take a look at an example dial plan so you'll know how to read your system's dial plan.

#### Dial plan access table

The Dial Plan Analysis Table defines the dialing plan for your system. The Call Type column in the Dial Plan Analysis Table indicates what the system does when a user dials the digit or digits indicated in the Dialed String column. The Total Length column indicates how long the dialed string will be for each type of call.

#### Dial plan parameters table

The Dial Plan Analysis Table works with the Dial Plan Parameters Table for fully defining your dial plan. The Dial Plan Parameters Table allows you to set system-wide parameters for your dial plan, or to define a Dial Plan Parameters Table per-location.

#### Uniform dial plan

To Administer a Uniform Dial Plan, you can set up a Uniform Dialing Plan that can be shared among a group of servers. For more information, see *Avaya Aura™ Communication Manager Feature Description and Implementation, 555-245-205*.

### Displaying your dial plan

- 
1. Go to the administration interface.
  2. Enter `display dialplan analysis` or `display dialplan analysis location n`, where `n` represents the number of a specific location.
  3. Press `Enter` to save your changes.
- 

### Modifying your dial plan

- 
1. Go to the administration interface.
  2. Enter `change dialplan analysis` or `display dialplan analysis location n` where `n` represents the number of a specific location. Press `Enter`.
  3. Move the cursor to an empty row.
  4. Type `7` in the **Dialed String** column. Press `Tab` to move to the next field.

5. Type 3 in the **Total Length** column. Press `Tab` to move to the next field.
6. Type `dac` in the **Call Type** column.
7. Press `Enter` to save your changes.

---

## Adding Extension Ranges

You might find that as your needs grow you want a new set of extensions. Before you can assign a station to an extension, the extension must belong to a range that is defined in the dial plan.

In this example, we will add a new set of extensions that start with 3 and are 4 digits long (3000 to 3999).

- 
1. Go to the administration interface.
  2. Enter `change dialplan analysis` or `change dialplan analysis location n`, where `n` represents the number of a specific location. Press `Enter`.
  3. Move the cursor to an empty row.
  4. Type 3 in the **Dialed String** column. Press `Tab` to move to the next field.
  5. Type 4 in the **Total Length** column. Press `Tab` to move to the next field.
  6. Type `ext` in the **Call Type** column.
  7. Press `Enter` to save your changes.

---

## Multi-location dial plan

### Definition

When a customer migrates from a multiple independent node network to a single distributed server whose gateways are distributed across a data network, it might initially appear as if some dial plan functions are no longer available.

The multi-location dial plan feature preserves dial plan uniqueness for extensions and attendants that were provided in a multiple independent node network, but appear to be unavailable when customers migrate to a single distributed server. This feature is available beginning with Communication Manager, release 2.0.

### Example

For example, in a department store with many locations, each location might have had its own switch with a multiple independent node network. The same extension could be used to represent a unique department in all stores (extension 123 might be the luggage department). If the customer migrates to a single distributed server, a user could no longer dial 123 to get the luggage department in their store.

The user would have to dial the complete extension to connect to the proper department. Instead of having to dial a complete extension, the multi-location dial plan feature allows a

user to dial a shorter version of the extension. For example, a customer can continue to dial 123 instead of having to dial 222-123.

Communication Manager takes leading digits of the location prefix and adds some or all of its leading digits (specified on the Uniform Dial Plan screen) to the front of the dialed number. The switch then analyzes the entire dialed string and routes the call based on the administration on the Dial Plan Parameters and Dial Plan Analysis screens.

 **Note:**

Before you can administer the multi-location dial plan feature, the **Multiple Locations** field on the System Parameters Customer-Options (Optional Features) screen must be enabled. To check if this is enabled, use the `display system-parameters customer-options` command. The **Multiple Locations** field is on page 3 of the Optional Features screen. Set this field to `y`.

## Location numbers

### How equipment gets location numbers

Equipment gets location numbers as follows:

- IP telephones indirectly obtain their location number. A location number is administered on the IP Network Region screen that applies to all telephones in that IP region.
- Non-IP telephones and trunks inherit the location number of the hardware they are connected to (for example, the cabinet, remote office, or media gateway).
- IP trunks obtain their location from the location of its associated signaling group. Either direct administration (only possible for signaling groups for remote offices), or the ways described for IP telephones, determines the location.

### Location administration

A location number is administered on the IP Network Region screen that applies to all telephones in that IP region. If a Location field is left blank on an IP Network Region screen, an IP telephone derives its location from the cabinet where the CLAN board is that the telephone registered

## Prepending the location prefix to dialed numbers

Complete the following steps to assign the location prefix from the caller's location on the Locations screen.

- 
1. Go to the administration interface.
  2. Enter `change uniform-dialplan`.
  3. Enter the prefix in the in the **Insert Digits** field.
  4. Press `Enter` to save your changes.

The system adds some or all of its leading digits (specified on the Uniform Dial Plan screen) to the front of the dialed number. The switch then analyzes the entire dialed string and routes the call based on the administration on the Dial Plan Parameters screen.

 **Note:**

- Non-IP telephones and trunks inherit the location number of the hardware they are connected to (for example, the cabinet, remote office, or media gateway).
- IP telephones indirectly obtain their location number.
  - A location number is administered on the IP Network Region screen that applies to all telephones in that IP region.
  - If a **Location** field is left blank on an IP Network Region screen, an IP telephone derives its location from the cabinet where the CLAN board is that the telephone registered through.
- IP trunks obtain their location from the location of its associated signaling group. Either direct administration (only possible for signaling groups for remote offices), or the ways described for IP telephones, determines the location.

---

### Other options for the dial plan

You can establish a dial plan so that users only need to dial one digit to reach another extension. You can also establish a dial plan that allows users to dial, for example, two digits to reach one extension, and three digits to reach another. This is particularly useful in the hospitality industry, where you want users to be able to simply dial a room number to reach another guest.

If you have Communication Manager 5.0 or later, you can administer dial plans per-location. To access a per-location screen, type change dialplan analysis location n, where n represents the number of a specific location. For details on command options, see online help, or *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

### Feature access codes

Feature access codes (FAC) allow users to activate and deactivate features from their telephones. A user who knows the FAC for a feature does not need a programmed button to use the feature. For example, if you tell your users that the FAC for the Last Number Dialed is \*33, then users can redial a telephone number by entering the FAC, rather than requiring a Last Number Dialed button. Many features already have factory-set feature access codes. You can use these default codes or you can change them to codes that make more sense to you. However, every FAC must conform to your dial plan and must be unique.

### Adding feature access codes

As your needs change, you might want to add a new set of FAC for your system. Before you can assign a FAC on the **Feature Access Code** screen, it must conform to your dial plan.

In our example, if you want to assign a feature access code of 33 to **Last Number Dialed**, first you need to add a new FAC range to the dial plan.

Complete the following steps to add a FAC range from 30 to 39.

- 
1. Go to the administration interface.
  2. Enter `change dialplan analysis` or `change dialplan analysis location n`, where `n` represents the number of a specific location. Press `Enter`. The Dial Plan Analysis screen appears.
  3. Move the cursor to an empty row.
  4. Type `3` in the **Dialed String** column and then tab to the next field.
  5. Type `2` in the **Total Length** column and then tab to the next field.
  6. Type `fac` in the **Call Type** column.
  7. Press `Enter` to save your changes.
- 

### Changing feature access codes

If you try to enter a code that is assigned to a feature, the system warns you of the duplicate code and does not allow you to proceed until you change one of them.



#### Tip:

To remove a feature access code, delete the existing FAC and leave the field blank.

Let us try an example. If you want to change the feature access code for Call Park to `*72` do the following.

- 
1. Go to the administration interface.
  2. Enter `change feature-access-codes`. Press `Enter`. The Feature Access Code(FAC) screen appears.
  3. Move the cursor to the **Call Park Access Code** field.
  4. Type `*72` in the **access code** field over the old code.
  5. Press `Enter` to save your changes.
- 

### Administering Dial Plan Transparency (DPT)

The Dial Plan Transparency (DPT) feature preserves users' dialing patterns when a media gateway registers with a Survivable Remote Server (Local Survivable Processor), or when a Port Network requests service from a Survivable Core Server (Enterprise Survivable Server). Note that this feature does not provide alternate routing for calls made between Port Networks connected through networks other than IP (for example, ATM or DS1C), and that register to different Survivable Core Servers during a network outage.

Administration of Dial Plan Transparency (DPT) is similar to setting up Inter-Gateway Alternate Routing (IGAR). You must first enable the DPT feature, then set up Network Regions and trunk resources for handling the DPT calls. For Survivable Core Servers, you must also assign Port

Networks to communities. The following table show the screens and field used in setting up Dial Plan Transparency:

| Screen Name                       | Purpose   | Fields   |
|-----------------------------------|---|--|
| Feature-Related System Parameters | <ul style="list-style-type: none"> <li>• Enable the DPT feature for your system.</li> <li>• Indicate the Class of Restriction to use for the Dial Plan Transparency feature.</li> </ul> | <ul style="list-style-type: none"> <li>• Enable Dial Plan Transparency in Survivable Mode</li> <li>• COR to use for DPT</li> </ul> |
| IP Network Region                 | Administer the DPT feature for Network Regions.   | <ul style="list-style-type: none"> <li>• Incoming LDN Extension</li> <li>• Dial Plan Transparency in Survivable Mode</li> </ul>    |
| System Parameters-ESS             | Enter the community assignments for each Port Network.  | Community  |

For more information on the Dial Plan Transparency feature, see *Dial Plan Transparency in Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

## Controlling the features your users can access

Class of service and class of restriction give you great flexibility with what you allow users to do. If you are in doubt about the potential security risks associated with a particular permission, contact your Avaya technical support representative.

### Features and functions

Communication Manager offers a wide range of features and functions. Some of these you can administer differently from one user to the next. For example, you can give one user a certain set of telephone buttons, and the next user a completely different set, depending on what each person needs to get his/her job done. You decide on these things as you administer the telephones for these individuals.

### Class of service

Often, groups of users need access to the same sets of Communication Manager features. You can establish several classes of service (COS) definitions that are collections of feature access permissions. Now, a user's telephone set can be granted a set of feature permissions by simply assigning it a COS.

### Class of restriction

Class of restriction (COR) is another mechanism for assigning collections of capabilities. COR and COS do not overlap in the access or restrictions they control.

## System-wide settings

There are some settings that you enable or disable for the entire system, and these settings effect every user. You might want to look over the various System Parameters screens and decide which settings best meet the needs of your users.

To see a list of the different types of parameters that control your system, type `display system-parameters`. Press **Help**. You can change some of these parameters yourself. Type `change system-parameters`. Press **Help** to see which types of parameters you can change. In some cases, an Avaya technical support representative is the only person who can make changes, such as to the System-Parameters Customer-Options screen.

Type `list usage` to see all the instances of an object, such as an extension or IP address, in your system. This is useful when you attempt to change administration and receive an “in use” error. See *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431, for more information.

## Changing system parameters

You can modify the system parameters that are associated with some of the system features. For example, you can use the system parameters to allow music to play if callers are on hold or to allow trunk-to-trunk transfers on the system.

Generally, Avaya sets your system parameters when your system is installed. However, you can change these parameters as your organization’s needs change.

For example, let us say that you are told that the number of rings between each point for new coverage paths should change from 4 to 2 rings. Complete the following steps to change the number of rings.

- 
1. Go to the administration interface.
  2. Enter `change system-parameters coverage/forwarding`. Press `Enter`.
  3. The System Parameters Call Coverage/Call Forwarding screen appears.
  4. In the **Local Coverage Subsequent Redirection/CFWD No Answer Interval** field, type `2`.
  5. Press `Enter` to save your changes.

Each telephone in a Call Coverage path now rings twice before the call routes to the next coverage point. The Local Cvg Subsequent Redirection/CFWD No Ans Interval field also controls the number of rings before the call is forwarded when you use Call Forwarding for busy/don’t answer calls. This applies only to calls covered or

forwarded to local extensions. Use Off-Net to set the number of rings for calls forwarded to public network extensions.

## WAN Bandwidth Limits between Network Regions

### Bandwidth limits

Using the Communication Manager Call Admission Control: Bandwidth Limitation (CAC-BL) feature, you can specify a VOIP bandwidth limit between any pair of IP network regions, and then deny calls that need to be carried over the WAN link that exceed that bandwidth limit.

Bandwidth limits can be administered in terms of:

- Kbit/sec WAN facilities
- Mbit/sec WAN facilities
- Explicit number of connections
- No limit

### Considerations for WAN bandwidth administration

#### Collect design information

It is highly recommended that you have the following design information before setting the bandwidth limits and mapping the connections:

- Network topology and WAN link infrastructure.
- An understanding of the Committed Information Rate (CIR) for the WAN infrastructure.
- Overlay/design of the Network Regions mapped to the existing topology.
- Codec sets administered in the system.
- Bandwidth is assumed to be full duplex.

#### Typical bandwidth usage

The following table can be used to help assess how much bandwidth (in Kbits/sec) is used for various types of codecs and packet sizes. The values shown assume a 7 byte L2 WAN header (and are rounded up).

| Packet Size | 10 ms | 20 ms | 30 ms | 40 ms | 50 ms | 20 ms <sup>6</sup> |
|-------------|-------|-------|-------|-------|-------|--------------------|
| G.711       | 102   | 83    | 77    | 74    | 72    | 71                 |
| G.729       | 46    | 27    | 21    | 18    | 16    | 15                 |
| G.723-6.3   | NA    | NA    | 19    | NA    | NA    | 13                 |
| G.723-5.3   | NA    | NA    | 18    | NA    | NA    | 12                 |

These values, when compared to the actual bandwidth used for 8 byte as well as 10 byte L2 WAN headers are not significantly different. In some cases, the rounded up values shown above are greater than values used for 10 bytes.

The bandwidth usage numbers shown above assume 6 bytes for Multilink Point-to-Point Protocol (MP) or Frame Relay Forum (FRF), 12 Layer 2 (L2) header, and 1 byte for the end-of-frame flag on MP and Frame Relay frames for a total of 7 byte headers only. They do not account for silence suppression or header compression techniques, which might reduce the actual bandwidth. For other types of networks (such as Ethernet or ATM) or for cases where there is a lot of silence suppression or header compression being used, the network might be better modeled by administering the CAC-BL limits in terms of number of connections rather than bandwidth used.

### Setting bandwidth limits between directly-connected network regions

- 
1. Enter **change ip-network region <n>**, where n is the region number you want to administer.
  2. Scroll to page 3 of the IP Network Region screen which is titled Inter Network Region Connection Management.
  3. In the **codec-set** field, enter the number (1-7) of the codec set to be used between the two regions.
  4. In the **Direct WAN** field, enter *y*.
  5. In the **WAN-BW-limits** field, enter the number and unit of measure (Calls, Kbits, Mbits, No Limit) that you want to use for bandwidth limitation.
  6. Press **Enter** to save your changes.
- 

### Administering Treatment for Denied or Invalid Calls

You can administer your system to reroute denied or invalid calls to an announcement, the attendant, or to another extension.

In this example, we want:

- all outward restricted call attempts to route to an announcement at extension 2040
- all incoming calls that are denied to route to the attendant
- all invalid dialed numbers to route to an announcement at extension 2045

- 
1. Enter **change system-parameters features**.  
The Feature-Related System Parameters screen appears.
  2. In the **Controlled Outward Restriction Intercept Treatment** field, type *announcement*.  
Another blank field appears.

3. In this blank field, type 2040.  
This is the extension of an announcement you recorded earlier.
  4. In the **DID/Tie/ISDN Intercept Treatment** field, type attd.  
This allows the attendant to handle incoming calls that have been denied.
  5. In the **Invalid Number Dialed Intercept** field, type announcement.  
Another blank field appears.
  6. In this blank field, type 2045.  
This is the extension of an announcement you recorded earlier.
  7. Press `Enter` to save your changes.
- 

## Music-on-hold

### Description

Music-on-Hold automatically provides music to a caller placed on hold. Music lets the caller know that the connection is still active. The system does not provide music to callers in a multiple-party connection who are in queue, on hold, or parked.

For more information on locally-sourced Music-on-Hold, see the Locally Sourced Announcements and Music feature in the *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

### Locally sourced announcements and music

The Locally Sourced Announcements and Music feature is based on the concept of audio source groups. This feature allows announcement and music sources to be located on any or all of the Voice Announcement with LAN (VAL) boards or on virtual VALs (vVAL) in a media gateway. The VAL or vVAL boards are assigned to an audio group. The audio group is then assigned to an announcement or audio extension as a group sourced location. When an incoming call requires an announcement or Music-on-Hold, the audio source that is closest to the incoming call trunk plays.

Storing audio locally minimizes audio distortion because the audio is located within the same port network or gateway as the caller. Therefore, this feature improves the quality of announcements and music on hold. This feature also reduces resource usage, such as VoIP resources, because the nearest available audio source of an announcement or music is played. Locally Sourced Announcements and Music also provides a backup for audio sources because multiple copies of the audio files are stored in multiple locations. Audio sources are assigned either to an audio group or a Music-on-Hold group.

### Audio groups

An audio group is a collection of identical announcement or music recordings stored on one or more VAL or vVAL boards. The audio group can contain announcements and music. The nearest recording to a call plays for that call.

### Music-on-hold groups

A Music-on-Hold (MOH) group is a collection of externally connected and continuously playing identical music sources. An example of a Music-on-Hold source is a radio station connected

to a media gateway using an analog station port. Multiple Music-on-Hold sources can be used in the same system. Like the audio group, the nearest music source to a call plays for that call.

### Music-on-hold sources

As with the Music-on-Hold feature, only one music source is defined for a system or for a tenant partition. However, you can define a music source as a group of Music-on-Hold sources.

Therefore, both non-tenant and tenant systems can use the group concept to distribute Music-on-Hold sources throughout a system.

### Adding an audio group

- 
1. Enter **add audio-group n**, where n is the group number you want to assign to this audio group, or next to assign the next available audio group number in the system.  
The system displays the Audio Group screen.
  2. In the **Group Name** field, type an identifier name for the group.
  3. In the **Audio Source Location** fields, type in the VAL boards or vVAL location designators for each audio source in the audio group.
  4. Press **Enter** to save your changes.

### Adding a Music-on-Hold group

- 
1. Enter **add moh-analog-group n**, where n is the Music-on-Hold group number.  
The system displays the MOH Group screen.
  2. In the **Group Name** field, type in an identifier name for the Music-on-Hold group.
  3. In the **MOH Source Location numbered** fields, type in the Music-on-Hold VAL or vVAL source locations.
  4. Press **Enter** to save your changes.

### Setting music-on-hold system parameters

You must administer the Music-on-Hold (MOH) feature at the system level to allow local callers and incoming trunk callers to hear music while on hold.

#### Note:

If your system uses Tenant Partitioning, follow the instructions in Providing music-on-hold service for multiple tenants instead of the instructions below.

- 
1. Enter **change system-parameters features**.

The Feature-Related System Parameters screen appears.

2. In the Music/Tone On Hold field, type `music`.  
The Type field appears.
3. In the **Type** field, enter the type of music source you want to utilize for MOH: an extension (`ext`), an audio group (`group`), or a port on a circuit pack (`port`).
4. In the text field that appears to the right of your **Type** selection, type the extension number, the audio group, or the port address of the music source.
5. In the **Music (or Silence) on Transferred Trunk Calls** field, type `all`.
6. Press `Enter` to save your changes.
7. Now administer a class of restriction with **Hear System Music on Hold** set to `y` to allow your local users to hear Music-on-Hold.

---

## Providing music-on-hold service for multiple tenants

### Prerequisites

Before you can administer tenants in your system, **Tenant Partitioning** must be set to `y` on the System-Parameters Customer-Options screen. This setting is controlled by your license file.

---

If you manage the switching system for an entire office building, you might need to provide individualized telephone service for each of the firms who are tenants. You can set up your system so that each tenant can have its own attendant, and can choose to have music or play special announcements while callers are on hold.

The following example illustrates how to administer the system to allow one tenant to play Country music for callers on hold, and another to play Classical music.

- 
1. Enter **change music-sources**.
  2. For Source No 1, enter `music` in the **Type** column.  
A **Type** field appears under the **Source** column.
  3. In the **Type** field, enter `port`.  
A blank text field appears.
  4. Enter the port number, `01A1001` in this case, in the text field.
  5. In the **description** field, enter `Country`.
  6. Move to Source 3, and enter `music` in the **Type** column, `port` in the **Type** field, `01A1003` for the port number, and `Classical` for the **Description**.
  7. Press `Enter` to save your changes.
  8. Enter **change tenant 1**.  
The Tenant screen appears.

9. In the **Tenant Description** field, type `Dentist`.  
This identifies the client in this partition.
10. In the **Attendant Group** field, type the attendant group number.

 **Note:**

The attendant group number must also appear in the **Group** field of the Attendant Console screen for this tenant.

11. In the **Music Source** field, type `1`.  
Callers to this tenant will now hear country music while on hold.
  12. Press `Enter` to save your changes.
  13. To administer the next partition, enter `change tenant 2`.
  14. Administer this tenant, Insurance Agent, to use Attendant Group 2 and Music Source 3. Be sure to change the Attendant Console screen so that this attendant is in group 2. This tenant's callers will hear classical music on hold.
- 

## Receiving Notification in an Emergency

If one of your users calls an emergency service such as the police or ambulance, someone, perhaps the receptionist, security or the front desk, needs to know who made the call. Thus, when the emergency personnel arrive, they can be directed to the right place. You can set up Communication Manager to alert the attendant and up to ten other extensions whenever an end-user dials an emergency number. The display on the notified user's telephone shows the name and number of the person who placed the emergency call. The telephones also ring with a siren-type alarm, which users must acknowledge to cancel.

 **Note:**

You must decide if you want one user to be able to acknowledge an alert, or if all users must respond before an alert is cancelled. Verify that the **ARS** field is **y** on the System Parameters Customer-Options (Optional Features) screen.

Also, make sure that the extensions you notify belong to physical digital display telephones. Refer to Telephone Reference on page 653 for a list of telephone types. When you assign crisis alert buttons to the telephones, check the Type field on the Station screen to be sure you are not using a virtual extension.

In this example, we will set up the system to notify the attendant and the security guards at all 3 entrances when someone dials the emergency number 5555. All three guards must acknowledge the alert before it is silent.

- 
1. Type `change ars analysis n`. Press `Enter`. The ARS Digit Analysis Table screen appears.
  2. In the **Dialed String** field, type `5555`.  
This is the number that end-users dial to reach emergency services.
  3. In the **Total Min** and **Max** fields, type `4`.  
In this example, the user must dial all 4 digits for the call to be treated as an emergency call.
  4. In the **Route Pattern** field, type `1`.  
In this example, we use route pattern 1 for local calls.
  5. In the **Call Type** field, type `alrt`.  
This identifies the dialed string `5555` as one that activates emergency notification.
  6. Press `Enter` to save your changes. Now set up the attendant console to receive emergency notification.
  7. Type `change attendant 1`. Press `Enter`.  
The Attendant Console screen appears.
  8. In the feature button area, assign a **crss-alert** button.
  9. Press `Enter` to save your changes.
  10. Assign a **crss-alert** button to each security guard's telephone.  
You cannot assign this button to a soft key.  
Finally, we make sure that all security personnel and the attendant will have to acknowledge the alert.
  11. Type `change system-parameters crisis-alert`. Press `Enter`.  
The Crisis Alert System Parameters screen appears.
  12. Go to the **Every User Responds** field and type `y`.
  13. Press `Enter` to save your changes.
- 

## Notifying a Digital Pager of an Emergency

You have the option of having your emergency calls go to a digital pager. When someone dials an emergency number (for example, 911), the system sends the extension and location (that originated the emergency call) to the administered pager.

### Prerequisites

Before you start,

- You need to administer a **crss-alert** button on at least one of the following.
  - Attendant Console (use the **change attendant** command)
  - Digital telephone set (use the **change station** command)
- The **ARS Digit Analysis** Table must have emergency numbers in the **Call Type** column set to **alrt** (crisis alert).
- You need a digital numeric pager.

- 
1. Type `change system-parameters crisis-alert`. Press `Enter`.  
The Crisis Alert System Parameters screen appears.
  2. In the **Alert Pager** field, type `y`.  
This allows you to use the Crisis Alert to a Digital Pager feature and causes additional crisis alert administration fields to appear.
  3. In the **Originating Extension** field, type a valid unused extension to send the crisis alert message. We will type `7768`.
  4. In the **Crisis Alert Code** field, type `911`.  
This is the number used to call the crisis alert pager.
  5. In the **Retries** field, type `5`.  
This is the number of additional times the system tries to send out the alert message in case of an unsuccessful attempt.
  6. In the **Retry Interval (sec)** field, type `30`.  
This is length of time between retries.
  7. In the **Main Number** field, type the number that is to be displayed at the end of the pager message. We will type `303-555-0800`.
  8. In the **Pager Number** field, type the number for the pager. We'll type `303-555-9001`.
  9. In the **Pin Number** field, type `pp77614567890`.  
This is the PIN number, if required, for the pager. Insert any pause digits (pp) as needed to wait for announcements from the pager service to complete before sending the PIN.
  10. In the **DTMF Duration - Tone (msec)** field, type `100`.  
This is the length of time the DTMF tone is heard for each digit.
  11. In the **Pause (msec)** field, type `100`.  
This is the length of time between DTMF tones for each digit.
  12. Press `Enter` to save your changes.

Refer to the Crisis Alert feature in Feature Description and Implementation for Communication Manager, 555-245-205, for more detailed information.

---

## Other Useful Settings

There are many settings that control how your system operates and how your users telephones work. Most of these you administer through one of the System Parameters screens. This section describes a few of the items you can enable in your system to help your users work more efficiently. See Feature-Related System Parameters for a more detailed description of the available system settings.

### **Automatic callback if an extension is busy**

You can allow users to request that the system call them back if they call a user whose telephone is busy. For more information, see the Automatic Callback feature in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

### **Automatic hold**

You can set a system-wide parameter that allows your users to initiate a call on a second line without putting the first call on Hold. This is called Automatic Hold, and you enable it on the Feature-Related System Parameters screen. If you do not turn this on, the active call drops when a the user presses the second line button.

### **Bridging onto a call that has gone to coverage**

You can allow users to join (bridge) on to a call that rang at their extension and then went to coverage before they could answer. For more information, see the Temporary Bridged Appearance feature in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

### **Distinctive ringing**

You can establish different ringing patterns for different types of calls. For example, you can administer your system so that internal calls ring differently from external calls or priority calls. For more information, see the Distinctive Ringing feature in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

### **Warning when telephones are off-hook**

You can administer the system so that if a telephone remains off-hook for a given length of time, Communication Manager sends out a warning. This is particularly useful in hospitals, where the telephone being off-hook might be an indication of trouble with a patient. See “Class of Service” for more information.

### **Warning users if their calls are redirected**

You can warn analog telephone users if they have features active that might redirect calls. For example, if the user has activated send all calls or call forwarding, you can administer the system to play a special dial tone when the user goes off-hook. See Distinctive Ringing in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information.

## Controlling the Calls Your Users Can Make and Receive

The Avaya Communication Manager provides several ways for you to restrict the types of calls your users can make, and the features that they can access.

You use class of restriction (COR) to define the types of calls your users can place and receive. Your system might have only a single COR, a COR with no restrictions, or as many CORs as necessary to effect the desired restrictions.

You will see the **COR** field in many different places throughout Communication Manager when administering telephones, trunks, agent logins, and data modules, to name a few. You must enter a COR on these screens, although you control the level of restriction the COR provides.

### Strategies for assigning CORs

The best strategy is to make it as simple as possible for you and your staff to know which COR to assign when administering your system. You can create a unique COR for each type of user or facility, for example, call center agents, account executives, administrative assistants, Wide Area Telecommunications Service (WATS) trunks, paging zones or data modules.

You can also create a unique COR for each type of restriction, for example, toll restriction, or outward restriction. If you have a number of people who help you administer your system, using this method would also require the additional step of explaining where you wanted to use each type of restriction.

#### Note:

COR-to-COR calling restrictions from a station to a trunk do not apply when Automatic Alternate Routing (AAR), Automatic Route Selection (ARS), or Uniform Dial Plan (UDP) is used to place the call. In these cases, use Facility Restriction Levels to block groups of users from accessing specific trunk groups. See *Class of Restriction and Facility Restriction Levels in Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information.

To find out what CORs are administered in your system already, type `list cor`. You can also display information for a single COR by typing `list cor #`.

### Allowing users to change CORs

You can allow specific users to change their Class of Restriction (COR) from their telephones using a Change COR feature access code. You can also limit this feature by insisting that the user enter a password as well as a feature access code before they can change their COR. The Station Lock feature also allows users to change their own COR.

Insert an optional short description to be used as link preview or summary text. See the `shortdesc` tag help for a more detailed description of appropriate usage of `shortdesc`.

### Prerequisites

Before you start:

- Be sure that **Change COR by FAC** field is set to `y` on the System-Parameters Customer-Options (Optional Features) screen. Note that you cannot have both **Change COR by FAC** and **Tenant Partitioning** enabled.
- Be sure that each user (who you want to allow to change a COR) has a class of service with console permissions.

---

To allow users to change their own class of restriction, you must define a feature access code and can, optionally, create a password. For example, we will create a change COR feature access code of `*55` and a password of `12344321`.

- 
1. Type `change feature-access-codes`. Press `Enter`.  
The Feature Access Code (FAC) screen appears.
  2. Move the cursor to the **Change COR Access Code** field.
  3. Type `*55` in the **access code** field.
  4. Press `Enter` to save your changes.  
Now we have to define the password.
  5. Type `change system-parameters features`. Press `Enter`.  
The Feature-Related System Parameters screen appears.
  6. Press `Next Page` to find the Automatic Exclusion Parameters section.
  7. Move to the **Password to Change COR by FAC** field and enter `12344321`.  
This field determines whether or not Communication Manager requires the user to enter a password when they try to change their COR. Avaya recommends that you require a password.
  8. Press `Enter` to save your changes.

---

## Station Lock

Station Lock provides users with the capability to manually lock their stations, using a button or feature access code, in order to prevent unauthorized external calls from being placed.

Station Lock can prevent unauthorized external calls. Telephones can be remotely locked and unlocked. Station Lock allows users to:

- Change their Class of Restriction (COR); usually the lock COR is set to fewer calling permissions than the station's usual COR
- Lock their telephones to prevent unauthorized outgoing calls.
- Block outgoing calls and still receive incoming calls.
- Block all outgoing calls except for emergency calls.

Station Lock is activated by pressing a telephone button, which lights the button indicator, or by dialing a FAC.

Analog and XMOBILE stations must dial a FAC to activate the feature. The user hears a special dial tone on subsequent origination attempts from the telephone to indicate that the lock feature is active.

Digital stations (including DCP, BRI, IP hardphones and softphones) access Station Lock with a feature button or via a FAC. If a digital station has a Station Lock button but activates the feature with the FAC, the LED for the button lights and no special dial tone is provided. However, if a digital station does not have a Station Lock button and activates the feature with the FAC, a special dial tone is provided.

A station can be locked or unlocked from any other station if the FAC is used and the Station Security Code is known. The attendant console can never be locked but can be used to lock or unlock other stations. A station also can be locked or unlocked via a remote access trunk.

## Interactions

- Attendant Console

Station Lock cannot be used for attendant consoles but it can be assigned to regular digital stations that might also have console permissions. The FAC cannot be used to activate Station Lock for the attendant console, but the FAC can be dialed from the attendant console in an attempt to remotely activate or deactivate Station Lock for another station.

- Personal Station Access (PSA)

Station Lock can be used for PSA stations as long as they are associated with an extension. When stations are disassociated, Station Lock cannot be activated.

- Remote Access

After a remote user dials a valid barrier code, the user receives system dial tone. To activate/deactivate Station Lock, the user must dial the FAC, then the extension number, then the security code number.

## Station Lock by time of day

Beginning with Communication Manager 4.0 or later, you can also lock stations using a Time of Day (TOD) schedule.

To engage the TOD station lock/unlock you do not have to dial the station lock/unlock FAC, or use **stn-lock** button push.

When the TOD feature activates the automatic station lock, the station uses the Class of Restriction (COR) assigned to the station lock feature for call processing. The COR used is the same as it is for manual station locks.

The TOD lock/unlock feature does not update displays automatically, because the system would have to scan through all stations to find the ones to update.

The TOD Station Lock feature works as follows:

- If the station is equipped with a display, the display will show “Time of Day Station Locked”, if the station invokes a transaction which is denied by the Station Lock COR. Whenever

the station is within a TOD Lock interval, the user will hear a special dial tone instead of the normal dial tone, if the special dial tone is administered.

- For analog stations or without a display, the user hears a special dial tone. The special dial tone has to be administered and the user hears it when the station is off hook.

After a station is locked by TOD, it can be unlocked from any other station if the Feature Access Code (FAC) or button is used. You have to also know the Station Security Code, and that the **Manual-unlock allowed?** field on the Time of Day Station Lock Table screen is set to *y*.

Once a station has been unlocked during a TOD lock interval, the station remains unlocked until next station lock interval becomes effective.

If the station was locked by TOD and by Manual Lock, an unlock procedure will unlock the Manual Lock as well as the TOD Lock (“Manual-unlock allowed?” field on the Time of Day Station Lock Table screen is set to *y*).

The TOD feature does not unlock a manually locked station.

 **Note:**

The attendant console cannot be locked by TOD or manual station lock.

**Screens for administering Station Lock**

| Screen name                       | Purpose   | Fields   |
|-----------------------------------|---|--|
| COR                               | Administer a Class of Restriction (COR) that allows the user to activate Station Lock with a feature access code (FAC). | <b>Station Lock COR</b>  |
| Feature Access Code (FAC)         | Assign one FAC for Station Lock activation, and another FAC for Station Lock Deactivation.                              | <b>Station Lock Activation</b><br><b>Station Lock Deactivation</b>           |
| Station                           | Assign the user a COR that allows the user to activate Station Lock with an FAC.  | <b>COR</b><br><b>Time of Day Lock Table</b>                                  |
|                                   | Assign a sta-lock feature button for a user.  | Any available button field in the <b>BUTTON ASSIGNMENTS</b> area             |
|                                   | Assign a Station Security Code (SSC) for a user.  | <b>Security Code</b>   |
| Time of Day Station Lock Table    | Administer station lock by time of day.   | <b>Table Active</b><br><b>Manual Unlock Allowed</b><br><b>Time Intervals</b> |
| Feature Related System Parameters | Enable special dial tone.   | <b>Special Dial Tone</b>   |

---

## Managing Telephones

### Installing New Telephones

Simple administration allows you to plug a telephone into a jack and dial a sequence to start up service to the telephone. The dialing sequence sets up an association between the telephone and the corresponding station administration.

 **Security alert:**

If you do not manage this feature carefully, its unauthorized use might cause you security problems. Consult the *Avaya Products Security Handbook* for suggestions on how to secure your system and find out about obtaining additional security information. For traditional instructions, see *Installing New Telephones*.

**Related topics:**

[Adding new telephones](#) on page 168

## Before You Start

- 
1. On the Feature-Related System Parameters screen, be sure the **Customer Telephone Activation (CTA) Enabled** field is y and the **TTI Enabled** field is y
  2. Complete the Station screen for the new telephone and type x in the **Port** field.

 **Note:**

The telephone type must match the board type. For example, match a two-wire digital telephone with a port on a two-wire digital circuit pack. Use this procedure with all circuit-switched telephones except BRI (ISDN) and model 7103A.

 **Caution:**

You can destroy your hardware if you attempt to connect an analog telephone to a digital port.

To associate a telephone with existing x-port station administration, complete the following steps from the telephone you want to install:

3. Plug the telephone into the wall jack.
4. Lift the receiver and continue if you hear the dial tone.
5. Dial #\*nnnn, where nnnn is the extension number of the telephone you are installing.
6. Hang up after you receive the confirmation tone.
7. Dial a test call to confirm that the telephone is in service.

If possible, call a telephone with a display so the person answering can confirm that you entered the correct extension number.

8. Repeat the process until all new telephones have been installed.
9. For security reasons, you should disable this feature when you are done. At the system administration terminal type change system-parameters features to access the Feature-Related System Parameters screen.
10. Type `n` in the **Customer Telephone Activation (CTA) Enabled** field.
11. Press `Enter` to save your changes.
12. Type `save translations`.
13. Press `Enter` to permanently save the changes.

Fixing problems: If you misdial and the wrong extension is activated for the telephone you are using, use the terminal translation initialization (TTI) unmerge feature access code to “uninstall” the telephone before you try again.

---

## Adding new telephones

When you are asked to add a new telephone to the system, what do you do first? To connect a new telephone you need to do three things:

Before you can determine which port to use for the new telephone, you need to determine what type of telephone you are installing, what ports are available, and where you want to install the telephone.

- 
1. Find an available port .
  2. Wire the port to the cross-connect field or termination closet.
  3. Tell the telephone system what you are doing.

---

### Related topics:

[Managing Telephones](#) on page 167

## Gathering necessary information

- 
1. Determine whether the telephone is an analog, digital, ISDN, or hybrid set. You can also administer a virtual telephone, one without hardware at the time of administration.

You need this information to determine the type of port you need, because the port type and telephone type must match.

2. If you do not know what type of telephone you have, see the **Type** field on the Station screen for a list of telephones by model number.
3. Record the room location, jack number, and wire number.  
You might find this information on the jack where you want to install the telephone, recorded in your system records, or from the technician responsible for the physical installation.
4. To view a list of boards on your system, type `list configuration station`. The available boards (cards) and ports appear.
5. Press `Enter`.  
The System Configuration screen appears. The System Configuration screen shows all the boards on your system that are available for connecting telephones. You can see the board number, board type, circuit-pack type, and status of each board's ports.
6. Choose an available port and record its port address.  
Each port that is available or unassigned is indicated by a "u". Choose an available port from a board type that matches your telephone type (such as a port on an analog board for an analog telephone). Every telephone must have a valid port assignment, also called a port address. The combined board number and port number is the port address. So, if you want to attach a telephone to the 3rd port on the 01C05 board, the port address is 01C0503 (01=cabinet, C=carrier, 05=slot, 03=port).



**Note:**

If you add several telephones at one time, you might want to print a paper copy of the System Configuration screen.

7. To print the screen to a printer attached to the system terminal, type `list configuration station print`
8. Press `Enter`.
9. To print to the system printer that you use for scheduled reports, type `list configuration station schedule immediate`.
10. Press `Enter`.
11. Choose an extension number for the new telephone.  
The extension you choose must not be assigned and must conform to your dial plan. You should also determine whether this user needs an extension that can be directly dialed (DID) or reached via a central telephone number. Be sure to note your port and extension selections on your system's paper records.

## Connecting the Telephone physically

Once you have collected all the information, you are ready to physically wire the port to the cross-connect field.

If you have an Avaya technical support representative or on-site technician who completes the physical connections, you need to notify them that you are ready to add the telephone to the system. To request that Avaya install the new connections, call your Avaya technical support representative to place an order.

If you are responsible for making the connections yourself and if you have any questions about connecting the port to the cross-connect field, see your system installation guide. Now you are ready to configure the system so that it recognizes the new telephone.

## Obtaining display labels for telephones

Instructions for downloading telephone display labels

You will need display labels for each telephone type that you will install.

- 
1. Set the **Display Language** field on the Station screen to English, Spanish, Italian, French, user-defined, or unicode.



### Note:

Unicode display is only available for Unicode-supported telephones. Currently, the 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones support Unicode display. Unicode is also an option for the 2420J telephone when **Display Character Set** on the System Parameters Country-Options screen is Katakana. For more information on the 2420J, see *2420 Digital Telephone User's Guide, 555-250-701*.

2. For a Eurofont character display for the 2420/2410 telephone, set the **Display Character Set** field on the System-Parameters Country-Options screen to Eurofont.
3. For a Katakana character display for the 2420/2410 telephone, set the **Display Character Set** field on the System-Parameters Country-Options screen to Katakana.

---

## Adding a new station

### Prerequisites

Make sure the extension number that you are about to use conforms to your dial plan.

---

The information that you enter on the Station screen advises the system that the telephone exists and indicates which features you want to enable on the telephone. Communication Manager allows customers enter extensions with punctuation on the command line. Punctuation is limited to dashes (hyphens) and dots (periods). Communication Manager cannot process a command like `add station 431 4875`. You must format a command in one of these ways:

- add station 431-4875
- add station 431.4875
- add station 4314875

---

1. To access the Station screen for the new telephone choose one the following actions.

- **Type** `add station nnnn`, where `nnnn` is the extension for the new telephone.
- **Type** `add station next` to automatically use the next available extension number.



**Note:**

If you have **Terminal Translation Initialization (TTI)** enabled, you might receive the following error message when attempting to add a new station:  
`No station/TTI port records available; 'display capacity' for their usage`

If your receive this error message, choose one or more of the following actions.

- Remove any DCP or Analog circuit packs that have no ports administered on them.
- If you are not using TTI or any related feature (such as PSA or ACTR), set the **Terminal Translation Initialization (TTI) Enabled?** field on the Feature Related System Parameters screen to `on`.
- Contact your Avaya technical support representative. For more information on TTI, see Terminal Translation Initialization in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.
- For more information on the System Capacity screen, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

2. Press `Enter`.

When the Station screen appears, you see the extension number and some default field values.

3. Type the model number of the telephone into the **Type** field. For example, to install a 6508D+ telephone, type `6480D+` in the **Type** field.



**Note:**

The displayed fields might change depending on the model you add.

4. Type the port address in the **Port** field.

 **Note:**

Port 1720 is turned off by default to minimize denial of service situations. This applies to all IP softphones release 5.2 or later. You can change this setting, if you have root privileges on the system, by typing the command: `/opt/ecs/sbin ACL 1720 on or off`.

5. Type a name to associate with this telephone in the **Name** field.

The name you enter displays on called telephones that have display capabilities. Some messaging applications, such as INTUITY, recommend that you enter the user's name (last name first) and their extension to identify the telephone. The name entered is also used for the integrated directory.

 **Tip:**

To hide a name in the integrated directory, enter two tildes (~~) before the name when you assign it to the telephone, and set **Display Character Set** on the System Parameters Country-Options screen to Roman. This hides the name in the integrated directory. The tildes are not displayed with Caller ID name. Note that this is the only method to hide a name in the integrated directory. Also, if a name is entered with only one tilde (~), the name is converted to Eurofont characters.

 **Note:**

For 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones, the **Name** field is supported by Unicode language display. You must be using ASA or MSA. For more information on Unicode language display, see *Administering Unicode display*. Unicode is also an option for the 2420J telephone when **Display Character Set** on the System Parameters Country-Options screen is Katakana. For more information on the 2420J, see *2420 Digital Telephone User's Guide, 555-250-701*.

6. Press `Enter` to save your changes.

---

## Changing a station

You can make changes to a new telephone, such as assigning coverage path or feature buttons.

- 
1. Enter `change station nnnn` where nnnn is the extension of the new telephone.
  2. Change the necessary fields, then press `Enter`.
- 

## Duplicating Telephones

A quick way to add telephones is to copy the information from an existing telephone and modify it for each new telephone. For example, you can configure one telephone as a template for an

entire work group. Then, you merely duplicate the template Station screen to add all the other extensions in the group.

 **Note:**

Only telephones of the same model can be duplicated. The `duplicate` command copies all the feature settings from the template telephone to the new telephones.

- 
1. Type `display station nnnn`, where `nnnn` is the extension of the Station screen you want to duplicate to use as a template.
  2. Press `Enter`.
  3. Verify that this extension is the one you want to duplicate.
  4. Press `Cancel` to return to the command prompt.
  5. Type `duplicate station nnnn`, where `nnnn` is the extension you want to duplicate; then press `Enter`.  
The system displays a blank duplicate Station screen.

Alternately, you can duplicate a range of stations by typing `duplicate station <extension> start nnnn count <1-16>`, where `<extension>` represents the station you want to duplicate, `nnnn` represents the first extension number in a series, and `count <1-16>` represents the number of consecutive extensions after the start extension to create as duplicates.

 **Note:**

If you want to duplicate the settings of another station, but need to change the port or station type, you must individually administer each station after creating the duplicates.

6. Type the extension, port address and telephone name for each new telephone you want to add.  
The rest of the fields on the Station screen are optional. You can complete them at any time.
  7. Press `Enter`.  
Changes are saved to system memory.
  8. To make changes to these telephones, such as assigning coverage paths or feature buttons, type `change station nnnn`, where `nnnn` is the extension of the telephone that you want to modify; then press `Enter`.
-

## Adding multiple call center agents

You can add multiple call center agents, all with the same settings, based on an agent that is already administered.

- 
1. Enter `command duplicate agent-loginID` and the extension of the agent you want to duplicate.
  2. Select `Start` and enter the extension you want to use for the first new agent
  3. Select `count` and the number of agents you want to add.
  4. Fill in the information on the Agent LoginID screen.

For more information, see *Avaya Call Center Release 4.0 Automatic Call Distribution (ACD) Guide, 07-600779*.

---

## Using an alias

Not every telephone model or device has a unique Station screen in the system. You might have to use an available model as an “alias” for another. If you need to enter a telephone type that the system does not recognize or support, use an alias. Defining aliases is also a useful method to identify items that act as analog stations on Communication Manager, such as fax machines, modems, or other analog device.

If you purchase a telephone model that is newer than your system, you can alias this telephone to an available model type that best matches the features of your new telephone. See your telephone’s manual to determine which alias to use. If your manual does not have this information, you can contact the DEFINITY helpline for an appropriate alias.

For example, we will create two aliases: one to add a new 6220 telephone and one to add modems to our system.

- 
1. See your new telephone’s manual to find the correct alias.  
In our example, we find that the 6220 should be administered on an older system as a 2500 telephone.
  2. Type `change alias station`.
  3. Press `Enter`.  
The Alias Station screen appears.
  4. Type `6220` in the **Alias Set Type** field.  
This is the name or model of the unsupported telephone.
  5. Type `2500` in the **Supported Set Type** field.

This is the name or model of the supported telephone.

6. Type `modem` in the **Alias Set Type** field.

You can call the alias set anything you like. Once you define the alias, you can use the alias set in the **Type** field on the Station screen.

7. Type `2500` in the **Supported Set Type** field.

Entering 2500 indicates to the system that these models are basic analog devices.

8. Press `Enter` to save your changes.

Now you can follow the instructions for adding a new telephone (or adding a fax or modem). Avaya Communication Manager now recognizes the new type (6220 or modem) that you enter in the **Type** field.

Be sure to see your telephone's manual for instructions on how to set feature buttons and call appearance buttons.

**Note:**

If you need to use an alias for a telephone, you might not be able to take advantage of all the features of the new telephone.

---

## Customizing your Telephone

This section provides recommendations for setting up or enhancing your personal telephone. You need a telephone that is powerful enough to allow you to use all the features you might give to other employees. You might want to add feature buttons that allow you to monitor or test the system, so that you can troubleshoot the system from your telephone.

It will be much easier to monitor and test your system if you have a telephone with:

- A large multi-button display (such as 8434D or 8410D)
- A class of service (cos) that has console permissions
- The following feature buttons
  - ACA and Security Violations (assign to lamp buttons)
  - Busy verify
  - Cover message retrieval button
  - Major/minor alarm buttons
  - Trunk ID buttons
  - Verify button

Once you select a telephone, you'll want to determine if you want to place this telephone at your desk or in the server room. If the telephone is in the server room (near the system administration terminal), you can quickly add or remove feature buttons to test features and

facilities. You might decide that you want a telephone at both your desk and in the server room — it's up to you.

You might also find it handy to set up multiple telephones for testing applications and features before you provide them to users. You might want to have a telephone that mimics each type of user telephone in your organization. For example, if you have four basic telephone templates, one for executives, one for marketing, one for technicians, and one for other employees, you might want to have examples of each of these telephones so you can test new features or options. Once you are satisfied that a change works on the test telephone, you can make the change for all the users in that group.

## Upgrading telephones

If you want to change telephone types for a user and do not need to change locations, you can just access the Station screen for that extension and enter the new model number.

### Note:

This method can be used only if the new telephone type matches the existing port type (such as digital telephone with a digital port).

For example, if a user at extension 4556 currently has a 7410+ telephone and you want to replace it with a new 8411D telephone:

- 
1. Type `change station 4556`.
  2. press `Enter`.  
The Station screen for 4556 appears.
  3. Overwrite 7410+ with 8411D in the **Type** field.
  4. Press `Enter`.  
Now you can access the functions and feature buttons that correspond to an 8411D telephone.
- 

## Swapping telephones

You will often find that you need to move or swap telephones. For example, employees moving from one office to another might want to bring their telephones. In this case, you can use X ports to easily swap the telephones.

In general, to swap one telephone (telephone A) with another telephone (B), you change telephone A's port assignment to x, change telephone B's port assignment to A's old port, and, finally, change the x for telephone A to B's old port. Note that these swapping instructions work only if the two telephones are the same type (both digital or both analog, etc.).

For example, to swap telephones for extension 4567 (port 01C0505) and extension 4575 (port 01C0516), complete the following steps:

- 
1. Type `change station 4567`.
  2. Press `Enter`.
  3. Record the current port address (01C0505) and type **x** in the **Port** field.
  4. Press `Enter` to save your changes.
  5. Type `change station 4575`.
  6. Press `Enter`.
  7. Record the current port address (01C0516)
  8. Type `01C0505` in the **Port** field.
  9. Update the **Room** and **Jack** fields.
  10. Press `Enter` to save your changes
  11. Type `change station 4567` again.
  12. Press `Enter`.
  13. Type `01C0516` in the **Port** field  
This is the port that used to be assigned to extension 4575
  14. Update the **Room** and **Jack** fields.
  15. Press `Enter` to save your changes.
  16. Physically unplug the telephones and move them to their new locations.  
When you swap telephones, the system keeps the old button assignments. If you are swapping to a telephone with softkeys, the telephone could have duplicate button assignments, because softkeys have default assignments. You might want to check your button assignments and modify them as necessary.
- 

## Automatic Customer Telephone Rearrangement

Automatic Customer Telephone Rearrangement (ACTR) allows a telephone to be unplugged from one location and moved to a new location without additional administration in Avaya Communication Manager. Communication Manager automatically associates the extension to the new port. ACTR works with 6400 Serialized telephones and with the 2420/2410 telephones. The 6400 Serialized telephone is stamped with the word “Serialized” on the faceplate for easy identification. The 6400 Serialized telephone memory electronically stores its own part ID (comcode) and serial number, as does the 2420/2410 telephone. ACTR uses the stored information and associates the telephone with new port when the telephone is moved.

ACTR is an enhancement to Terminal Translation Initialization (TTI), Personal Station Access (PSA), Customer Telephone Activation (CTA). ACTR makes it easy to identify and move telephones.

 **Caution:**

When a telephone is unplugged and moved to another physical location, the **Emergency Location Extension** field must be changed for that extension or the USA Automatic Location Identification database must be manually updated. If the **Emergency Location Extension** field is not changed or if the USA Automatic Location Identification database is not updated, the DID number sent to the Public Safety Access Point (PSAP) could send emergency response personnel to the wrong location.

On the Feature-Related System Parameters screen, set the **Terminal Translation Initialization (TTI) Enabled** field to voice and the **TTI State** field to voice.

 **Note:**

When a telephone is moved, if there is any local auxiliary power (a power supply plugged into a local AC outlet), the telephone must be plugged into an AC outlet at the telephone's new location. A telephone with remote auxiliary power must be supplied remote auxiliary power at its new location. If you do not supply auxiliary power in either case after a telephone is moved, some optional adjuncts (for example, an expansion module) do not operate.

When you enter always or once in the **Automatic Moves** field on the Station screen, Communication Manager adds the extension to its ACTR Move List database. When the telephone is plugged in, Communication Manager asks the telephone for its serial number and records the serial number on the ACTR Move List. If you change the entry in the **Automatic Moves** field from always or once to no, Communication Manager removes the extension from the Move List.

### How calls are processed during a move

When a telephone is unplugged while on a call, and a 6400 Serialized telephone or a 2420/2410 telephone that is administered for automatic moves is plugged into the port within 60 seconds.

- Both extensions are placed in idle state
- Active calls on either extension are dropped, unless the call is active on a bridged appearance at some other telephone
- Held calls remain in a hold state
- Any calls ringing on either extension instantly proceed to the next point in coverage or station hunting path, unless the call is ringing on a bridged appearance at some other telephone
- User actions that were pending when the new telephone was plugged in are aborted

You can use the `list station movable` command to keep track of extensions on the move list. Once you reach the maximum number, Communication Manager does not allow additional extensions.

## Using ACTR to move telephones

### Prerequisites

- Be sure the **TTI** field on the Feature-Related System Parameters screen is set to y.
- Before you move a telephone in your system, set the **TTI State** field to voice on the Feature-Related System Parameters screen.

---

You can allow a telephone to be unplugged from one location and moved to a new location without additional administration on Avaya Communication Manager. For example, to allow moves anytime for a telephone at extension 1234:

- 
1. Type `change station 1234`.
  2. Press `Enter`.
  3. Move to the **Automatic Moves** field
  4. Type `always` in the **Automatic Moves** field.
  5. Press `Enter` to save your changes.
- 

## Terminal Translation Initialization

Terminal Translation Initialization (TTI) allows you to merge an x-ported station to a valid port by dialing a TTI merge code, a system-wide security code, and the x-port extension from a telephone connected to that port. TTI also allows you to separate an extension from its port by dialing a similar separate digit sequence. This action causes the station to revert to an x-port.

TTI can be used for implementing telephone and data module moves from office to office. That is, you can separate a telephone from its port with TTI, unplug the telephone from the jack, plug in the telephone in a jack in a different office, and merge the telephone to its new port with TTI.

If you are moving telephones and concerned about security, you might also want to see *Setting up Personal Station Access* for more information about setting the security code for each extension.



### Security alert:

If you do not manage this feature carefully, its unauthorized use might cause you security problems. For example, someone who knows the TTI security code could disrupt normal business functions by separating telephones or data terminals. You can help protect against this action by frequently changing the TTI security code. You can further enhance system security by removing the feature access code (FAC) from the system when it does not need to be used (for example, there are no moves going on at present). Consult the *Avaya Products Security Handbook* for additional steps to secure your system and find out about obtaining information regularly about security developments.

## Merging an extension with a TTI telephone

### Prerequisites

Before you can merge a telephone, you must set the **TTI State** field to voice on the Feature-Related System-Parameters screen. You also must set the extension to match the port type of the TTI port making the merge request. For example, a digital telephone type can merge only to a port on a digital board.

---

 **Caution:**

When a telephone is unplugged and moved to another physical location, the **Emergency Location Extension** field must be changed for that extension or the USA Automatic Location Identification database must be manually updated. If the **Emergency Location Extension** field is not changed or if the USA Automatic Location Identification database is not updated, the DID number sent to the Public Safety Network could send emergency response personnel to the wrong location.

 **Note:**

You cannot use TTI to change a virtual extension.

 **Caution:**

You can destroy your hardware if you attempt to connect an analog telephone to a digital port.

- 
1. Dial the TTI merge FAC
    - If the code is correct, you receive the dial tone.
    - If the code is not correct, you receive the intercept tone.
  2. Dial the TTI security code from the telephone you want to merge.
    - If the code is correct, you receive the dial tone.
    - If the code is not correct, you receive the intercept tone.
  3. Dial the extension of the telephone you want to merge.
    - If the extension is valid, you receive confirmation tone, which might be followed by dial tone. (It is possible to receive the intercept tone immediately following the confirmation tone. If this happens, you need to attempt the merge again.)
    - If the extension is valid, but the extension is being administered, you receive the reorder tone. Try the merge again later.
    - If the extension is invalid, you receive the intercept tone.
    - If the system is busy and cannot complete the merge, you receive the reorder tone. Try the merge again later.

- If the telephone has a download status of pending, you receive the reorder tone. You need to change the download status to complete to successfully complete the TTI merge.

---

## Separating TTI from a telephone

---

1. Dial the TTI separate FAC.
2. Dial the TTI security code.
  - If the code is correct, you receive the dial tone.
  - If the code is not correct, you receive the intercept tone.
3. Dial the extension of the telephone to be separated.
  - If you have dialed the extension of the telephone currently merged with this telephone, you receive the confirmation tone.
  - If you have dialed the extension of the telephone currently merged with this telephone, but the extension is being administered, you receive reorder tone. Try the separation again later.
  - If you have not dialed the extension of the telephone currently merged with this telephone, you receive the intercept tone.
  - If the system is busy and cannot complete the separation, you receive the reorder tone. Try the separation again later.

---

## Troubleshooting TTI

If you are having difficulty using TTI, you might want to review the following system restrictions

| Problem  | Restriction   |
|--|---|
| The <b>TTI Ports</b> field on the System Capacity screen (type display capacity) shows the number of TTI ports used in a server running Communication Manager. | This field shows only the number of TTI ports being administered. If a TTI exceeds the maximum number of ports, the port is not administered and cannot be added. In that case, a telephone cannot be added. For details on the System Capacity screen, see <i>Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers</i> , 03-300431.<br>BRI endpoints are only counted as one TTI port. For example, for every two BRI endpoints, one TTI port is counted. As such, you can have two telephones assigned to one port. If either endpoint is administered, the TTI port count is reduced by 1. |
| The total number of translated telephones and Voice TTI ports  | The total number of translated data terminals and Data TTI ports in a system is limited to the maximum number of administered data modules allowed in the system.   |

| Problem   | Restriction  |
|---|--|
| <p>in a system is limited to the maximum number of administered telephones supported in the system.</p>   |  |
| <p>Set the <b>TTI State</b> field to voice and then set the <b>TTI State</b> field to data. When you use this order, voice and then data, you reduce the chance of a user trying to use TTI on a data-only terminal that does not have TTI port translation</p> | <p>This can happen when the number of telephones allowed by the system is twice the number of data terminals. For example, if the system limit for telephones is 15,000 and 7,500 for data, then when TTI was turned on for data first, only the first 7,500 unadministered ports would get TTI port translations.</p>   |
| <p>When TTI is activated for the system, these actions take place</p>   | <ul style="list-style-type: none"> <li>• If the <b>TTI State</b> field was previously activated but in a different state (such as, a voice to data state), the old TTI translations are removed and the new ones added on a board by board basis</li> <li>• If the <b>TTI State</b> field is set to voice, then default TTI translations are generated for every unadministered port on all digital, hybrid, and analog boards.</li> <li>• If the <b>TTI State</b> field is set to data, then default TTI translations are generated for every unadministered port on all digital and data line boards in the system.</li> <li>• Whenever a new digital board is inserted when the system is in TTI Data mode, or when a digital, hybrid, or analog board is inserted when the system is in TTI Voice mode, the unadministered ports on the board become TTI ports.</li> <li>• When TTI is deactivated, all translation for the TTI ports are removed in the system; the ports return to an unadministered state.</li> </ul> |

## Removing telephones

### Prerequisites

Before you physically remove a telephone from your system, check the telephone's status, remove it from any group or usage lists, and then delete it from the system's memory. For example, to remove a telephone at extension 1234:

- 
1. Type `status station 1234`.
  2. Press `Enter`.  
The General Status screen appears.
  3. Make sure that the telephone:
    - a. is plugged into the jack
    - b. is idle (not making or receiving calls)
    - c. has no messages waiting
    - d. has no active buttons (such as **Send All Calls** or **Call Forwarding**)
  4. Type `list groups-of-extension 1234`.
  5. Press `Enter`.  
The Extension Group Membership screen shows whether the extension is a member of any groups on the system.
  6. Press `Cancel`.
  7. If the extension belongs to a group, access the group screen and delete the extension from that group.  
If extension 1234 belongs to pickup group 2, type `change pickup group 2` and delete the extension from the list.
  8. Type `list usage extension 1234`.
  9. Press `Enter`.  
The Usage screen shows where the extension is used in the system.
  10. Press `Cancel`.
  11. If the extension appears on the Usage screen, access the appropriate feature screen and delete the extension.  
If extension 1234 is bridged onto extension 1235, type `change station 1235` and remove the appearances of 1234.
  12. Type `change station 1234`.
  13. Press `Enter`.
  14. Type `remove station 1234`.

15. Press `Enter`.  
The system displays the Station screen for this telephone so you can verify that you are removing the correct telephone.



**Tip:**

Be sure to record the port assignment for this jack in case you want to use it again later

16. If this is the correct telephone, press `Enter`.
  - a. If the system responds with an error message, the telephone is busy or still belongs to a group.
  - b. Press `Cancel` to stop the request, correct the problem.
  - c. Enter `remove station 1234` again
17. Remove the extension from voice mail service if the extension has a voice mailbox.
18. Type `save translations`.
19. Press `Enter` to save your changes



**Note:**

You do not need to delete the extension from coverage paths. The system automatically adjusts coverage paths to eliminate the extension.

---

### Next steps

Now you can unplug the set from the jack and store it for future use. You do not need to disconnect the wiring at the cross-connect field. The extension and port address remain available for assignment at a later date.

Once you successfully remove a set, that set is permanently erased from system memory. If you want to reactivate the set, you have to add it again as though it were a new telephone.

## Adding a fax or a modem

Connecting a fax machine or modem to your system is similar to adding a telephone, with a few important exceptions. If you have not added a telephone, you might want to read *Adding Telephones*.

Because the system does not recognize the concept of “fax” or “modem”, you need to administer these items as basic analog stations. You can merely use the supported station type 2500 (analog, single line).

Alternatively, you can create aliases to the 2500 for fax machines and modems. If you want to be able to create reports that indicate which stations are faxes or modems, you should create aliases for these items. For more information about aliasing, see *Using Alias*.

For this example, let us assume that we have already defined an alias for “fax” as a 2500 and that we now want to add a fax machine to extension 4444.

- 
1. Type `add station 4444`.
  2. Press `Enter`.
  3. In the **Type** field, type `fax`.
  4. In the **Port** field, type the port address.
  5. In the **Name** field, type a name to associate with this fax.
  6. Move to the **Data Restriction** field and type `y`.  
Entering `y` in this field prevents calls to and from this extension from being interrupted by tone signals. This is important for fax machines and modems as these signals can disrupt transmissions of data.
  7. In the **Distinctive Audible Alert** field, type `n`.  
This eliminates the distinct 2-burst ring for external calls, which often interferes with the auto-answer function on fax machines or modems.
  8. Press `Enter` to save changes.
- 

## Enabling transmission over IP networks for modem, TTY, and fax calls

### Prerequisites

The ability to transmit fax, modem, and TTY calls over IP trunks or LANs and WANs assumes that the endpoints sending and receiving the calls are connected to a private network that uses H.323 trunking or LAN connections between gateways and/or port networks. This type of transmission also assumes that calls can either be passed over the public network using ISDN-PRI trunks or passed over an H.323 private network to Communication Manager switches that are similarly enabled. As a result, it is assumed that you have assigned, or will assign, to the network gateways the IP codec you define in this procedure. For our example, the network region 1 will be assigned codec set 1, which you are enabling to handle fax, modem, and TTY calls.

- 
1. Type `ip-codec-set 1`.
  2. Press `Enter`.  
The IP Codec Set screen appears.
  3. Complete the fields as required for each media type you want to enable.
  4. Press `Enter`.

For more information on modem/fax/TTY over IP, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

---

## IP Softphones

Avaya IP Softphones enable the end user to control telephone calls directly from a personal computer (PC). An end user can log in remotely to your company's server running Avaya Communication Manager and then make and receive telephone calls from the telephone extension.

Avaya IP Softphones supports the following modes:

- **Road-Warrior**

You typically use this mode for laptop users who are travelling. In this mode, the PC LAN connection carries both the call control signaling and the voice path. Because the audio portion of the voice call is handled by the PC, you must have some kind of audio device (e.g., handset, headset) PC to provide the audio connection.

- **Telecommuter or Avaya IP Agent**

For the telecommuter or Avaya IP Agent mode, you make two separate connections to the Avaya DEFINITY server. The signaling path is carried over an IP network and the voice path is carried over the standard circuit-switched telephone network (PSTN). Since you are using a telephone for audio, you do not need an H.323 PC audio application.

The telecommuter mode uses the Avaya IP Softphone interface (on the user's PC) and a standard telephone. The Avaya IP Agent mode uses the Avaya IP Agent interface (on the agent's PC) and a call center telephone.

- **Native H.323 (only available with Avaya IP Softphone R2)**

The stand-alone H.323 mode enables travelers to use some Communication Manager features from a remote location. This mode uses a PC running an H.323 v2-compliant audio application, such as Microsoft NetMeeting. The H.323 mode controls the call signaling and the voice path. However, since it does not use the IP Softphone interface, this configuration is capable of operating only as an analog or single-line telephone making one call at a time without any additional assigned features. You can provide stand-alone H.323 users only features that they can activate with dial access codes.

- **Control of IP Telephone (only available with IP Softphone R4 and later)**

This mode allows you to make and receive calls under the control of the IP Softphone - just like in the **Telecommuter** or **Road Warrior** mode. The big difference is that you have a real digital telephone under your control. In the **Road Warrior** mode, there is no telephone. In the Telecommuter mode, the telephone you are using (whether analog, digital, or IP telephone is brain dead). In this mode (if you have an IP telephone), you get the best of both worlds.

- **Control of DCP Telephone (only available with IP Softphone R5 and later)**

This feature provides a registration endpoint configuration that will allow an IP softphone and a non-softphone telephone to be in service on the same extension at the same time. In

this new configuration, the call control is done by both the softphone and the telephone endpoint. The audio is done by the telephone endpoint.

**+ Tip:**

Use status station to show the part (product) ID, serial number, and the audio connection method used by existing stations.

**\* Note:**

Beginning with the November 2003 release of Communication Manager, R1 and R2 IP Softphone and IP Agent, which use a dual connect (two extensions) architecture, are no longer supported. R3 and R4 IP Softphone and IP Agent, which use a single connect (one extension) architecture, continue to be supported. This applies to the RoadWarrior and the Telecommuter configurations for the IP Softphone. Native H.323 registrations for R1 and R2 Softphones continue to be supported.

**Related topics:**

[Troubleshooting IP Softphones](#)

## Enabling the system to use IP softphone

---

1. Display the System Parameters Customer-Options (Optional Features) screen.
  2. Verify the following field settings:
    - **Maximum Concurrently Registered IP Stations** is greater than 0.
    - **IP Stations** field is y
    - Information has been entered in the fields on the Maximum IP Registrations by Product ID page
  3. Verify that your DEFINITY CSI has a CLAN board and an IP Media Processor board.
  4. Install the IP Softphone software on each IP Softphone user's PC.
- 

## Road Warrior Mode

You can use the road-warrior mode when you have only a single telephone line available to access Avaya Communication Manager over the IP network.

You also can "take over" an IP telephone. Typically you would not have a different extension for your softphone. When you log in, the softphone takes over the existing telephone extension (turn the DCP or IP telephone off). During this time, that DCP or IP telephone is out of service. This is accomplished if, on the Station screen, the **IP Softphone** field is y.

We will add a road-warrior mode at extension 3001. Except for single-connect IP telephones, you have to actually administer two extensions for each road-warrior mode.

### ***Adding a Road Warrior mode***

---

1. Type `add station 3000`.
2. Press `Enter`.  
The Station screen appears.
3. In the **Type** field, enter `H.323`.
4. Press `Enter` to save your work.

### ***Administering Road Warrior***

---

1. Type `add station next`.
2. Press `Enter`.  
The Station screen appears.

 **Note:**

You choose to change an existing DCP extension by using `change station nnnn` in this step, where `nnnn` is the existing DCP extension.

3. In the **Type** field, enter the model of telephone you want to use.  
For example, enter `6408D`.
4. In the **Port** field, type `x` for virtual telephone or enter the port number if there is hardware.

 **Note:**

Port 1720 is turned off by default to minimize denial of service situations. This applies to all IP softphones release 5.2 or later. You can change this setting, if you have root privileges on the system, by typing the command: `/opt/ecs/sbin ACL 1720 on or off`.

5. In the **Security Code** field, enter the password for this remote user.  
For example, enter `1234321`.  
  
This password can be 3-8 digits in length.
6. In the **Media Complex Ext** field, type `3000`.  
This is the H.323 extension just administered.
7. In the **IP Softphone** field, type `y`.
8. On page 2, in the **Service Link Mode** field, type `as-needed`.  
Set this field to `permanent` only for extremely busy remote telephone users, such as call center agents.

9. In the **Multimedia Mode** field, type `enhanced`.
10. Press `Enter` to save your work.

Now you can install and configure the software on the user's PC. In this example, the user will login by entering their DCP extension (3001) and password (1234321).

---

### Adding a telecommuter mode

Assign this configuration to remote users who have two available telephone lines. For example, the following steps show how to administer a telecommuter mode for a home user at extension 3010.

- 
1. Type `add station 3010`.
  2. Press `Enter`.  
The Station screen appears.

 **Note:**

Use the `add station` command if this is a new DCP extension. Use the `change station` command for an existing DCP extension and ignore steps 3 and 4.)

3. In the **Port** field, type `x` for virtual telephone or enter the port number if there is hardware.
4. In the **Security Code** field, enter the password for this remote user.  
For example, enter `1234321`.  
  
This password can be up to 7 digits in length.
5. In the **IP Softphone** field, type `y`.
6. On page 2, in the **Service Link Mode** field, type `as-needed`.  
Set this field to permanent only for extremely busy remote telephone users, such as call center agents.
7. In the **Multimedia Mode** field, type `enhanced`.
8. Press `Enter` to save your work.  
  
Now you can install and configure the software on the user's PC. In this example, the user will login by entering their DCP extension (3010) and password (1234321).

---

### Troubleshooting IP Softphones

#### Problem

Display characters on the telephone can not be recognized.

#### Possible Causes

Microsoft Windows is not set to use Eurofont characters.

### **Proposed solution**

- 
1. Set the Microsoft Windows operating system to use Eurofont.
  2. Refer to user documentation on the Avaya IP Softphone for more information on how to install and configure the IP Softphone software.
- 

## **IP Telephones**

The 4600-series IP Telephones are physical sets that connect to Avaya Communication Manager via TCP/IP.

### **Caution:**

An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. Please be advised that an Avaya IP endpoint cannot dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. You should not use an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations.

### **Adding an IP telephone**

#### **Prerequisites**

Verify the system has a:

- TN2302 IP Media Processor circuit pack for audio capability
- TN799 Control-LAN circuit pack for signaling capability (for CSI Servers only)

Be sure that your system has been enabled to use IP Telephones. Display the System-Parameters Customer-Options (Optional Features) screen and verify the following field settings.

- **Maximum Concurrently Registered IP Stations** is greater than 0
- **IP Stations** field is y
- Information has been entered in the fields on the Maximum IP Registrations by Product ID page.

---

These steps show how to add an IP telephone at extension 4005 and how to assign an extension.

- 
1. Type `add station 4005`.
  2. Press `Enter`.  
The Station screen appears.

 **Note:**

When adding a new 4601 or 4602 IP telephone, you must use the 4601+ or 4602+ station type. This station type enables the Automatic Callback feature. When making a change to an existing 4601 or 4602, you receive a warning message, stating that you should upgrade to the 4601+ or 4602+ station type in order to access the Automatic Callback feature.

The **Port** field is display-only, and IP appears

3. In the **Security Code** field, enter the password for the IP telephone user.  
Although the system accepts a null password, the IP telephone will not work unless you assign a password.
4. Press `Enter` to save your work.

---

### Changing from dual-connect to single-connect IP telephones

When you have a dual extension telephone and you upgrade to a single extension telephone, you can remove the connection that is no longer used for that telephone. To remove the H.323 connection that is no longer needed, first record the media complex extension number:

- 
1. Type `change station nnnn` where `nnnn` is the extension number of the original dual-connect telephone that you are replacing with a single-connect telephone.  
The Station screen appears.
  2. Move to the **Media Complex Extension** field.
  3. Write down the number in the **Media Complex** field, then delete the number from the field.
  4. Press `Enter` to save your work.
  5. Remove the extension you recorded. Before you remove an H.323 extension from your system, check the status, remove it from any group or usage lists, and then delete it from the system's memory.  
For example, if you wrote down extension 1234 before you removed it from the **Media Complex** field on the Station screen, then remove extension 1234 using these steps:
  6. Type `status station 1234`.
  7. Press `Enter`.  
The General Status screen appears.

8. Make sure that the extension is idle (not making or receiving calls), has no messages waiting and has no active buttons (such as **Send All Calls** or **Call Forwarding**)
9. Type `list groups-of-extension 1234`.
10. Press `Enter`.  
The Extension Group Membership screen shows whether the extension is a member of any groups on the system.
11. Press `Cancel`.
12. If the extension belongs to a group, access the group screen and delete the extension from that group.  
If extension 1234 belongs to pickup group 2, type `change pickup group 2` and delete the extension from the list.
13. Type `list usage extension 1234`
14. Press `Enter`.  
The Usage screen shows where the extension is used in the system.
15. Press `Cancel`.
16. If the extension appears on the Usage screen, access the appropriate feature screen and delete the extension.  
If extension 1234 belongs to hunt group 2, type `change hunt group 2` and delete the extension from the list.
17. Type `change station 1234`
18. Press `Enter`.
19. Delete any bridged appearances or personal abbreviated dialing entries
20. Press `Enter`.  
The system displays the Station screen for this telephone so you can verify that you are removing the correct telephone.
21. Type `remove station 1234`.
22. Press `Enter`.
23. If this is the correct telephone, press `Enter`.
  - The system responds with `command successfully completed`.
  - If the system responds with an error message, the telephone is busy or still belongs to a group.
24. Press `Cancel` to stop the request, correct the problem, and type `remove station 1234` again.
25. Remove the extension from voice mail service if the extension has a voice mailbox.

26. Type `save translations`.
27. Press `Enter` to save your changes.

 **Note:**

You do not need to delete the extension from coverage paths. The system automatically adjusts coverage paths to eliminate the extension

Once you successfully remove the extension, it is permanently erased from system memory. If you want to reactivate the extension, you have to add it again as though it were new.

---

### Setting up emergency calls on IP telephones

Set up which “calling number” to send to the public safety access point when an emergency call is placed from an IP telephone

You use the Station screen to set up emergency call handling options for IP telephones. As an example, we'll administer the option that prevents emergency calls from an IP telephone.

- 
1. Type `change station nnnn` where `nnnn` is the extension of the telephone you want to modify.
  2. Press `Enter`.  
The Station screen appears.
  3. Click `Next Page` to find the **Remote Softphone Emergency calls** field.
  4. Type `block` in the **Remote Softphone Emergency calls** field.
  5. Press `Enter` to save your changes.

 **Caution:**

An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. Please be advised that an Avaya IP endpoint cannot dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. You should not use an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations. Please contact your Avaya representative if you have questions about emergency calls from IP telephones.

---

### Remote office setup

Avaya Remote Office provides IP processing capabilities to traditional call handling for voice and data between Avaya Communication Manager and offices with Remote Office hardware.

You need to add the information about Remote Office as a node in Communication Manager, add its extensions, and set up the trunk and signaling groups.

## Adding Remote Office to Communication Manager

### Prerequisites

Be sure the following fields on the System Parameters Customer-Options (Optional Features) screen are set to y or completed. If not, contact your Avaya representative.

- **Maximum Administered Remote Office Trunks**
- **Maximum Administered Remote Office Stations**
- **Product ID registration limit**
- **Remote Office**
- **IP station**
- **ISDN-PRI**

Also, be sure your Remote Office hardware is installed and administered at the remote location. You need the following information from the remote administration:

- IP address
- Password

---

In our example, we will set up a remote-office location using Avaya R300 Remote Office Communicator hardware in our branch office in Santa Fe. We will add a new node, and set up the signaling group and trunk group.

- 
1. Type `change node-names IP`.
  2. Press `Enter`.  
The Node Name screen appears.
  3. In the **Name** field, type in a word to identify the node.  
Type `Remote 6`.
  4. In the IP address field, type in the IP address to match the one on the Avaya R300 administration.
  5. Press `Enter` to save your changes.
  6. Type `add remote office` and the number for this remote office.
  7. Press `Enter`.  
The Remote Office screen appears.
  8. Fill in the following fields
    - **Node Name** - match the name on the IP Node Names screen.

- **Network Region** - this must match the network region on the IP Interfaces screen for the circuit packs that connect this remote office. Use display ip-interfaces to find this information.
- **Location** - match the one set up on the Location screen for this remote office.
- **Site Data** - identify the street address or identifier you want to use.

9. Press `Enter` to save your changes.



**Tip:**

Use status remote office to verify that your server running Communication Manager recognizes the Remote Office information. It also displays the extensions and signaling group you administer next.

---

### Setting up a trunk group

You can modify an existing trunk group or add a new one. In our example, we will add trunk group 6. Before you start, perform [Setting up a signaling group](#) on page 195.

- 
1. Type `add trunk group 6`.  
The Trunk Group screen appears.
  2. In the **Group Type** field, type `ISDN`.  
ISDN-PRI or ISDN-BRI must be `y` on the System Parameters Customer-Options (Optional Features) screen.
  3. In the **TAC** field, type in the trunk access code that conforms to your dial plan.
  4. In the **Carrier Medium** field, type `H.323 (Medpro)`.
  5. In the **Dial Access** field, type `y`.
  6. In the **Service Type** field, type `tie`.
  7. In the **Signaling Group** field, type in the signaling group you created.
  8. Press `Enter` to save your changes.
- 

### Setting up a signaling group

Each Remote Office has its own listen port and signaling group. Set up a new trunk group, or use an existing trunk group administered for H.323 signaling. To set up the signaling group for remote office:

- 
1. Type `add signaling-group` and the number of the group you want to add.  
The Signaling Group screen appears.
  2. In the **Group Type** field, type `H.323`

3. In the **Remote Office** field, type `y`.
4. In the **Trunk Group for Channel Selection** field, type the number of the trunk you set up for the remote office.
5. In the **Near-end Node Name** field, identify the node name assigned to the CLAN that supports the R300.
6. In the **Far-end Node Name** field, identify the node name assigned to the CLAN that supports the R300.
7. In the **Near-end Listen Port** field, type a port number in the 5000-9999 range.
8. In the **Far-end Listen Port** field, type `1720`.
9. In the **RRQ** field, type `y`.
10. Tab to the **Direct IP-IP Audio Connection** field on another page of this screen and type `y`.
11. Press `Enter` to save your changes.

---

### Setting up Remote Office on network regions

Now we will set up a network region and show the connections between regions. We begin with network region 1.

- 
1. Type `add ip-network-region 1`.
  2. Press `Enter`.  
The IP Network Region screen appears.
  3. In the **Name** field, describe the region you are setting up
  4. In the **Code Set** field, type the codec set you want to use in this region
  5. In the **UDP Port Range** field, type the range of the UDP port number to be used for audio transport.
  6. In the **Intra-region IP-IP Direct Audio** field, type `y`
  7. In the **Inter-region IP-IP Direct Audio** field, type `y`.
  8. Move to page 3 to set up connections between regions and assign codecs for inter-region connections.

 **Note:**

Page 2 of the IP Network Region screen shows a list of Survivable Remote Server for the network region, and pages 4 through 19 are duplicates of page 3, providing the ability to administer upto 250 locations.

The following connections are administered in this example.

- codec-set 2 is used between region 1 and region 4

- codec-set 5 is used between region 1 and region 99
  - codec-set 6 is used between region 1 and region 193
9. Assign the region number to the CLAN circuit pack. All the endpoints registered with a specific CLAN circuit pack belong to the CLAN's region.
- See *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504, for more information.

---

## Adding telephones to Remote Office

### Prerequisites

Be sure the extensions you add fit your dialing plan.

- 
1. Type `add station nnnn`, where `nnnn` is the extension you are adding.
  2. Press `Enter`.  
The Station screen appears.
  3. In the **Type** field, type in the model of the telephone you are adding.
  4. In the **Port** field, type `x`.  
This indicates that there is no hardware associated with the port assignment.
  5. In the **Name** field, identify the telephone for your records.
  6. In the **Security Code** field, match the password set up on the Remote Office administration.
  7. In the **Remote Office Phone** field, type `y`.
  8. Press `Enter` to save your changes.

---

## Updating files in the 2410, 2420, 1408, and 1416 DCP telephones

You can copy updated application code into Communication Manager using TFTP over a TCP/IP connection. This eliminates the need to physically remove the telephone and send it to the factory for the firmware update. This feature is available on all of the servers running Avaya Communication Manager.

To allow additional language support for the 1408 and 1416 DCP telephones, the font and language files are available for download. You can visit the Avaya Support site or contact Avaya representative for more information.

## Preinstallation tasks for firmware download

- 
1. Type `change node-name ip`.
  2. Press `Enter`.  
The IP Node Names screen appears.

3. Administer the TFTP server node name and the local node name (CLAN) and IP address.
4. Press `Enter` to save your changes.
5. Type `change ip-interfaces`.
6. Press `Enter`.  
The IP Interfaces screen appears
7. Administer the CLAN Ethernet interface or processor CLAN.
8. Press `Enter` to save your changes.

---

## Downloading the firmware file to Communication Manager

---

1. Place the file on the TFTP server using TFTP, FTP, HTTP or another file transfer program .
2. From the **Web Interface** menu, click the **Set LAN Security** link.
3. Click `Advanced`.  
A list of settings that can be enabled or disabled through the use of check boxes appears.
4. Scroll to **tftp** and check the box enabling inbound tftp traffic.
5. Click `Submit`.
6. Log into SAT and enter `change tftp-server`.
7. Press `Enter`.  
The TFTP Server Configuration screen appears.
8. In the **Local Node Name** field, enter the valid local node name from the IP Node Names screen.  
The node must be assigned to a CLAN ip-interface or procr (processor CLAN).
9. In the **TFTP Server Node Name** field, enter the valid TFTP server node name from the IP Nodes Names. screen
10. In the **TFTP Server Port** field, enter the TFTP server port number from where the file download begins.
11. In the **File to Retrieve** field, enter the name of the file to be retrieved.
12. Press `Enter` to save your changes.  
The file transfer begins.
13. Type `display tftp-server`.
14. Press `Enter` to view the status of the file transfer.  
A File download successful

message appears when the file transfer completes. It also displays the file size and the file name in memory.

After the file is successfully loaded the "Station Type:" will also identify the type of file, either firmware, font, or language, and the phone type the file can be downloaded into which is the 2410, 2420, or 1408/1416. The 1408 and 1416 share common firmware and font/language files.

---

## Downloading firmware to a single station

### Prerequisites

You must have console permissions to download someone else's telephones.

#### Note:

Steps 1 through 5 need be done only once to set up the FAC for file downloads. Thereafter, start at step 6 to download files.

Only one FAC download can be active at a time.

A FAC download cannot be started if a scheduled download is active.

The firmware file and type that is display via the "display tftp" form must be compatible with the station you are downloading.

The target extension must be administered as one of the DCP station types that support firmware download.

Set up a FAC for file downloads

- 
1. Type `change feature-access-codes`.
  2. Press `Enter`.
  3. Click `Next Page` until you see the **Station Firmware Download Access Code** field on the Feature Access Code (FAC) screen.
  4. In the **Station Firmware Download Access Code** field, enter a valid FAC as defined in the dial plan.
  5. Press `Enter` to save your changes.
  6. Take the 2410, 2420, 1408, or 1416 DCP telephone off-hook.
  7. Dial the Station Firmware Download FAC.  
For instance, \*36.
  8. Press `#` if you are dialing from the target station (or dial the telephone's extension to be downloaded).
  9. Place the telephone on-hook within 4 seconds after the confirmation tone.  
The telephone is placed in a busy-out state (not able to make or receive calls) and displays `Firmware Download in Progress`, the amount of the file downloaded,

and a timer. The telephone displays error messages and a success message before rebooting.

When the download completes, the telephone reboots and is released from the busy-out state.

---

### Downloading firmware to multiple stations

You can download firmware to multiple stations of the same type, either 2410, 2420, 1408, or 1416 DCP telephone. Download firmware to as many as 1000 stations per download schedule. You can schedule a specific time for the download, or you can administer the download to run immediately. To download 2410, 2420, 1408, or 1416 DCP station firmware to multiple stations:

- 
1. Type `change firmware station-download`.
  2. Press `Enter`.  
The Firmware Station Download screen appears.
  3. In the **Schedule Download** field, type `y`.  
The **Start Date/Time** and **Stop Date/Time** fields appear.
  4. In the **Start Date/Time** field, enter the month (mm), day (dd), year (yyyy), and time (hh:mm) that you want the download to begin.
  5. In the **Stop Date/Time** field, enter the month (mm), day (dd), year (yyyy), and time (hh:mm) that you want the download to begin.
  6. In the **Continue Daily Until Completed** field, enter `y` if you want the system to execute the firmware download each day at the scheduled time until all specified telephones have received the firmware.
  7. In the **Beginning Station** field, enter the first extension number in the range of telephones to which you want to download the firmware.  
Up to 1000 stations can be included in a scheduled download.
  8. In the **Ending Station** field, enter the last extension number in the range of telephones to which you want to download firmware.  
Up to 1000 stations can be included in a scheduled download.

 **Note:**

Although you can specify a range of up to 1000 extensions, all 1000 stations are not downloaded simultaneously because there is a limit of how many concurrent phones will be downloaded on a board, gateway, and port network. These limits will likely result in multiple "passes" required to attempt a download to the phone. Also note that on the first "pass" that only two phones will be attempted and if multiple phones fail then the schedule may stop.

9. Press `Enter`.

The firmware download is set to run at the scheduled time. If you entered `n` in the **Schedule Download?** field, pressing `Enter` immediately initiates the download to the specified range of telephones.

---

### Displaying firmware download status

You can use the `status firmware download` command to display status information for an active download schedule. To display download status:

- 
1. Type `status firmware download`.  
The Status Firmware Station Download screen appears.
  2. Press `Enter`.

 **Note:**

If you add the qualifier `last` to the `status firmware download` command, status information on the last download schedule is displayed.

---

### Disabling firmware downloads

You can use the `disable firmware download` command to disable any active download schedule. To disable active downloads:

- 
- Type `disable firmware download`.  
This command disables any active download schedule and the system displays `Command successfully completed` at the bottom of the screen.

---

### Native Support of Avaya 1408 and 1416 digital telephones

Native support of Avaya 1408 (1400 Mid) and 1416 (1400 High) digital telephones is available from Communication Manager 6.0 and later. Communication Manager supports call processing features for the Avaya 14xx digital telephones in a similar way as the Avaya 24xx digital telephones, along with support for the following:

- Fixed feature buttons (Hold, Conference, Transfer, Message waiting lamp, Drop and Redial)
- Message button
- 40 Unicode, Eurofont, or Kanafont character display message support
- Speakerphone functionality (including Group Listen)
- Eight call appearances or feature buttons

 **Note:**

In order to allow firmware upgrades and to utilize the new capabilities of the sets, the phone type must be administered as either a “1408” or “1416”.

### **Native Support of Avaya 1408 digital telephone**

Communication Manager provides native administration for the Avaya 1408 digital telephone. The Avaya 1408 digital telephone administration is similar to the Avaya 2410 digital telephone with the same fields and default values except for the following:

- Support for eight call appearances or feature buttons
- No “Customizable Labels?” field
- No “Media Complex Ext:” field
- Support for display languages which include English, Spanish, French, Italian, User defined, Unicode, Unicode2, Unicode3, and Unicode4

### **Native Support of Avaya 1416 digital telephone**

Communication Manager provides native administration for the Avaya 1416 digital telephone. The Avaya 1416 digital telephone administration is similar to the Avaya 2420 digital telephone with the same fields and default values except for the following:

- Support for 16 call appearances or feature buttons
- No “Customizable Labels?” field
- No “Data Option:” field
- No “Media Complex Ext:” field
- Support for display languages which include English, Spanish, French, Italian, User defined, Unicode, Unicode2, Unicode3, and Unicode4
- Support for “Button Modules” field rather than “Expansion Module” field

### **BM32 Button Support**

The Avaya 1416 digital telephone uses the BM32 button expansion module. Communication Manager supports two BM32 buttons for the Avaya 1416 digital telephone.

## **Administer location per station**

Use the Administer location per station feature to:

- Allow IP telephones and softphones connected through a VPN to be associated with the branch that an employee is assigned to.
- Allow a VPN connected employee to have the same dialing experience as others in the office who are connected through a gateway.

### **Related topics:**

[Preparing to administer location number on Station screen](#) on page 203

[Setting up location number on Station screen](#) on page 203

## Preparing to administer location number on Station screen

---

On the Optional Features screen, ensure that the **Multiple Locations** field is set to `y`. If this field is set to `n`, your system is not enabled for the Administer location per station feature. Contact your Avaya representative for assistance.



### Note:

If the **Multiple Locations** field on the Optional Features screen is set to `n`, the **Location** field on the Station screen is hidden.

To view the Optional Features screen, type `display system-parameters customer-options`. Press `Enter`.

For a complete description of the many Optional Features screens, see *Administering Avaya Aura™ Communication Manager*, 03-300509.

## Setting up location number on Station screen

---

1. Enter `change station n`, where `n` is the extension number to which you want to assign a location.
2. In the **Location** field, enter a valid location number.  
This field appears only when the **Type** field is set to H.323 or SIP.
3. Select `Enter` to save your changes.



### Note:

If the station extension is a SIP telephone type and if the application type is OPS on the Stations with Off-PBX Telephone Integration screen, then the Off-PBX screen's **Location** field is display-only and displays the value of the **Location** field of the corresponding Station screen.

---

## Telephone Features

Once you add a telephone to the system, you can use the Station screen to change the settings for the telephone, such as adding or changing feature button assignments. The system allows you to assign features or functionality to each programmable button. It is up to you to decide which features you want for each telephone and which feature you want to assign to each button. If you have 6400-series telephones, your users can administer some of their own feature buttons. See *Setting up Terminal Self-Administration* for more information.



### Note:

An NI-BRI telephone with Communication Manager has only the **Conference**, **Transfer**, **Hold**, and **Drop** feature buttons, none of which requires administration. On an NI-BRI

telephone, you can assign additional feature buttons only as call appearances. As a result, NI-BRI telephone users must access all other features of Communication Manager using feature access codes. Additionally, the number of call appearance buttons administered in Communication Manager (the default is three) must match the number of call appearances programmed on the telephone. Finally, Communication Manager does not support bridged call appearances for NI-BRI telephones.

## Adding feature buttons

---

1. Type `change station nnnn` where `nnnn` is the extension for the telephone you want to modify.
2. Press `Enter`.
3. Press `Next Page` until you locate the **Button Assignment** section of the Station screen.

Some telephones have several feature button groups. Make sure that you are changing the correct button. If you do not know which button on the telephone maps to which button-assignment field, see your telephone's manual, or see *Telephone Reference*.

4. Enter the button name that corresponds to the feature you want to assign a feature button. To determine feature button names, press `Help`, or refer to *Telephone Feature Buttons Table*.

 **Note:**

For certain newer telephones with expanded text label display capabilities, you can customize feature button labels to accept up to 13 alphanumeric characters. For more information about this feature, see *Increasing Text Fields for Feature Buttons*.

5. Press `Enter` to save your changes.

Some telephones have default assignments for buttons. For example, the 8411D includes defaults for 12 softkey buttons. It already has assignments for features like Leave Word Calling and Call Forwarding. If you do not use an alias, you can easily assign different features to these buttons if you have different needs. If you use an alias you must leave the default softkey button assignments. The system allows you to change the button assignments on the screen and the features work on the alias telephone, however the labels on the display do not change.

---

### Related topics:

[Increasing Text Fields for Feature Buttons](#) on page 205

[Telephone Feature Buttons Table](#) on page 206

## Increasing Text Fields for Feature Buttons

If you are using certain newer phones with expanded text label display capabilities, the Increase Text Fields for Feature Buttons feature allows you to program and store up to 13 character labels for associated feature buttons and call appearances. This feature is available for the following telephones:

- 2410 (Release 2 or newer)
- 2420 (Release 4 or newer)
- 4610 (IP Telephone Release 2.2 or later)
- 4620 (IP Telephone Release 2.2 or later)
- 4621 (IP Telephone Release 2.2 or later)
- 4622 (IP Telephone Release 2.2 or later)
- 4625 (IP Telephone Release 3.1 or later)

### Related topics:

[Adding feature buttons](#) on page 204

[Telephone Feature Buttons Table](#) on page 206

## Enabling extended text fields for feature buttons

To enable extended text fields for feature buttons:

- 
1. Type `add station next` or `change station nnnn`, where `nnnn` is the extension of the telephone you want to customize feature button labels for. The Station screen appears.
  2. Ensure that **Customizable Labels** is set to `y`.  
This allows the user to enter 13-character labels for all feature buttons and call appearances associated with this station.
  3. Press `Enter` to save your changes
  4. Assign specific feature buttons as described in *Adding Feature Buttons*.

 **Note:**

You can also use the existing Abbreviated Dialing (AD) button type (Abr Program) to program AD labels. However, if you choose to utilize the Abr Program button to program AD labels, you are limited to 5 upper case characters. For more information on Abbreviated Dialing, see *Adding Abbreviated Dialing Lists*.

---

## Restricting customization of feature button types

In order to manage the usage of your system's allocation of customized button labels to ensure that VIP users have the button label customization resource available to them, you can restrict button label customization of up to 50 specified button types for users who are not considered to be VIP users. To restrict customization of specific feature button types:

- 
1. Type `change button-restriction`.  
The Button Type Customization Restrictions screen appears.
  2. Ensure that **Restrict Customization Of Button Types** is set to `y`.
  3. In the fields under Restrict Customization Of Labels For The Following Button Types, enter the button type you want to restrict users from customizing.

 **Note:**

When you enter the special button types `abr-spchar` or `abr-dial`, an additional field appears to the right of the button type as shown in Figure 45. Use this special field to specify the special character associated with the `abr-spchar` button type or the **Abbreviated Dialing List** associated with the `abr-dial` button type.

4. Press `Enter` to save your changes.
- 

## Telephone Feature Buttons Table

The following table provides descriptions of the feature buttons that you can administer on multiappearance telephones. It also lists the administrable software names and recommended button label names. **Display** buttons support telephones equipped with alphanumeric displays. Note that some buttons might require 1-lamp or 2-lamp buttons. Some buttons are not allowed on some systems and on some telephones.

 **Note:**

An NI-BRI telephone with Communication Manager has only the **Conference**, **Transfer**, **Hold**, and **Drop** feature buttons, none of which requires administration. On an NI-BRI telephone, you might assign additional feature buttons only as call appearances. As a result, NI-BRI telephone users must access all other features of Communication Manager using feature access codes.

Additionally, the number of call appearance buttons administered in Communication Manager (the default is three) must match the number of call appearances programmed on the telephone.

Finally, Communication Manager does not support bridged call appearances for NI-BRI telephones.

Table 2: Telephone Feature Buttons

| Button Name                 | Button Label   | Description  | Maximum                     |
|-----------------------------|----------------|--|-----------------------------|
| #                           | AD             | You can administer the # button as an autodial feature button by entering the Audix number in the <b>BUTTON ASSIGNMENTS</b> field on the Station screen.   | 1 per station               |
| abr-prog                    | Abr Program    | Abbreviated Dialing Program: allows users to program abbreviated dialing and autodial buttons or to store or change numbers in a personal list or group list associated with the station   | 1 per station               |
| abr-spchar                  | AbvDial (char) | Abbreviated Dialing Special Character: allows users to enter an associated special character [~, ~m (mark), ~p (pause), ~s (suppress), ~w (wait for dial tone), or ~W (wait forever)] when programming   | 1 each per station          |
| abrdg-appr (Ext: ____)      | (extension)    | Bridged Appearance of an analog telephone: allows the user to have an appearance of a single-line telephone extension. Assign to a 2-lamp appearance button.   | Depends on station type     |
| abrv-dial (List: __ DC: __) | AD             | Abbreviated Dialing: dials the stored number on the specified abbreviated dialing list. List: specify the list number 1 to 3 where the destination number is stored DC: specify the dial code for the destination number   | 1 per AD list per dial code |
| abrv-ring                   | AbRng          | Abbreviated and Delayed Ringing: allows the user to trigger an abbreviated or delayed transition for calls alerting at an extension  |                             |
| ac-alarm                    | AC Alarm       | Administered Connection alarm notification: allows the user to monitor when the number of failures for an administered connection has met the specified threshold.   | 1 per station               |
| aca-halt                    | Auto-Ckt Halt  | Automatic Circuit Assurance (display button): allows users of display telephones to identify trunk malfunctions. The system automatically initiates a referral call to the telephone when a possible failure occurs. When the user presses ACA Halt, the system turns off ACA monitoring for the entire system. The user must press ACA Halt again to restart monitoring | 1 per system                |
| account                     | Account        | Account: allows users to enter Call Detail Recording (CDR) account codes. CDR account codes allow the system to associate  | 1 per station               |

| Button Name           | Button Label  | Description  | Maximum           |
|-----------------------|---------------|--|-------------------|
|                       |               | and track calls according to a particular project or account number.   |                   |
| admin                 | Admin         | Administration: allows a user to program the feature buttons on their 6400-series telephone.   | 1 per station     |
| after-call<br>Grp:___ | AfterCall     | After Call Work Mode: allows an agent to temporarily be removed from call distribution in order for the agent to finish ACD-related activities such as completing paperwork.<br>Grp: specify the ACD split group number. | 1 per split group |
| alrt-agchg            | Alert Agent   | Alert Agent: indicates to the agent that their split/skill hunt group changed while active on a call. This button blinks to notify the agent of the change.  | 1 per station     |
| alt-frl               | Alternate FRL | Alternate Facility Restriction Level (FRL): activates or deactivates an alternate facility restriction level for the extension.  | 1 per system      |
| ani-request           | ANI Request   | Automatic Number Identification Request: allows the user to display the calling party's number from incoming trunks during the voice state of call. The trunk must support this functionality.                           | 1 per station     |
| assist<br>(Group: __) | Assist        | Supervisory Assistance: used by an ACD agent to place a call to a split supervisor.<br>Group: specify the ACD split group number.  | 1 per split group |
| asvn-halt             | ASVN Halt     | Authorization Code Security Violation Notification: activates or deactivates call referral when an authorization code security violation is detected.  | 1 per system      |
| atd-qcalls            | AttQueueCall  | Attendant Queue Calls (display button): tracks the number of calls in the attendant group's queue and displays the queue status. Assign this button to any user who you want to backup the attendant.                    | 1 per station     |
| atd-qtime             | AttQueueTime  | Attendant Queue Time (display button): tracks the calls in the attendant group's queue according to the oldest time a call has been queued, and obtains a display of the queue status.                                   | 1 per station     |
| audix-rec             | Audix Record  | Audix One-Step Recording (display button): activates/deactivates recording of the current call. An Audix hunt group extension that is  | 1 per station     |

| Button Name                         | Button Label           | Description  | Maximum                      |
|-------------------------------------|------------------------|--|------------------------------|
|                                     |                        | valid for the user must be entered in the Ext: field after the name.   |                              |
| aut-msg-wt<br>(Ext: __)             | Msg (name or ext #)    | Automatic Message Waiting: associated status lamp automatically lights when an LWC message has been stored in the system for the associated extension (can be a VDN). This lamp will not light on the mapped-to physical station for messages left for virtual extensions.   | 1 per aut-<br>mst-ex t       |
| auto-cback                          | Auto<br>CallBack       | Automatic Call Back: when activated, allows inside user who placed a call to a busy or unanswered telephone to be called back automatically when the called telephone becomes available to receive a call.   | 1 per station                |
| auto-icom<br>(Group: __)            | Autoic (name or ext #) | Automatic Intercom: places a call to the station associated with the button. The called user receives a unique alerting signal, and a status lamp associated with a Intercom button flashes. Grp: Intercom — Auto-Icom group number. This extension and destination extension must be in the same group.   | 1 per group<br>per dial code |
| auto-in<br>(Group: __)              | Auto in                | Auto-In Mode: allows the user to become automatically available for new ACD calls upon completion of an ACD call. Grp: The split group number for ACD.   | 1 per split<br>group         |
| auto-wkup                           | Auto Wakeup            | Automatic Wakeup (display button): allows attendants, front-desk users, and guests to request a wakeup call to be placed automatically to a certain extension (cannot be a VDN extension) at a later time.   | 1 per station                |
| autodial                            | SD                     | Allows a user to dial a number that is not part of a stored list.  |                              |
| aux-work<br>(RC: __)<br>(Group: __) | AuxWork                | Auxiliary Work Mode: removes agent from ACD call distribution in order to complete non-ACD-related activities. RC: Optional assignment for the 1- or 2-digit Reason Code to be used to change to Aux Work using this button, when Reason Codes is active. Multiple Aux Work buttons, each with a different RC, can be assigned to the same station set. Grp: The split group number for ACD. | 1 per split<br>group         |

| Button Name                    | Button Label | Description   | Maximum                 |
|--------------------------------|--------------|---|-------------------------|
| brdg-appr<br>(Btn: __ Ext: __) | (extension)  | Bridged Call Appearance: provides an appearance of another user's extension on this telephone. For example, an assistant might have a bridged appearance of their supervisor's extension. The bridged appearance button functions exactly like the original call appearance, for instance it indicates when the appearance is active or ringing. You can assign brdg-appr buttons only to 2-lamp appearance buttons. You must indicate which extension and which call appearance button the user wants to monitor at this telephone.  | Depends on station type |
| btn-ring                       | Button Ring  | Station User Button Ring Control: allows users to toggle between audible and silent call alerting.  | 1 per station           |
| btn-view                       | Button View  | Button View: allows users to view, on the telephone's display, the contents of any feature button. Button View does more than the "View" or "stored-num" feature button; these only display what is contained in abbreviated dialing and autodial buttons. When the user presses the btn-view button and then a specific feature button, they see the feature name and any auxiliary data for that button. This allows users to review the programming of their feature buttons. You can assign this soft-key button to any 6400-, 7400-, or 8400-series display telephone. |                         |
| busy-ind<br>(TAC/Ext: __)      | Busy         | Busy Indication: indicates the busy or idle status of an extension, trunk group, terminating extension group (TEG), hunt group, or loudspeaker paging zone. Users can press the busy-ind button to dial the specified extension. You can assign this button to any lamp button and must specify which Trunk or extension the user wants to monitor.   | 1 per TAC/Ext           |
| call-appr                      | extension    | Call Appearance: originates or receives calls. Assign to a 2-lamp appearance button.  | Depends on station type |
| call-disp                      | Return Call  | Call Displayed Number (display button): initiates a call to the currently displayed number. The number can be from a leave word calling message or a number the user retrieved from the Directory.  | 1 per station           |

| Button Name         | Button Label                           | Description   | Maximum          |
|---------------------|--|---|------------------|
| call-fwd (Ext: ___) | CFrwd (Ext #) Call Forward (no ext #)  | Activates or deactivates Call Forwarding All Calls.   | 64 per extension |
| call-park           | Call Park                              | Allows the user to place the current call in the call park state so it can be retrieved from another telephone.   | 1 per station    |
| call-pkup           | Call Pickup                            | Allows the user to answer a call that is ringing in the user's pickup group.  | 1 per station    |
| call-timer          | Call Timer                             | Used only on the 6400 sets. Allows users to view the duration of the call associated with the active call appearance button   | 1 per station    |
| call-unpk           | Unpark Call                            | Allows the user to unpark a call from another telephone than the telephone that originally parked the call. This feature button applies only to the SIP station types.  | 1 per station    |
| callr-info          | Caller Info                            | (display button) Used with Call Prompting to allow users to display information collected from the originator.  | 1 per station    |
| cas-backup          | CAS Backup                             | Centralized Attendant Service Backup: used to redirect all CAS calls to a backup extension in the local branch if all RLTs are out-of-service or maintenance busy. The associated status lamp indicates if CAS is in the backup mode. | 1 per station    |
| cdr1-alm            | CDR 1 Fail                             | CDR Alarm: associated status lamp is used to indicate that a failure in the interface to the primary CDR output device has occurred.  | 1 per station    |
| cdr2-alm            | CDR 2 Fail                             | CDR Alarm: associated status lamp is used to indicate that a failure in the interface to the secondary CDR output device has occurred.  | 1 per station    |
| cfwd-bsyda          | CFBDA                                  | Call Forward Busy/Don't Answer: activates and deactivates call forwarding for calls when the extension is busy or the user does not answer.   | 64 per extension |
| cfwd-enh            | ECFwd (ext #) Enhanced Cfwd (no ext #) | Call Forwarding - Enhanced allows the user to specify the destination extension for both internal and external calls.   |                  |
| check-in            | Check In                               | Check In (display button): changes the state of the associated guest room to occupied and   | 1 per station    |

| Button Name | Button Label | Description   | Maximum       |
|-------------|--------------|---|---------------|
|             |              | turns off the outward calling restriction for the guest room's station.   |               |
| check-out   | Check Out    | Check Out (display button): Changes the state of the associated guest room to vacant and turns on the outward calling restriction for the guest room's station. Also clears (removes) any wake-up request for the station.  | 1 per station |
| clk-overid  | ClkOverride  | Clocked Manual Override (display button): Used only by authorized attendants and system administrators, in association with Time of Day Routing, to override the routing plan in effect for the system. The override is in effect for a specified period of time. This feature can only be assigned to display telephones.  | 1 per station |
| conf-dsp    | Conf Display | Allows a user to display information about each party of a conference call. This button can be assigned to stations and attendant consoles.   | 1 per station |
| consult     | Consult      | The Consult button allows a covering user, after answering a coverage call, to call the principal (called party) for private consultation. Activating Consult places the caller on hold and establishes a private connection between the principal and the covering user. The covering user can then add the caller to the conversation, transfer the call to the principal, or return to the caller. | 1 per station |
| cov-cback   | CovrCallBack | Allows a covering party to store a leave word calling message for the principal (called party).   | 1 per station |
| cov-msg-rt  | Covr Msg Ret | Coverage Message Retrieval (display button): places a covering station into the message retrieval mode for the purposes of retrieving messages for the group.   | 1 per station |
| cpn-blk     | CPN Block    | Blocks the sending of the calling party number for a call.  | 1 per station |
| cpn-unblk   | CPN Unblock  | Deactivates calling party number (CPN) blocking and allows the CPN to be sent for a single call.  | 1 per station |

| Button Name          | Button Label      | Description   | Maximum                        |
|----------------------|-------------------|---|--------------------------------|
| crss-alert           | Crisis Alert      | Crisis Alert (display button): provide this button to the telephones or consoles that you want to notify when any user makes an emergency call. (You define which calls are emergency calls on the AAR/ARS Analysis screen by setting the Call Type to alrt.) After a user receives an alert, they can press the crss-alert button to disable the current alert. If tenant partitioning is active, the attendants within a partition can receive emergency notification only from callers in the same partition.  | 1 per station<br>10 per system |
| data-ext             | Data (data ext #) | Data Extension: sets up a data call. Can be used to pre-indicate a data call or to disconnect a data call. Cannot be a VDN or ISDN-BRI extension.   | 1 per data extension group     |
| date-time            | Time/Date         | Date and Time (display button): displays the current date and time. Do not assign this button to 6400-series display telephones as they normally show the date and time.  | 1 per station                  |
| delete-msg           | Delete Msg        | Delete message (display button): deletes a stored LWC message or wakeup request.  | 1 per station                  |
| dial-icom (Grp: ___) | Dial Icom         | Dial Intercom: accesses the intercom group assigned to the button. Grp: Intercom — Dial (Dial Icom) group number.   | 1 per group                    |
| did-remove           | DID Remove        | DID Remove (display button): allows DID assignments to be removed.  | 1 per station                  |
| did-view             | DID View          | DID View (display button): allows DID assignments to be displayed and changed. Allows choice between XDID and XDIDVIP numbers   | 1 per station                  |
| directory            | Directory         | Directory (display button): allows users with display telephones to access the integrated directory, use the touch-tone buttons to key in a name, and retrieve an extension from the directory. The directory contains the names and extensions that you have assigned to the telephones administered in your system. If you assign a directory button, you should also assign a Next and Call-Disp button to the telephone. These buttons allow the user to navigate within the integrated directory and call an extension once they find the correct one. | 1 per station                  |

| Button Name | Button Label  | Description  | Maximum       |
|-------------|---------------|--|---------------|
|             |               |  <b>Note:</b><br>Vector Directory Numbers do not appear in the integrated directory. Also, if you assign a name beginning with two tildes (~~) to a telephone, and Display Character Set on the System Parameters Country-Options screen is set to Roman, the name does not appear in the integrated directory. Note that this is the only way to hide a name in the integrated directory.  |               |
| dir-pkup    | Dir Pickup    | Directed call pickup: allows the user to answer a call ringing at another extension without having to be a member of a pickup group.   |               |
| disp-chrg   | Disp Charges  | Provides your display telephone with a visual display of accumulated charges on your current telephone call. Used exclusively outside the U.S. and Canada.   | 1 per station |
| disp-norm   | Local/ Normal | Normal (display button): Toggles between LOCAL display mode (displays time and date) and NORMAL mode (displays call-related data). LED off = LOCAL mode and LED on = NORMAL.   | 1 per station |
| dn-dst      | DoNotDisturb  | Places the user in the do not disturb mode.  | 1 per station |
| drop        | Drop          | Allows users to drop calls. Users can drop calls from automatic hold or drop the last party they added to a conference call.   |               |
| ec500       | EC500         | Administers an Extension to Cellular feature button on the office telephone. When you enter this value, the Timer subfield displays, and defaults to n. Set the optional <b>Timer</b> subfield to y to include an Extension to Cellular timer state for the administered feature button. When the timer state is included, the Extension to Cellular user can activate a one-hour timer to temporarily disable Extension to Cellular through this administered feature button. Leaving the default setting of n excludes the timer state | 1 per station |
| exclusion   | Exclusion     | Exclusion: allows multiappearance telephone users to keep other users with appearances of the same extension from bridging onto an existing call. If the user  | 1 per station |

| Button Name | Button Label         | Description   | Maximum       |
|-------------|----------------------|---|---------------|
|             |                      | <p>presses the Exclusion button while other users are already bridged onto the call, the other users are dropped. There are two means of activating exclusion.</p> <ul style="list-style-type: none"> <li>• Manual Exclusion — when the user presses the Exclusion button (either before dialing or during the call).</li> <li>• Automatic Exclusion — as soon as the user picks up the handset. To turn off Automatic Exclusion during a call, the user presses the Exclusion button.</li> </ul> <p>To use Automatic Exclusion, set the <b>Automatic Exclusion by COS</b> field to <math>\bar{y}</math> on the Feature-Related System Parameters screen.</p> |               |
| ext-dn-dst  | ExtDoNotDisturb      | Extension — Do Not Disturb (display button): used by the attendant console or hotel front desk display telephone to activate do not disturb and assign a corresponding deactivate time to an extension.   | 1 per station |
| ext-pkup    | Call Pickup Extended | Allows the user to answer calls directly from another call pickup group. This feature button applies only to the SIP station types.   | 1 per station |
| extnd-call  | Extend Call          | Allows the user to extend the current call to an Off-PBX/EC500 telephone  | 1 per station |
| fe-mute     | fe-mute Far End Mute | Allows a user to mute a selected party on a conference call. This button can be assigned to stations and attendant consoles.  | 1 per station |
| flash       | Flash                | 1) Allows a station on a trunk call with Trunk Flash to send a Trunk Flash signal to the far end (e.g., Central Office); 2) allows a station on a CAS main call to send a Trunk Flash signal over the connected RLT trunk back to the branch to conference or transfer the call.  | 1 per station |
| goto-cover  | Goto Cover           | <p>Go To Coverage: sends a call directly to coverage instead of waiting for the called inside-user to answer. Go to Cover forces intercom and priority calls to follow a coverage path.</p> <p> <b>Note:</b><br/>Go to Cover cannot be activated for calls placed to a Vector Directory Number</p>   | 1 per station |

| Button Name                           | Button Label                                      | Description   | Maximum                    |
|---------------------------------------|---|---|----------------------------|
|                                       |   | extension. Go to Cover can be used to force a call to cover to a VDN if the called principal has a VDN as a coverage point.   |                            |
| grp-dn-dst                            | GrpDoNotDs<br>trb                                 | Group Do Not Disturb (display button): places a group of telephones into the do not disturb mode.   | 1 per station              |
| grp-page<br>(Number:____<br>)         | GrpPg   | Allows users to make announcements to groups of stations by automatically turning on their speakerphones. Number: The extension of the page group.  |                            |
| headset                               | Headset   | Signals onhook/offhook state changes to Communication Manager. The green LED is on for offhook state and off (dark) for onhook state.   | 1 per station              |
| hunt-ns (Grp:<br>____)                | HuntNS  | Hunt-Group Night Service: places a hunt-group into night service. Grp: Hunt group number.   | 3 per hunt group           |
| in-call-id<br>(Type: __<br>Grp: ____) | INCallID<br>(group #,<br>type, name,<br>or ext #) | The Coverage Incoming Call Identification (ICI) button allows a member of a coverage answer group or hunt group to identify an incoming call to that group even though the member does not have a display telephone. In the Type field, enter c for coverage answer groups and type of h for a hunt group. In the Grp field, enter the group number.  | 1 per group-type per group |
| inspect                               | Inspect   | Inspect (display button): allows users on an active call to display the identification of an incoming call. Inspect also allows users to determine the identification of calls they placed on Hold.   | 1 per station              |
| Inst-trans                            | Instant<br>Transfer                               | An Instant Transfer button does an instant transfer by performing an immediate unsupervised transfer to the button's administered destination. The Instant Transfer button is intended for transfer to Polycom room systems, which are capable of hosting a conference and auto-answering calls as well. The Instant Transfer button is not limited to video set-types; however, it may be useful on other set-types as well. | 1 per station              |
| int-aut-an                            | IntAutoAnsw<br>er                                 | Internal Automatic Answer: causes any hybrid or digital station to automatically answer incoming internal calls.  | 1 per station              |

| Button Name             | Button Label             | Description   | Maximum                                    |
|-------------------------|--------------------------|---|--|
| last-numb               | LastNumb Dialed          | Last Number Dialed (redial): originates a call to the number last dialed by the station.  | 1 per station                              |
| lic-error               | License Error            | License-Error: indicates a major License File alarm. Pressing the button does not make the light go out. The button goes out only after the error is cleared and Communication Manager returns to License-Normal Mode. You can administer this button on telephones and attendant consoles.   | 1 per telephone 20 per system (Server CSI) |
| limit-call              | LimitInCalls             | Limit Number of Concurrent Calls feature: allows user to limit the number of concurrent calls at a station to one call, where normally multiple call appearances can terminate at the station.  | 1 per station                              |
| link-alarm (link# ____) | Link Fail (link #)       | Link Alarm: associated status lamp indicates that a failure has occurred on one of the Processor Interface circuit pack data links. Link: Link number — 1 to 8 for multi-carrier cabinets or 1 to 4 for single-carrier cabinets.  | 8 per station                              |
| lsvn-halt               | LSVN Halt                | Login Security Violation Notification: activates or deactivates referral call when a login security violation is detected.  | 1 per system                               |
| lwc-cancel              | Cancel LWC               | Leave Word Calling Cancel: cancels the last leave word calling message originated by the user.  | 1 per station                              |
| lwc-lock                | Lock LWC                 | Leave Word Calling Lock: locks the message retrieval capability of the display module on the station.   | 1 per station                              |
| lwc-store               | Store LWC                | Leave Word Calling Store: leaves a message for the user associated with the last number dialed to return the call to the originator.  | 1 per station                              |
| major-alm               | Major Alarm              | Major Alarm: assign to a status lamp to notify the user when major alarms occur. Major alarms usually require immediate attention.  | 1 per station                              |
| man-msg-wt (Ext: ____)  | Msg Wait (name or ext #) | Manual Message Waiting: allows a multiappearance telephone user to press a button on their telephone in order to light the Manual Message Waiting button at another telephone. You can administer this feature only to pairs of telephones, such as an assistant and an executive. For example, an assistant can press the man-msg-wt button to signal the executive that they have a call. | None                                       |

| Button Name              | Button Label         | Description   | Maximum           |
|--------------------------|----------------------|---|-------------------|
| man-overid<br>(TOD: _)   | ManOverride          | Immediate Manual Override (display button): allows the user (on a system with Time of Day Routing) to temporarily override the routing plan and use the specified TOD routing plan. TOD: specify the routing plan the user wants to follow in override situations.  | 1 per station     |
| manual-in<br>(Group: __) | Manual In            | Manual-In Mode: prevents the user from becoming available for new ACD calls upon completion of an ACD call by automatically placing the agent in the after call work mode. Grp: The split group number for ACD.   | 1 per split group |
| mct-act                  | MCT Activate         | Malicious Call Trace Activation: sends a message to the MCT control extensions that the user wants to trace a malicious call. MCT activation also starts recording the call, if your system has a MCT voice recorder.   | 1 per station     |
| mct-contr                | MCT Control          | Malicious Call Trace Control: allows the user to take control of a malicious call trace request. Once the user becomes the MCT controller, the system stops notifying other MCT control extensions of the MCT request. NOTE: To add an extension to the MCT control group, you must also add the extension on the Extensions Administered to have an MCT-Control Button screen. When the user presses the MCT Control button, the system first displays the called party information. Pressing the button again displays the rest of the trace information. The MCT controller must dial the MCT Deactivate feature access code to release control. | 1 per station     |
| mf-da-intl               | Directory Assistance | Multifrequency Operator International: allows users to call Directory Assistance.   | 1 per station     |
| mf-op-intl               | CO attendant         | Multifrequency Operator International: allows users to make international calls to the CO attendant.  | 1 per station     |
| mj/mn-almr               | Mj/Mn Alarm          | Minor Alarm: assign to a status lamp to notify the user when minor or major alarms occur. Minor alarms usually indicate that only a few trunks or a few stations are affected.  | 1 per station     |
| mm-basic                 | MM Basic             | Multimedia Basic: used to place a multimedia complex into the "Basic" mode or to return it to the "Enhanced" mode   | 1 per station     |

| Button Name | Button Label  | Description  | Maximum          |
|-------------|---------------|--|------------------|
| mm-call     | MM Call       | Multimedia Call: used to indicate a call is to be a multimedia call.   | 1 per station    |
| mm-cfwd     | MM Call Fwd   | Multimedia Call Forward: used to activate forwarding of multimedia calls as multimedia calls, not as voice calls.  | 1 per station    |
| mm-datacnf  | MM Data Cnf   | Multimedia Data Conference: used to initiate a data collaboration session between multimedia endpoints; requires a button with a lamp.   | 1 per station    |
| mm-multnbr  | MM Mult Nbr   | Indicate that the user wants to place calls to 2 different addresses using the 2 B-channels.   | 1 per station    |
| mm-pcaudio  | MM PC Audio   | Switches the audio path from the telephone (handset or speakerphone) to the PC (headset or speakers/ microphone).  | 1 per station    |
| msg-retr    | Msg Retrieve  | Message Retrieval (display button): places the station's display into the message retrieval mode.  | 1 per station    |
| mwn-act     | MsgWaitAct    | Message Waiting Activation: lights a message waiting lamp on an associated station.  | 1 per station    |
| mwn-deact   | MsgWaitDeact  | Message Waiting Deactivation: dims a message waiting lamp on an associated station.  | 1 per station    |
| next        | Next          | Next (display button): steps to the next message when the telephone's display is in Message Retrieval or Coverage Message Retrieval mode. Shows the next name when the telephone's display is in the Directory mode. | 1 per station    |
| night-serv  | Night Service | Night Service Activation: toggles the system in or out of Night Service mode.  | 1 per station    |
| noans-ahrt  | NoAnsAirt     | Redirection on No Answer Alert: indicates a Redirection on No Answer timeout has occurred for the split.   | 1 per hunt group |
| no-hld-cnf  | No Hold Conf  | No Hold Conference: can automatically conference another party while continuing the existing call.   | 1 per station    |
| normal      | Normal        | Normal (display button): places the station's display into normal call identification mode.  | 1 per station    |

| Button Name           | Button Label                | Description  | Maximum                      |
|-----------------------|-----------------------------|--|------------------------------|
| off-bd-alm            | OffBoardAlarm               | Off board Alarm: associated status lamp lights if an off-circuit pack major, minor, or warning alarm is active on a circuit pack. Off-board alarms (loss of signal, slips, misframes) relate to problems on the facility side of the DS1, ATM, or other interface. | 1 per attendant              |
| per-COLine (Grp: ___) | COLine (line #)             | Personal CO Line: allows the user to receive calls directly via a specific trunk. Grp: CO line group number.   | 1 per group                  |
| pms-alarm             | PMS Failure                 | Property Management System alarm: associated status lamp indicates that a failure in the PMS link occurred. A major or minor alarm condition raises the alarm.   | 1 per station                |
| post-msgs             | Posted MSGs                 | Posted Messages: Allows the user to display a specific message to callers.   | 1 per station                |
| pr-awu-alm            | pr-awu-alm<br>AutoWakeAlarm | Automatic Wakeup Printer Alarm: associated status lamp indicates that an automatic wakeup printer interface failure occurred.  | 1 per station                |
| pr-pms-alm            | PMS Ptr Alarm               | PMS Printer Alarm: associated status lamp indicates that a PMS printer interface failure occurred.   | 1 per station                |
| pr-sys-alm            | Sys Ptr Alarm               | System Printer Alarm: associated status lamp indicates that a system printer failure occurred.   | 1 per station                |
| print-msgs            | Print Msgs                  | Print Messages: allows users to print messages for any extension by pressing the button and entering the extension and a security code.  | 1 per station                |
| priority              | Priority Call               | Priority Calling: allows a user to place priority calls or change an existing call to a priority call.   | 1 per station                |
| q-calls (Grp: ___)    | QueueCall                   | Queue Calls: associated status lamp flashes if a call warning threshold has been reached. Grp: Group number of hunt group.   | 1 per hunt group per station |
| q-time (Grp: ___)     | QueueTime                   | Queue Time: associated status lamp flashes if a time warning threshold has been reached. Grp: Group number of hunt group.  | 1 per hunt group per station |
| release               | Release                     | Releases an agent from an ACD call.  | 1 per station                |
| ring-stat             | Ringer Status               | Users can display the ringer status for a line or bridged appearance by pressing the ring-stat button followed by a call-appr, brdg-   | 1 per station                |

| Button Name               | Button Label  | Description   | Maximum          |
|---------------------------|---------------|---|------------------|
|                           |               | appr or abrdg-appr button. Depending on the ringer status, the display shows <ul style="list-style-type: none"> <li>• Ringer On</li> <li>• Ringer Off</li> <li>• Ringer Delayed</li> <li>• Ringer Abbreviated</li> </ul>  |                  |
| ringer-off                | Ringer Off    | Ringer-Cutoff: silences the alerting ringer on the station.   | 1 per station    |
| rs-alert                  | ResetAlert    | The associated status lamp lights if a problem escalates beyond a warm start.   | 1 per station    |
| rsvn-halt                 | RSVN Halt     | Remote Access Barrier Code Security Violation Notification Call: activates or deactivates call referral when a remote access barrier code security violation is detected.   | 1 per station    |
| scroll                    | Scroll        | Scroll (display button): allows the user to select one of the two lines (alternates with each press) of the 16-character LCD display. Only one line displays at a time.   | 1 per station    |
| send-calls<br>(Ext: ____) | SAC (ext #)   | Send All Calls allows users to temporarily direct all incoming calls to coverage regardless of the assigned call-coverage redirection criteria. Assign to a lamp button.  | 64 per extension |
| send-term                 | Send TEG      | Send All Calls For Terminating Extension Group: allows the user to forward all calls directed to a terminating extension group.   | 1 per TEG        |
| serv-obsrv                | Service Obsrv | Service Observing: activates Service Observing. Used to toggle between a listen-only and a listen-talk mode.  | 1 per station    |
| share-talk                | Share Talk    | Share Talk: enables multiple DCP or H323 IP endpoints that are registered to the same extension to share talk capability. Normally, when more than one endpoint requests RTP (Real Time Transfer Protocol) media, only one of the endpoints (Base Set) is capable of talking and listening, while the other endpoints are connected in listen-only mode. This button allows all the endpoints that are associated with the extension to share the talk capability. Note that in Communication Manager 5.0, only AE Server DMCC (Device, | 1 per station    |

| Button Name         | Button Label         | Description  | Maximum                   |
|---------------------|----------------------|--|---------------------------|
|                     |                      | Media, and Call Control) endpoints are capable of requesting RTP while they are sharing control of the extension. For more information on DMCC, see <i>Avaya MultiVantage® Application Enablement Services Administration and Maintenance Guide, 02-300357</i> .   |                           |
| signal (Ext: ___)   | Sgnl (name or ext #) | Signal: allows the user to use one button to manually signal the associated extension. The extension cannot be a VDN extension.  | 1 per signal extension    |
| ssvn-halt           | SSVN Halt            | Toggle whether or not station security code violation referrals are made to the referral destination.  | 1 per station             |
| sta-lock            | Station Lock         | When Station Lock is enabled, the only calls that can be made from the station are those allowed by the COR administered in the Station Lock COR field.  | 1 per station             |
| start-bill          | Start Bill           | After an ACD agent answers a call, the agent can press this button to send an ISDN CONNECT message to the PSTN network to start the PSTN call-billing for a call at the PSTN switch.   | 1 per station             |
| stored-num          | Stored Number        | Enables a display mode that displays the numbers stored in buttons.  | 1 per station             |
| stroke-cnt (Code:_) | Stroke Count (#)     | Automatic Call Distribution Stroke Count # (0, 1, 2, 3, 4, 5, 6, 7, 8, or 9) sends a message to CMS to increment a stroke count number.  | Upto 10 per station       |
| team                | Team                 | The Team Button has two generic functions, a display function and an execution function. The display function allows any member of a team (monitoring station) to observe the station state of other team members (monitored station). As an execution function, the Team Button can be used as Speed Dial Button or Pick-Up Button where a call to the monitored station is established directly or a ringing call is picked from the monitored station. Ext: This field appears when you enter the button type team. Enter the extension of the principal station of the virtual "team." Rg This field appears when you enter the button type team. Enter the kind of audible ringing for the team button. Valid | 15 per monitoring station |

| Button Name             | Button Label                 | Description   | Maximum           |
|-------------------------|------------------------------|---|-------------------|
|                         |                              | entries are a(bbbreviated), d(elayed), n(o-ring), and r(ing).   |                   |
| term-x-gr<br>(Grp: ___) | TermGroup<br>(name or ext #) | Terminating Extension Group: provides one or more extensions. Calls can be received but not originated with this button. Grp: TEG number.   | 1 per TEG         |
| timer                   | Timer                        | Used only on the 6400 sets. Allows users to view the duration of the call associated with the active call appearance button   | 1 per station     |
| togle-swap              | Toggle-Swap                  | Allows a user to toggle between two parties before completing a conference or a transfer  | 1 per station     |
| trk-ac-alm              | FTC Alarm                    | Facility Test Call Alarm: associated status lamp lights when a successful Facility Test Call (FTC) occurs.  | 1 per station     |
| trk-id                  | Trunk ID                     | Trunk Identification (display button): identifies the tac (trunk access code) and trunk member number associated with a call.   | 1 per station     |
| trunk-name              | Trunk Name                   | (display button) Displays the name of the trunk as administered on the CAS Main or on a server without CAS.   | 1 per station     |
| trunk-ns<br>(Grp: ___)  | Trunk NS                     | Trunk-Group Night Service: places a trunk-group into night service. Grp: Trunk group number.  | 3 per trunk group |
| usr-addbsy              | Add Busy Indicator           | Adds the busy indicator.  | 1 per station     |
| usr-rembsy              | Remove Busy Indicator        | Removes the busy indicator.   | 1 per station     |
| uui-info                | UUI-Info                     | Allows users to see up to 32 bytes of ASAI-related UUI-IE data.   | 1 per station     |
| verify                  | Verify                       | Busy Verification: allows users to make test calls and verify a station or a trunk.   | 1 per station     |
| vip-chkin               | VIP Check In                 | VIP Check-in (display button): allows user to assign the XDIDVIP number to the room extension.  | 1 per station     |
| vip-retry               | VIP Retry                    | VIP Retry: starts to flash when the user places a VIP wakeup call and continues to flash until the call is answered. If the VIP wakeup call is not answered, the user can press the VIP Retry button to drop the call | 1 per station     |

| Button Name                          | Button Label            | Description  | Maximum   |
|--------------------------------------|-------------------------|--|---|
|                                      |                         | and reschedule the VIP wakeup call as a classic wakeup call. To assign this button, you must have both Hospitality and VIP Wakeup enabled.   |   |
| vip-wakeup                           | VIP Wakeup              | VIP Wakeup: flashes when a VIP wakeup reminder call is generated. The user presses the button to place a priority (VIP) wakeup call to a guest. To assign this button, you must have both Hospitality and VIP Wakeup enabled.  | 1 per station   |
| voa-repeat                           | VOA Repeat              | VDN of Origin Announcement. VDN of Origin Announcement must be enabled.  | 1 per station   |
| voice-mail                           | Message                 | This is not an administrable button, but maps to the fixed hard "message" button on newer telephones.  | 1 per station   |
| vu-display<br>(format: __<br>ID: __) | Vu Display #            | VuStats Display: allows the agent to specify a display format for the statistics. If you assign a different VuStats display format to each button, the agent can use the buttons to access different statistics. You can assign this button only to display telephones. format: specify the number of the format you want the button to display ID (optional): specify a split number, trunk group number, agent extension, or VDN extension | limited to the number of feature buttons on the telephone |
| whisp-act                            | whisp-act<br>WhisperAct | Whisper Page Activation: allows a user to make and receive whisper pages. A whisper page is an announcement sent to another extension who is active on a call where only the person on the extension hears the announcement; any other parties on the call cannot hear the announcement.<br>The user must have a class of restriction (COR) that allows intra-switch calling to use whisper paging.  | 1 per station   |
| whisp-anbk                           | WhisperAnbk             | Whisper Page Answerback: allows a user who received a whisper page to respond to the user who sent the page.   | 1 per station   |
| whisp-off                            | WhisperOff              | Deactivate Whisper Paging: blocks other users from sending whisper pages to this telephone.  | 1 per station   |

| Button Name | Button Label | Description   | Maximum       |
|-------------|--------------|---|---------------|
| work-code   | Work Code    | Call Work Code: allows an ACD agent after pressing "work-code" to send up to 16 digits (using the dial pad) to CMS. | 1 per station |

**Related topics:**

[Adding feature buttons](#) on page 204

[Increasing Text Fields for Feature Buttons](#) on page 205

## Abbreviated Dialing Lists

Abbreviated dialing is sometimes called speed dialing. It allows you to dial a short code in place of an extension or telephone number. When you dial abbreviated-dialing codes or press abbreviated-dialing buttons, you access stored numbers from special lists. These lists can be personal (a list of numbers for an individual telephone), group (a department-wide list), system (a system-wide list), or enhanced numbers (allows for a longer list of numbers). The version and type of your system determine which lists are available and how many entries you can have on each list.

 **Note:**

You can designate all group-number lists, system-number lists, and enhanced-number lists as "privileged." Calls automatically dialed from a privileged list are completed without class of restriction (COR) or facility restriction level (FRL) checking. This allows access to selected numbers that some telephone users might otherwise be restricted from manually dialing. For example, a user might be restricted from making long-distance calls. However, you can program the number of a branch office that is long distance into an AD list as privileged. Then, the user can call this office location using AD, while still being restricted from making other long-distance calls.

 **Security alert:**

Privileged group-number, system-number, and enhanced-number lists provide access to numbers that typically would be restricted.

### Setting up a station to access a new group list

We will set up station 4567 so it has access to the new group list

- 
1. Type `change station 4567`.
  2. Press `Enter`.
  3. Press `Next Page` until you see Station screen (page 4), containing the **Abbreviated Dialing List** fields.
  4. Type `group` in any of the **List** fields.
  5. Press `Enter`.

A blank **list number** field appears.

6. Type 3 in the **list number** field.

When you assign a group or personal list, you must also specify the personal list number or group list number.

7. Press `Enter` to save your changes.

The user at extension 4567 can now use this list by dialing the feature access code for the list and the dial code for the number they want to dial. Alternatively, you can assign an abbreviated dialing button to this station that allows the user press one button to dial a specific stored number on one of their three assigned abbreviated lists.

---

### **Adding Abbreviated Dialing Lists**

You can program a new group list.

- 
1. Type `add abbreviated-dialing group next`.

2. Press `Enter`.

The Abbreviated Dialing List screen appears. In our example, the next available group list is group 3.

3. Enter a number (in multiples of 5) in the **Size** field.

This number defines the number of entries on your dialing list.

if you have 8 telephone numbers you want to store in the list, type 10 in the **Size** field.

4. If you want another user to be able to add numbers to this list, enter their extension in the **Program Ext** field.

If you want the user at 4567 to be able to change group list 3, enter `4567` in this field

5. Enter the telephone numbers you want to store, one for each dial code.

Each telephone number can be up to 24 digits long.

6. Press `Enter` to save your changes.

You can display your new abbreviated-dialing list to verify that the information is correct or print a copy of the list for your paper records. Once you define a group list, you need to define which stations can use the list.

---

### **Troubleshooting abbreviated dialing lists**

#### ***Dial list connects to wrong number***

##### **Problem**

A user complains that using an abbreviated dial list dials the wrong number.

### Possible Causes

- The user entered an wrong dial code.
- The dial code was wrongly defined.

#### Proposed solution

- 
1. Ask the user what number they dialed or button they pressed to determine which list and dial code they attempted to call.
  2. Access the dialing list and verify that the number stored for the specific dial code corresponds to the number the user wanted to dial.  
To access a group list, type `display abbreviated-dialing group x`, press `Enter`, where `x` is a group list number
  3. If the user dialed the wrong code, give them the correct code.
  4. If the dial code is wrong, press `Cancel` and use the appropriate change command to re-access the abbreviated dialing list.
  5. Correct the number.
  6. Press `Enter`.
- 

### **Cannot access dial list**

#### **Problem**

A user cannot access a dial list

#### **Possible Causes**

- The specific list was not assigned to the user's telephone.
- The user dialed the wrong feature access code
- The user pressed the wrong feature button.
- The feature button was wrongly defined.

#### Proposed solution—Verify list assigned to telephone

- 
1. Type `display station nnnn`, where `nnnn` is the user's extension.
  2. Press `Enter`.
  3. Review the current settings of the **List1** , **List2** , and **List3** fields to determine if the list the user wants to access is assigned to their telephone.
-

#### Proposed solution—Verify feature access code

- 
1. Type `display feature-access-codes`.
  2. Press `Enter`.
  3. Verify that the user is dialing the appropriate feature access code.
- 

#### Proposed solution—Verify feature button assignment

- 
1. Type `display station nnnn`, where `nnnn` is the user's extension.
  2. Press `Enter`.
  3. Review the current feature button assignments to determine whether:
    - The user was pressing the assigned button.
    - The list number and dial code are correct.
- 

#### **Abbreviated Dialing Lists-Limitations**

There are limits to the total number of abbreviated dialing list entries, the number of personal dial lists, and the number of group dial lists that your system can store. Because of these limitations, you should avoid storing the same number in more than one list. Instead, assign commonly dialed numbers to the system list or to a group list. You can determine the abbreviated dialing storage capacity, by referring to the System Capacity screen for the abbreviated dialing values (type `display capacity`). For details on the System Capacity screen, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

## **Bridged Call Appearances**

Think of a bridged call appearance as a telephone (the primary set) with an extension (the bridged-to appearance). Both telephones can be used to call in and out and both show when a line is in use. A call to the primary telephone is bridged to a specific appearance, or button, on the secondary telephone. The secondary telephone retains all its functions, and a specific button is dedicated as the bridged-to appearance from the primary telephone. Bridged call appearances have to be assigned to telephones with double-lamp buttons, or lights. The telephone types do not need to match, but as much consistency as possible is recommended for all telephones in a bridged group. When a call comes in on bridged telephones, the buttons assigned to the bridged appearances flash. You can assign as many bridged appearances as there are line appearances on the primary telephone, and you can assign ringing (alerting) to one or more of the telephones.

#### **Setting Up Bridged Call Appearances**

Create a bridged call appearance.

- 
1. Note the extension of the primary telephone .  
A call to this telephone lights the button and, if activated, rings at the bridged-to appearance on the secondary telephone.
  2. If you want to use a new telephone for the bridged-to extension, duplicate a station.  
For information, see [Duplicating Telephones](#).
  3. Type `change station` and the bridged-to extension.
  4. Press `Enter`.
  5. Press `Next Page` until the **Feature Options** page of the Station screen appears
  6. For the **Per Button Ring Control** field (digital sets only):
    - If you want to assign ringing separately to each bridged appearance, type `y`.
    - If you want all bridged appearances to either ring or not ring, leave the default `n`.
  7. Move to Bridge Call Alerting.
  8. If you want the bridged appearance to ring when a call arrives at the primary telephone, type `y`. Otherwise, leave the default `n`.
  9. Complete the appropriate field for your telephone type.
    - If your primary telephone is analog, move to the **Line Appearance** field and enter `abrdg-appr`
    - If your primary telephone is digital, move to the **BUTTON ASSIGNMENTS** field and enter `brdg-appr`.
  10. Press `Enter`.  
**Btn** and **Ext** fields appear. If **Per Button Ring Control** is set to `y` on the Station screen for the digital set, **Btn**, **Ext**, and **Ring** fields appear
  11. Enter the primary telephone's button number that you want to assign as the bridged call appearance.  
This button flashes when a call arrives at the primary telephone.
  12. Enter the primary telephone extension.
  13. If the Ring field appears:
    - If you want the bridged appearance to ring when a call arrives at the primary telephone, type `y`.
    - If you do not want the bridged appearance to ring, leave the default `n`.
  14. Press `Enter` to save your changes.

15. To see if an extension has any bridged call appearances assigned, type list bridge and the extension.

16. Press `Enter`.

The user at extension 4567 can now use this list by dialing the feature access code for the list and the dial code for the number they want to dial. Alternatively, you can assign an abbreviated dialing button to this station that allows the user press one button to dial a specific stored number on one of their three assigned abbreviated lists.

---

## When to use Bridged Call Appearances

Following is a list of example situations where you might want to use bridged appearances.

- A secretary making or answering calls on an executive's primary extension: These calls can be placed on hold for later retrieval by the executive, or the executive can simply bridge onto the call. In all cases, the executive handles the call as if he or she had placed or answered the call. It is never necessary to transfer the call to the executive.
- Visitor telephones: An executive might have another telephone in their office that is to be used by visitors. It might be desirable that the visitor be able to bridge onto a call that is active on the executive's primary extension number. A bridged call appearance makes this possible.
- Service environments: It might be necessary that several people be able to handle calls to a particular extension number. For example, several users might be required to answer calls to a hot line number in addition to their normal functions. Each user might also be required to bridge onto existing hot line calls. A bridged call appearance provides this capability.
- A user frequently using telephones in different locations: A user might not spend all of their time in the same place. For this type of user, it is convenient to have their extension number bridged at several different telephones.

## Extension to Cellular

Use the Extension to Cellular feature to extend your office calls and Communication Manager features to a cellular telephone. For a detailed description of the Extension to Cellular feature and how to administer it, see *Extension to Cellular in Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, or *Avaya Extension to Cellular User's Guide*, 210-100-700.

### Extension to Cellular Setup Table

The following table provides a quick reference to the screens and fields used in administering the Extension to Cellular feature.

Table 3: Screens for administering Extension to Cellular

| Screen Name                                       | Purpose  | Fields   |
|---|--|--|
| Stations with Off-PBX Telephone Integration       | Map station extensions to application types and  | All  |
| Off-PBX Telephone Mobile-Feature-Extension        | Administer CTI feature.  | Mobile Call (CTI) Extension  |
| Feature Access Code (FAC)                         | Set up access codes for Communication Manager features.  | Feature Access Code  |
| Extension to Call Which Activate Features by Name | Map a dialed extension to activate a feature (FNE) within Communication Manager from a cell phone. Some FNEs require FAC administration.   | Extension  |
| Telecommuting Access                              | Create an Extension to Cellular remote access number.  | All  |
| Security-Related System Parameters                | Define a system-wide station security code length.   | Minimum Station Security Code Length   |
| Station   | Assign feature buttons and timers.   | BUTTON ASSIGNMENTS   |
| Language Translations                             | To review the office telephone feature button assignments  | All  |
| Numbering-Public/ Unknown Format                  | Assign 10-digit caller identification.   | All  |
| Coverage Path                                     | Set up number of unanswered rings prior to coverage.   | Number of Rings  |
| Trunk Group                                       | Enable Call Detail Recording for outgoing trunk.   | CDR Reports  |
| DS1 Circuit Pack                                  | Administer a DS1 Circuit pack for R2MFC for EC500 use.   | Signaling Mode: CAS<br>Interconnect: CO  |
| Trunk Group                                       | Administer a trunk group for EC500 use.<br><br> <b>Note:</b><br>For more information, see Extension to Cellular in <i>Avaya Aura™ Communication Manager Feature Description and Implementation</i> , 555-245-205. | Group Type<br>Trunk Type<br>Outgoing Dial Type<br>Incoming Dial Type<br>Receive Answer<br>Supervision? |
| Multifrequency-signaling-related-parameters       | Administer MFC parameters needed for EC500.  | Incoming Call Type:<br>group-ii-mfc (for MFC signaling)  |

| Screen Name     | Purpose   | Fields   |
|-----------------|---|--|
|                 |  <b>Note:</b><br>For more information, see Guidelines for administering Multifrequency Signaling in <i>Avaya Aura™ Communication Manager Feature Description and Implementation</i> , 555-245-205. | <b>Outgoing Call Type:</b><br><b>group-ii-mfc (for MFC signaling)</b><br><b>Request Incoming ANI (non-AR/ARS) y</b>                        |
| System Capacity | Verify used, available, and system station limits.  | <b>Off-PBX Telephone - EC500</b><br><b>Off-PBX Telephone - OPS</b><br><b>Off-PBX Telephone - PBFMC</b><br><b>Off-PBX Telephone - PVFMC</b> |

### Setting Up Extension To Cellular Feature Access Button

Extension to Cellular provides the capability to administer an Extension to Cellular feature access button on the user's office telephone to enable and disable the feature. You can also configure an optional timer. You administer this feature button on page 3 of the Station screen for the "host" office extension to which Extension to Cellular is linked. The process described below explains how to administer an Extension to Cellular feature button and include the optional Extension to Cellular timer. The Extension to Cellular feature button is available on telephones which support administrable feature buttons.

1. Type `change station n`, where `n` is the extension of an Extension to Cellular enabled station  
 Type `1034`.
2. Press the `Next Page` button twice to display the Station screen (page 4).
3. Select an available feature button under the `BUTTON ASSIGNMENTS` header (button 4 was used in this example) and type `ec500` to administer an Extension to Cellular feature button on the office telephone.
4. Press `Enter`.

 **Note:**

The **Timer** subfield displays, and defaults to `n`. Leaving the default setting of `n` excludes the timer state

5. Set the optional **Timer** subfield to `y` to include an Extension to Cellular timer state for the administered feature button  
 When the timer state is included, the Extension to Cellular user can activate a one-hour timer to temporarily disable Extension to Cellular through this administered feature button.
6. Press **Enter**.

The corresponding feature button on the office telephone is now administered for Extension to Cellular.

 **Note:**

The feature status button on the office telephone indicates the current state of Extension to Cellular regardless of whether the feature was enabled remotely or directly from the office telephone.

For additional information, see the *Avaya Extension to Cellular User's Guide*, 210-100-700.

---

## Terminal Self-Administration

Before a user can enter the TSA Admin mode, their telephone must be completely idle. After a user presses the Admin button and enters a security code (if necessary), they are prompted, via the telephone's display, to choose features to administer to buttons on their telephone. The user can add, replace, or delete any of the following feature-button types from their telephone.

- CDR Account Code
- Automatic Dial
- Blank
- Call Forwarding
- Call Park
- Call Pickup
- Directed Call Pickup
- Group Page
- Send All Calls
- Toggle Swap
- Activate Whisper Page
- Answerback for Whisper Page
- Whisper Page Off

End-user button changes are recorded to the Communication Manager server's history log so that remote services can know what translations are changed.

## Setting Up Terminal Self-Administration

### Prerequisites

To prevent users from changing another user's telephone administration, you can enable the system-wide option that requires users to enter a station security code before they can administer their telephone.

To enable this option:

1. Set the **Station Security Code for Terminal Self-Administration Required** on the Security-Related System Parameters screen to *y*.
2. If you enable this option, the user is prompted for the station security code when they press the **Admin** button. The user must enter the security code, followed by the pound (#) button or the **Done** softkey.

---

Terminal self-administration (TSA) allows users to administer some of their own feature buttons from their telephones. TSA is available for 6400-series, and 4612 and 4624 telephones. Users are prompted, via the telephone's display, to choose features to assign to buttons on their telephones.

You need to assign a security code to the user's Station screen for each user you want to enable access to TSA. You also need to assign the user an Admin feature button. For example, to assign a security code of 12345678 to extension 4234, complete the following steps:

- 
1. Type `change station 4234,`.
  2. Press `Enter`.  
The Station screen for extension 4234 appears.
  3. In the **Security Code** field, type `12345678`  
You should assign unique security codes for each user. Once you enter the code and move off the field, the system changes the field to `'**'` for extra security.
  4. In one of feature button fields, type `admin`.  
You can assign this button to a feature button or a softkey.
  5. Press `Enter` to save your changes.

---

### Fixing Problems in Terminal Self-Administration

| Symptom  | Cause and Solution   |
|--|--|
| When a telephone is in the Admin mode, the telephone is not able to accept any calls | The telephone is treated as if it were busy. Also, a user cannot make calls while in the Admin mode. |
| Any button state a telephone is in when the telephone enters the Admin mode          |  |

| Symptom  | Cause and Solution   |
|--|--|
| stays active while the telephone is in the Admin mode.   |  |
| ACD agents who wish access to the Admin mode of TSA must be logged off before pressing the Admin button. | If they are not logged off when they attempt to enter the Admin mode, they receive a denial (single-beep) tone.  |
| Call Forwarding can be active and works correctly in the Admin mode.                                     | An active <b>Call Forwarding</b> button cannot be removed when the telephone is in the Admin mode.   |
| The telephone must be on-hook to go into the Admin mode.   | The <b>Headset On/Off</b> button must be in the OFF position.  |
| A telephone that is in the Admin mode of TSA cannot be remotely unmerged by the PSA feature.             | If a user has Abbreviated and Delayed Ringing active, a call can be silently ringing at a telephone and the user might not realize it. This ringing prevents the user from entering the Admin mode of TSA. |

## Enterprise Mobility User

Enterprise Mobility User (EMU) is a software-only feature that provides the ability to associate the buttons and features of a primary telephone to a telephone of the same type anywhere within your company's enterprise.

A home station can be visited by another EMU user while the user is registered as an EMU visitor elsewhere. A home station can be used as a visited station while the principal user's EC500 or other Off-PBX applications are active. And the principal user can activate an Off-PBX application even if their home station is being visited by another EMU user.

 **Note:**

In this document, any telephone that is not the primary telephone is referred to as the “visited” telephone and any server that is not the home server of the primary telephone is referred to as the “visited server.”

### System Requirements — EMU

The following is a list of requirements that you need for the EMU feature:

- QSIG must be the private networking protocol in the network of Communication Manager systems. This requirement also includes QSIG MWI

 **Note:**

All systems in a QSIG network must be upgraded to Communication Manager 4.0 or later in order for the Enterprise Mobility User feature to function properly. If only some systems are upgraded, and their extensions expanded, the EMU feature might not work with the systems that have not been upgraded. See your Avaya technical representative for more information

- Communication Manager Release 3.1 or later software must be running on the home server and all visited servers.
- All servers must be on a Linux platform. EMU is not supported on DEFINITY servers.
- The visited telephone must be the same model type as the primary telephone to enable a optimal transfer of the image of the primary telephone. If the visited telephone is not the same model type, only the call appearance (**call-appr**) buttons and the message waiting light are transferred.
- All endpoints must be terminals capable of paperless button label display.
- Uniform Dial Plan (UDP)
- To activate the EMU feature, a user enters the EMU activation feature access code (FAC), the extension number of their primary telephone, and the security code of the primary telephone on the dial pad of a visited telephone. The visited server sends the extension number, the security code, and the set type of the visited telephone to the home server. When the home server receives the information, it:
  - Checks the class of service (COS) for the primary telephone to see if it has PSA permission
  - Compares the security code with the security code on the Station screen for the primary telephone
  - Compares the station type of the visited telephone to the station type of the primary telephone. If both the visited telephone and the primary telephone are of the same type, the home server sends the applicable button appearances to the visited server. If a previous registration exists on the primary telephone, the new registration is accepted and the old registration is deactivated

If the registration is successful, the visited telephone assumes the primary telephone’s extension number and some specific administered button types. The display on the primary telephone shows **Visited Registration Active: <Extension>**: The extension number that displays is the extension number of the visited telephone

 **Note:**

The speed dialing list that is stored on the primary telephone and the station logs are not downloaded to the visited telephone.

## Configuring your System for the Enterprise Mobility User

---

1. Type `display cos` to view your Class of Service settings.  
The system displays the Class of Service screen.
2. Verify that the **Personal Station Access (PSA)** field is set to `y`.  
This field applies to the primary telephone and must be set to `y` for EMU.
3. Type `display feature-access-codes`.  
The system displays the Feature Access Code (FAC) screen
4. In one of feature button fields, type `admin`.
5. Scroll down until you see the fields for **Enterprise Mobility User Activation and Deactivation**.  
The feature access codes (FACs) for both EMU activation and EMU deactivation must be set on all servers using EMU. You must enter the FAC of the server in the location from which you are dialing.

 **Note:**

To avoid confusion, Avaya recommends that all the servers in the network have the same EMU feature access codes.

6. On page 3 of the Feature Related System Parameters screen, use the **EMU Inactivity Interval for Deactivation** (hours) field to administer a system-wide administrable interval for EMU deregistration at a visited switch.
7. Click `Enter` to save your changes.

## Setting EMU options for stations

---

1. Enter `add station next`.
2. Enter the security code of your primary telephone when you activate or deactivate EMU. The security code is administered on page one of the Station screen. The security code can be up to eight numbers. No letters or special characters are allowed. Once the security code is entered, the system displays a \* in the **Security Code** field.
3. On the Station screen, scroll down till you find the **EMU Login Allowed** field.

The **EMU Login Allowed** field applies to the visited station and must be set to *y* for EMU. The valid entries to this field are *y* or *n*, with *n* as the default. You must set this field to *y* to allow this telephone to be used as a visited station by an EMU user.

4. Select *Enter* to save your changes.

---

## Defining options for calling party identification

---

1. Type `display trunk-group x`, where *x* is the number of the trunk group. The system displays the Trunk Group screen.
2. Scroll down till you see the **Send EMU Visitor CPN** field. This field controls calling party identification, that is, the extension of the primary telephone or the extension of the visited telephone that is used when a call is made from a visited telephone.
3. If you want the system to display calling party information of the primary telephone, the **Send EMU Visitor CPN** field must be set to *y*. There are areas where public network trunks disallow a call if the calling party information is invalid. In this case, there can be instances where the extension of the primary telephone is considered invalid and the extension of the visited telephone must be used. To use the extension of the visited telephone, set the **Send EMU Visitor CPN** field to *n*.



**Note:**

If you set the **Send EMU Visitor CPN** field to *y*, you must set the **Format** field on the same page to either *public* or *unk-pvt*.

4. Click *Enter* to save your changes.

---

## Activating EMU

---

1. At the visited telephone, enter the EMU activation facility-access-code (FAC). You must enter the EMU activation FAC of the server in the location where you are dialing from.
2. Enter the extension of your primary telephone set.
3. Enter the security access code of your primary telephone set. This is the security code administered on the primary telephone's station form on the home server.
  - If the registration is successful, you hear confirmation tone.
  - If the registration is not successful, you hear audible intercept.

Audible intercept is provided when:

- The registration was rejected by the home server.

- The telephone where the registration attempt is made is not administered for EMU use.
- The 15 second timer expires at the visited server.

If the home server receives a request from a visited server for a telephone that already has an EMU visitor registration active, the old registration is terminated and the new registration is approved. If the primary telephone is in-use when a registration attempt is made, the registration attempt fails.

---

## Deactivating EMU

---

1. At the visited telephone, enter the EMU deactivation FAC.  
You must enter the EMU deactivation FAC of the server in the location where you are dialing from.
2. Enter the extension number of the primary telephone.
3. Enter the security code of the visited telephone.  
If the visited telephone does not deactivate, the telephone remains in the visited state.
4. To deactivate the visited telephone you can perform a busy-out, release busy-out at the visited server.
5. Enter the EMU feature deactivation code and the security code of the visited telephone at the home server location.
6. Press the <mute>RESET function on the IP telephone.

 **Note:**

Anytime the visited telephone performs a reset, the EMU registration is deactivated.

7. Unplug the visited DCP set for a period of one minute  
Unplugging or disconnecting a 4600 series set will not deactivate the set.
- 

---

## Managing Attendant Consoles

### Attendant Consoles

The attendant console is the main answering position for your organization. The console operator is responsible for answering incoming calls and for efficiently directing or "extending"

calls to the appropriate telephone. The attendant console also can allow your attendants to monitor:

- system problems
- toll fraud abuse
- traffic patterns

The number of consoles you can have in your organization varies depending on your Avaya solution.

### **302 attendant consoles**

Avaya Communication Manager supports the following 302 attendant consoles: the 302A/B, 302C, and 302D consoles. You might have a basic or enhanced version of these consoles.

To compare and contrast the consoles, view the diagrams below.

- 302A/B
- 302C
- 302D

### **302D Console**

The 302D console provides the following enhancements to the 302C console:

- Modular handset/headset connection

The console accepts a standard RJ11, 4-pin modular handset or headset. This connection replaces the quarter-inch, dual-prong handset/headset connection.

- Activate/deactivate push-button

You can use the push-button on the left side of the console to activate or deactivate the console. A message appears on the console identifying that the button must be pressed to activate the console.

- Two-wire DCP compatibility

The console is compatible with two-wire DCP circuit packs only, not four-wire DCP circuit packs.

- Headset volume control

The console can now control the volume of an attached headset.

- Noise expander option

The console has circuitry to help reduce background noise during pauses in speech from the console end of a conversation. This option is normally enabled.

- Support for Eurofont or Katakana character set

The console can show the Eurofont or Katakana character set. Administration of these character sets must be coordinated with the characters sent from Avaya Communication Manager.

## Avaya PC consoles

The Avaya PC Console is a Microsoft Windows-based call handling application for Avaya Communication Manager attendants. It provides an ideal way to increase your productivity and to better serve your customers.

PC Console offers all the call handling capabilities of the hardware-based Avaya 302 attendant console with a DXS module, plus several enhanced features and capabilities. The enhanced features provide you with the ability to see up to six calls at once, and to handle all calls more efficiently.

PC Console also provides a powerful directory feature. You are able to perform searches, display user information, including a photo. You are able to place a call immediately from the directory.

And, because PC Console resides on a Windows-based PC, you are able to use other software applications at the same time. If a call comes in while you are in another application, you are able to handle it immediately.

For more information about the Avaya PC Console, contact your Avaya account team or representative.

## SoftConsole IP Attendant

The SoftConsole is a Windows-based application that can replace the 302B hard console. The SoftConsole is similar to PC Console, but it performs call answering and routing through a PC interface via IP. For more information, contact your Avaya account team or representative.

### Related topics:

[302A/B Console](#) on page 241

[302C Console](#) on page 242

[302D Console](#) on page 243

### 302A/B Console

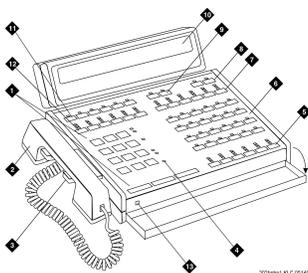


Figure 1: 302A and 302B1 attendant console

### \* Note:

Button numbers map to physical positions on the console.

Figure notes:

1. Call processing area
2. Handset

## Managing inventory

3. Handset cradle
4. Warning lamps and call waiting lamps
5. Call appearance buttons
6. Feature area
7. Trunk group select buttons
8. Volume control buttons
9. Select buttons
10. Console display panel
11. Display buttons
12. Trunk group select buttons
13. Lamp Test Switch

## 302C Console

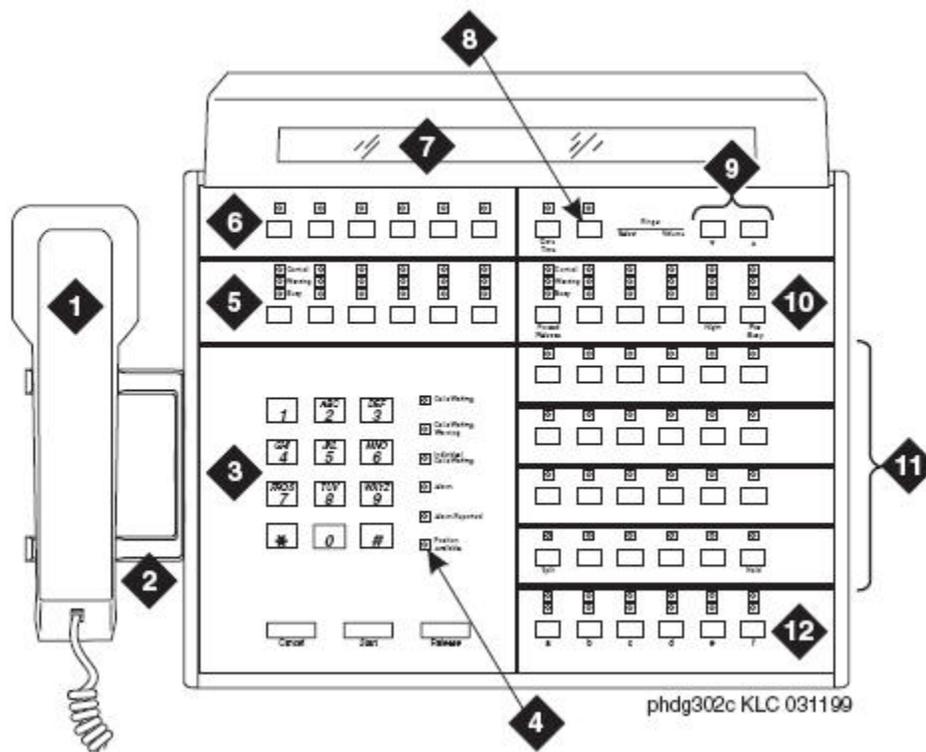


Figure 2: 302C attendant console

**\* Note:**

Button numbers map to physical positions on the console.

Figure notes:

1. Handset
2. Handset cradle
3. Call processing area
4. Warning lamps and call waiting lamps
5. Outside-line buttons
6. Display buttons
7. Display
8. Select buttons
9. Volume control buttons
10. Outside-line buttons
11. Feature buttons
12. Call appearance buttons

### 302D Console

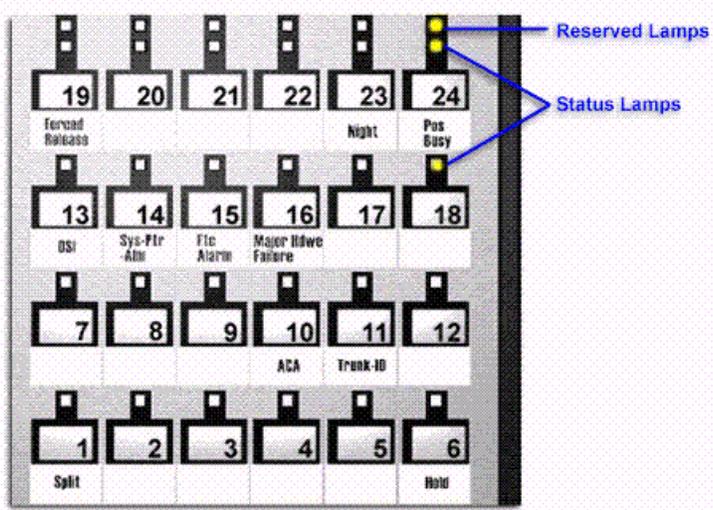


Figure 3: Console feature button layout

**\* Note:**

Button numbers map to physical positions on the console.

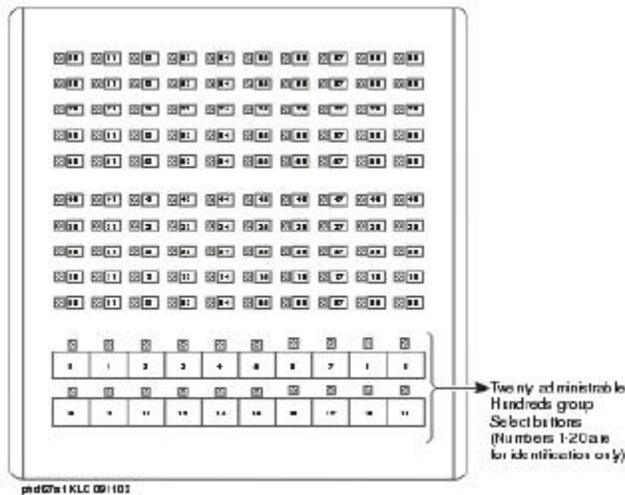


Figure 4: Enhanced Selector Console

## Adding an Attendant Console

Usually Avaya connects and administers your primary attendant console during cutover. However, you might find a need for a second attendant console, such as a backup console that is used only at night. This example shows how to add a night-only attendant console.

**\* Note:**

These instructions do not apply to adding a PC Console or SoftConsole. For more information, see the appropriate console documentation.

1. Type `add attendant`.
2. Press `Enter`  
The Attendant Console screen appears.
3. In the **Type** field, enter `302`. This is the type of attendant console.
4. If you want this attendant to have its own extension, enter one in the **Extension** field.

**+ Tip:**

If you assign an extension to the console, the class of restriction (COR) and class of service (COS) that you assign on this Attendant Console screen override the COR and COS you assigned on the Console Parameters screen. To avoid unexpected behavior, you should assign the same COR and same COS on both screens.

If you give your attendants an individual extension, users can call the attendant directly by dialing the extension.

Individual attendant extensions also allow attendants to use features that an attendant group cannot use — for example, you can assign them to hunt groups.

5. In the **Console Type** field, enter `night-only`.  
This indicates how this console is used in your organization—as a principal, day only, night only, or day/night console. You can have only one night-time console (night only or day/ night) in the system.
6. In the **Port** field , enter the port address for this console.
7. Type a name to associate with this console in the **Name** field.
8. In the **DIRECT TRUNK GROUP SELECT BUTTON ASSIGNMENTS** fields, enter trunk access codes for the trunks you want the attendant to be able to select with just one button.
9. If you are using the **Enhanced Selector** console, set the **HUNDREDS SELECT BUTTON ASSIGNMENTS** that you want this console to have.  
If you want this console to be able to access extensions in the range 3500 to 3999, you need to assign them 5 **Hundreds Select Buttons**: 35 for extensions 3500 to 3599, 36, 37, 38, and 39.
10. Assign the Feature Buttons that you want the 302 console to have.  
To determine which buttons you can assign to a console, see *Attendant Console Feature Buttons*.



**Tip:**

Feature buttons are not numbered top-to-bottom on the attendant console, as you might expect.

11. Press **Enter** to save your changes.

**Related topics:**

[Attendant Console Feature Buttons](#) on page 245

## Attendant Console Feature Buttons

### Feature Buttons

The following table lists the feature buttons that you can assign to an attendant console.

| Feature or Function | Recommended Button Label | Value Entered on Attendant Console Screen | Maximum Allowed | Notes |
|---------------------|--------------------------|---|-----------------|-------|
| Abbreviated Dialing | AD                       | abrv-dial (List:____<br>DC:____)          | 1 per List/ DC  | 1     |

| Feature or Function                                  | Recommended Button Label | Value Entered on Attendant Console Screen           | Maximum Allowed   | Notes |
|--|--------------------------|---|-------------------|-------|
| Administered Connection [status lamp]                | AC Alarm                 | ac-alarm  | 1                 |       |
| Automatic Call Distribution (ACD)                    | After Call Work          | after-call (Grp. No.__)                             | N                 | 2     |
|  | Assist                   | assist (Grp. No:__)                                 | 1 per split group | 2     |
|  | Auto In                  | auto-in (Grp. No.__)                                | 1 per split group | 2     |
|  | Auxiliary Work           | aux-work (Grp. No.__)                               | 1 per split group | 2     |
|  | Manual-In                | manual-in (Grp. No.__)                              | 1 per split group | 2     |
|  | Release                  | release   | 1                 |       |
|  | Work Code                | work-code   | 1                 |       |
|  | Stroke (0-9)             | stroke-cnt (Code:_)                                 | 1                 | 3     |
| Attendant Console (Calls Waiting)                    | CW Aud Off               | cw-ringoff  | 1                 |       |
| Attendant Control of Trunk Group Access (Activate)   | Cont Act                 | act-tr-grp  | 1                 |       |
| Attendant Control of Trunk Group Access (Deactivate) | Cont Deact               | deact-tr-g  | 1                 |       |
| Attendant Direct Trunk Group Select                  | Local TG<br>Remote TG    | local-tgs (TAC:__)<br>remote-tgs (LT:__)<br>(RT:__) | 12                | 4     |
| Attendant Crisis Alert                               | Crisis Alert             | crss-alert  | 1                 |       |
| Attendant Display [display buttons]                  | Date/Time                | date-time   | 1                 |       |
|  | Inspect Mode             | inspect   | 1                 |       |
|  | Normal Mode              | normal  | 1                 |       |
|  | Stored Number            | stored-num  | 1                 |       |
| Attendant Hundreds Group Select                      | Group Select _           | hundrd-sel (Grp:__)                                 | 20 per console    | 5     |
| Attendant Room Status                                | Occupied Rooms Status    | occ-rooms   | 1                 | 6     |

| Feature or Function                            | Recommended Button Label | Value Entered on Attendant Console Screen | Maximum Allowed | Notes |
|--|--------------------------|---|-----------------|-------|
|  | Maid Status              | maid-stat                                 | 1               | 6     |
| Attendant Override                             | Override                 | override                                  | 1               |       |
| Automatic Circuit Assurance                    | ACA                      | aca-halt                                  | 1 per system    |       |
| Automatic Wakeup (Hospitality)                 | Auto Wakeup              | auto-wkup                                 | 1               |       |
| Busy Verification                              | Busy Verify              | verify                                    | 1               |       |
| Call Coverage                                  | Cover Cback              | cov-cback                                 | 1               |       |
|  | Consult                  | consult                                   | 1               |       |
|  | Go To Cover              | goto-cover                                | 1               |       |
| Call Coverage [display button]                 | Cover Msg Rt             | cov-msg-rt                                | 1               |       |
| Call Offer (Intrusion)                         | Intrusion                | intrusion                                 | 1               |       |
| Call Prompting [display button]                | Caller Info              | callr-info                                | 1               |       |
| Call Type                                      | Call Type                | type-disp                                 | 1               |       |
| Centralized Attendant Service                  | CAS-Backup               | cas-backup                                | 1               |       |
| Check In/Out (Hospitality) [display buttons]   | Check In                 | check-in                                  | 1               |       |
|  | Check Out                | check-out                                 | 1               |       |
| Class of Restriction [display button]          | COR                      | class-rstr                                | 1               |       |
| Conference Display [display button]            | Conference Display       | conf-dsp                                  | 1               |       |
| Demand Print                                   | Print Msgs               | print-msgs                                | 1               |       |
| DID View                                       | DID View                 | did-view                                  | 1               |       |
| Do Not Disturb (Hospitality)                   | Do Not Disturb           | dn-dst                                    | 1               |       |
| Do Not Disturb (Hospitality) [display buttons] | Do Not Disturb Ext       | ext-dn-dst                                | 1               |       |
|  | Do Not Disturb Grp       | grp-dn-dst                                | 1               |       |
| Don't Split                                    | Don't Split              | dont-split                                | 1               |       |
| Emergency Access To the Attendant              | Emerg. Access To Attd    | em-acc-att                                | 1               |       |

| Feature or Function                                       | Recommended Button Label                      | Value Entered on Attendant Console Screen | Maximum Allowed | Notes |
|---|---|---|-----------------|-------|
| Facility Busy Indication [status lamp]                    | Busy (trunk or extension#)                    | busy-ind (TAC/Ext: _)                     | 1 per TAC/ Ext. | 7     |
| Facility Test Calls [status lamp]                         | FTC Alarm                                     | trk-ac-alm                                | 1               |       |
| Far End Mute [display button]                             | Far End Mute for Conf                         | fe-mute                                   | 1               |       |
| Group Display   | Group Display                                 | group-disp                                | 1               |       |
| Group Select  | Group Select                                  | group-sel                                 | 1               |       |
| Hardware Failure [status lamps]                           | Major Hdwe Failure                            | major-alm                                 | 10 per system   |       |
|   | Auto Wakeup                                   | pr-awu-alm                                | 1               |       |
|   | DS1 (facility)                                | ds1-alm                                   | 10 per system   |       |
|   | PMS Failure                                   | pms-alm                                   | 1               |       |
|   | PMS Ptr Alm                                   | pr-pms-alm                                | 1               |       |
|   | CDR 1 Failure                                 | cdr1-alm                                  | 1               |       |
|   | CDR 2 Failure                                 | cdr2-alm                                  | 1               |       |
|   | Sys Ptr Alm                                   | pr-sys-alm                                | 1               |       |
| Hold  | Hold  | hold                                      | 1               |       |
| Integrated Directory [display button]                     | Integrtd Directory                            | directory                                 | 1               |       |
| Incoming Call Identification                              | Coverage (Group number, type, name, or ext.#) | in-call-id                                | N               |       |
| Intrusion (Call Offer)                                    | Intrusion                                     | intrusion                                 | 1               |       |
| Leave Word Calling  | Cancel LWC                                    | lwc-cancel                                | 1               |       |
|   | LWC   | lwc-store                                 | 1               |       |
| Leave Word Calling [display buttons]                      | Delete Msg                                    | delete-msg                                | 1               |       |
|   | Next  | next                                      | 1               |       |
|   | Call Display                                  | call-disp                                 | 1               |       |
| Leave Word Calling (Remote Message Waiting) [status lamp] | Msg (name or extension #)                     | aut-msg-wt (Ext:___)                      | N               |       |

| Feature or Function                              | Recommended Button Label   | Value Entered on Attendant Console Screen | Maximum Allowed   | Notes |
|--|----------------------------|---|-------------------|-------|
| Link Failure                                     | Link Failure (Link No. __) | link-alarm (Link No. __)                  | 1 per Link #      | 8     |
| Login Security Violation                         | lsvn-halt                  | lsvn-halt                                 | 1 per system      |       |
| Message Waiting                                  | Message Waiting Act.       | mwn-act                                   | 1 per system      |       |
|  | Message Waiting Deact.     | mwn-deact                                 | 1 per system      |       |
| Night Service                                    | Trunk Grp. NS              | trunk-ns (Grp. No. __)                    | 1 per trunk group | 9     |
| No Answer Alert                                  | noans-altr                 | noans-altr                                | 1 per group       |       |
| Off Board Alarm                                  | off-bd-alm                 | off-bd-alm                                | 1 per group       |       |
| Page 1 Link Alarm Indication                     | PAGE1 Alarm                | pg1-alarm                                 | 1 per station     |       |
| Page 2 Link Alarm Indication                     | PAGE2 Alarm                | pg2-alarm                                 | 1 per station     |       |
| PMS Interface [display buttons]                  | PMS display                |   |                   |       |
| Priority Attendant Group                         | prio-grp                   | prio-grp                                  | 1                 |       |
| Priority Calling                                 | Prior Call                 | priority                                  | N                 |       |
| Position Busy                                    | Position Busy              | pos-busy                                  | 1                 |       |
| Queue Status Indications (ACD) [display buttons] | AQC                        | atd-qcalls                                | 1                 |       |
|  | AQT                        | atd-qtime                                 |                   |       |
| Queue Status Indications (ACD) [status lamps]    | NQC                        | q-calls (Grp: _)                          | 1                 | 10    |
|  | OQT                        | q-time Grp: _)                            | 1 per hunt group  | 10    |
| Remote Access Security Violation                 | rsvn-halt                  | rsvn-halt                                 | 1 per system      |       |
| Ringing  | In Aud Off                 | in-ringoff                                | 1                 |       |
| Security Violation Notification Halt             | ssvn-halt                  | ssvn-halt                                 | 1 per system      |       |
| Serial Call                                      | Serial Call                | serial-cal                                | 1                 |       |
| Split/Swap                                       | Split-swap                 | split-swap                                | 1                 | 11    |

| Feature or Function                     | Recommended Button Label         | Value Entered on Attendant Console Screen | Maximum Allowed  | Notes |
|---|----------------------------------|---|------------------|-------|
| System Reset Alert                      | System Reset Alert [status lamp] | rs-alert                                  | 1                |       |
| Station Security Code Notification Halt | ssvn-halt                        | ssvn-halt                                 | 1 per system     |       |
| Night Service (ACD)                     | Hunt Group                       | hunt-ns (Grp. No.__)                      | 3 per hunt group | 12    |
| Time of Day Routing [display buttons]   | Immediate Override               | man-ovrid                                 | 1                |       |
|   | Clocked Override                 | clk-overid                                | 1                |       |
| Timed Reminder                          | RC Aud Off                       | re-ringoff                                | 1                |       |
| Timer                                   | Timer                            | timer                                     | 1                |       |
| Trunk Identification [display button]   | Trunk-ID                         | trk-id                                    | 1                |       |
| Trunk Group Name [display button]       | Trunk-Name                       | trunk-name                                | 1                |       |
| Visually Impaired Service (VIAS)        | VIS                              | vis                                       | 1                |       |
|   | Console Status                   | con-stat                                  | 1                |       |
|   | Display                          | display                                   | 1                |       |
|   | DTGS Status                      | dtgs-stat                                 | 1                |       |
|   | Last Message                     | last-mess                                 | 1                |       |
|   | Last Operation                   | last-op                                   | 1                |       |
| VDN of Origin Announcement Repeat       | VOA Repeat                       | voa-repeat                                | 1                | 12    |
| VuStats                                 | VuStats                          | vu-display                                | 1                |       |

1. List: List number 1 to 3 where the destination number is stored. DC: Dial codes of destination number.
2. Grp: The split group number for ACD.
3. Code: Enter a stroke code (0 through 9).
4. TAC: local-tgs — TAC of local TG  
remote-tgs — (L-TAC) TAC of TG to remote PBX  
remote-tgs — (R-TAC) TAC of TG on remote PBX

The combination of local-tgs/remote-tgs per console must not exceed 12 (maximum). Label associated button appropriately so as to easily identify the trunk group.

5. Grp: Enter a hundreds group number (1 through 20).
6. **Enhanced Hospitality** must be enabled on the System-Parameters Customer-Options (Optional Features) screen.
7. Ext: Can be a VDN extension.
8. Link: A link number — 1 to 8 for multi-carrier cabinets, 1 to 4 for single-carrier cabinets.
9. Grp: A trunk group number.
10. Grp: Group number of the hunt group.
11. Allows the attendant to alternate between active and split calls.
12. VDN of Origin must be enabled.

## Setting Console Parameters

You can define system-wide console settings on the Console Parameters screen. For example, if you want to warn your attendants when there are more than 3 calls in queue or if a call waits for more than 20 seconds, complete the following steps:

- 
1. Type `change console-parameters`.
  2. Press `Enter`  
The Console Parameters screen appears.
  3. In the **Calls in Queue Warning** field, enter 3.  
The system lights the console's second call waiting lamp if the number of calls waiting in the attendant queue exceeds 3 calls. Click **Next** to display page 2.
  4. In the **Time in Queue Warning** field, enter 20.  
The system issues a reminder tone if a call waits in the attendant queue for more than 20 seconds.
  5. Press `Enter` to save changes.



**Note:**

Some of the settings on the individual Attendant Console screens can override your system-wide settings.

---

## Removing an Attendant Console

Before you physically remove an attendant from your system, check the attendant's status, remove it from any group or usage lists, and then delete it from the system's memory. For example, to remove attendant 3, which also is assigned extension 4345:

- 
1. Type `status attendant 3`.
  2. Press `Enter`.  
The Attendant Status screen appears.
  3. Make sure that the attendant:
    - is plugged into the jack
    - is idle (not making or receiving calls)
  4. Type `list usage extension 4345`.
  5. Press `Enter`.  
The Usage screen shows where the extension is used in the system.
  6. Press `Cancel`.
  7. If the attendant extension appears on the Usage screen, access the appropriate feature screen and delete the extension.  
For example, if extension 1234 belongs to hunt group 2, type `change hunt group 2` and delete the extension from the list.
  8. Type `remove attendant 3`.
  9. Press `Enter`.  
The system displays the Attendant Console screen so you can verify that you are removing the correct attendant.
  10. If this is the correct attendant, press `Enter`.  
If the system responds with an error message, the attendant is busy or still belongs to a group. Press **Cancel** to stop the request, correct the problem, and type `remove attendant 3` again.
  11. Remove the extension from voice mail service if the extension has a voice mailbox.
  12. Type `save translations`.
  13. Press `Enter` to save your changes.

 **Note:**

You do not need to delete the extension from coverage paths. The system automatically adjusts coverage paths to eliminate the extension.

Now you can unplug the console from the jack and store it for future use. You do not need to disconnect the wiring at the cross-connect field. The extension and port address remain available for assignment at a later date.

---

## Providing Backup for an Attendant

### Prerequisites

- You can assign the attendant backup alerting only to multiappearance telephones that have a client room class of service (COS) set to No. For more information, see *Class of Service*.
- If you have not yet defined a Trunk Answer Any Station (TAAS) feature access code, you need to define one and provide the feature access code to each of the attendant backup users. For more information, see *Feature Access Code (FAC)*.

To enable your system to alert backup stations, you need to administer the Console Parameters screen for backup alerting. You also need to give the backup telephones an attendant queue calls feature button and train your backup users how to answer the attendant calls.

---

Communication Manager allows you to configure your system so that you have backup positions for your attendant. Attendant Backup Alerting notifies backup telephones that the attendant need assistance in handling calls. The backup telephones are alerted when the attendant queue reaches the queue warning level or when the console is in night service.

Once a backup telephone receives an alert, the user can dial the Trunk Answer Any Station (TAAS) feature access code (FAC) to answer the alerting attendant calls.

### Tip:

You can find more information about attendant backup in the *GuestWorks Technician Handbook*.

---

1. Type `change console-parameters`.
2. Press `Enter`.  
The Console Parameters screen appears.
3. In the **Backup Alerting** field, enter `y`.
4. Press `Enter` to save changes.  
The system will now notify anyone with an attendant queue calls button when the attendant queue reaches the warning level or when the console is in night service.
5. Type `change station 4345`.
6. Press `Enter`.

The Station screen appears

7. In one of the Button Assignment fields, enter `atd-qcalls`.

The `atd-qcalls` button provides the visual alerting for this telephone. When this button is dark (idle state), there are no calls in the attendant queue. When the button shows a steady light (busy state), there are calls in the attendant queue. When the button shows a flashing light (warning state), the number of calls in the attendant queue exceeds the queue warning. The backup-telephone user also hears an alerting signal every 10 seconds.

8. Press `Enter` to save changes.

Now you need to train the user how to interpret the backup alerting and give them the TAAS feature access code so that they can answer the attendant calls.

---

## Managing Telephone Displays

### Display Administration

#### Displaying Caller Information

This chapter provides information on the messages that appear on the screens of display telephones.

Your system uses automatic incoming call display to provide information about incoming calls to a display telephone that is in use, or active on a call. The information is displayed for 30 seconds on all telephones except for CALLMASTER telephones, where the display goes blank after 30 seconds. However, the information for each new call overrides the existing message.

Call information appears on the display only if the call terminates at the telephone. For example, if the call is forwarded to another extension, no call information appears.

For more information on the buttons and languages you can set up for the messages that appear on the display, see the Telephone Displays feature description in the *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-505.

### Displaying ANI Calling Party Information

Calling party information might consist of either a billing number that sometimes is referred to as Automatic Number Identification (ANI), or a calling party number. Your telephone might display the calling party number and name, or the incoming trunk group name.

To set up a tie trunk group to receive calling party information and display the calling party number on the telephone of the person called:

- 
1. Type `change trunk group nnnn`, where `nnnn` is the trunk group you want to change.
  2. Click **Next Page** until you see the **Trunk Parameters** fields on the Trunk Group screen (page 2).
  3. Type `tone` in the **Incoming Dial Type** field.
  4. Click **Next Page** and type `*ANI*DNIS` in the **Incoming Tone (DTMF) ANI** field.
  5. Press `Enter` to save your changes.
- 

## Displaying ICLID Information

### Prerequisites

Be sure the **Analog Trunk Incoming Call ID** field is set to `y` on the System-Parameters Customer-Options (Optional Features) screen. See the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207 for information on the required circuit pack.

---

Communication Manager collects the calling party name and number (Incoming Call Line Identification, or ICLID) received from the central office (CO) on analog trunks.

This example shows how to set up the analog diod trunk group 1 to receive calling party information and display the calling party number on the telephone of the person called.

- 
1. Type `change trunk group 1`.  
The Trunk Group screen for trunk group 1 appears. The **Group Type** field is already set to `diod`.
  2. Click **Next Page** to display the **Trunk Features** fields on the Trunk Group screen (page 3).
  3. Type `Bellcore` in the **Receive Analog Incoming Call ID** field.
  4. Click **Next Page** to display the Administrable Timers screen.
  5. Type `120` in the Incoming **Seizure (msec)** field.
  6. Click **Enter** to save your changes.
-

## Setting the Display Language

- 
1. Type `change station nnnn`, where `nnnn` is the extension of the station that you want to change.
  2. Press **Enter**.  
The System displays the Station screen.
  3. In the **Display Language** field, enter the display language you want to use.

 **Tip:**

Time of day is displayed in 24-hour format (00:00 - 23:59) for all languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.). To display time in 24-hour format and display messages in English, set the **Display Language** field to `unicode`. When you enter `unicode`, the station displays time in 24-hour format, and if no Unicode file is installed, displays messages in English by default. For more information on Unicode, see *Administering Unicode display*.

4. Press **Enter** to save your changes.

---

### Related topics:

[Administering Unicode Display](#) on page 256

### Administering Unicode Display

To use Unicode display languages, you must have the appropriate Avaya Unicode Message files loaded on Communication Manager. These files are named `avaya_unicode.txt` (standard phone messages), `custom_unicode.txt` (posted messages and system labels), `avaya_user-defined.txt` (standard phone messages using Eurofont), and `custom_user-defined.txt` (posted messages and system labels using Eurofont).

To use the Phone Message files `avaya_unicode.txt` and `custom_unicode.txt`, you must have Unicode-capable stations, such as the 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones, and Avaya Softphone R5.0. Unicode is also an option for the 2420J telephone when **Display Character Set** on the System Parameters Country-Options screen is `katakana`. For more information on the 2420J, see *2420 Digital Telephone User's Guide*, 555-250-701.

Only Unicode-capable stations have the script (font) support that is required to match the scripts that the Unicode Phone Message file uses. To use the user-defined messages files `avaya_user-defined.txt` and `custom_user-defined.txt` you must use an Avaya digital phone that supports Eurofont or Kanafont.

 **Note:**

To view the dial pad letter/number/symbol mapping tables used for the integrated directory, see Telephone Display in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

For Communication Manager 2.2 and later, the following languages are available using Unicode display:

- Chinese
- Czech
- Danish
- Dutch
- German
- Hebrew
- Hungarian
- Icelandic
- Italian
- Japanese
- Korean
- Macedonian
- Polish
- Romanian
- Russian
- Servian
- Slovak
- Swedish
- Ukrainian

### ***Obtaining and Installing Phone Message Files***

A Unicode Message file for each supported language is available in a downloadable ZIP file on the Avaya support Web site (<http://www.avaya.com/unicode>). You can also create a new translation or edit an existing translation with the Avaya Message Editing Tool (AMET) (<http://support.avaya.com/amet>). Additional languages are periodically becoming available, so check this site often for the most up-to-date message files.

 **Note:**

Refer to the *Communication Manager Messages Job Aid* for details on the following procedures.

- 
1. Download the appropriate Unicode message file to your PC. For an existing translation, download the desired language from <http://www.avaya.com/unicode>.
  2. If necessary, create a new translation, or modify an existing translation, using the Avaya Message Editing Tool (AMET), available at <http://support.avaya.com/amet>.

 **Note:**

Only the Avaya Message Editing Tool (AMET) can be used for translation edits, using any other editor will not update the Phone Message File correctly and such files will fail to install. See the *Avaya Message Editing Tool (AMET) Job Aid* in the Generic Phone Message Package file for more details on using AMET.

3. Transfer the Phone Message file to an Avaya S8XXX Server that is running Communication Manager 2.2 or later, using the Avaya Web pages, the Avaya Installation Wizard, or ftp.
4. Install Phone Message files with the Communication Manager System Management Interface (SMI). The Avaya Installation Wizard only supports install of Unicode Phone Message files. Note that the Installation Wizard is the same wizard that you use to transfer Phone Message files to an Avaya S8XXX Server that is running Communication Manager 2.2 or later.
5. The strings in a Communication Manager Phone Message File (avaya\_unicode[2-4].txt, custom\_unicode[2-4].txt, avaya\_user-defined.txt, custom\_user-defined.txt) are loaded in real-time into Communication Manager memory after you click the Install button on the “Communication Manager Phone Message File” page of Communication Manager SMI.
6. Set the **Display Language** field on the Station screen to `unicode`. Note that the keyword `unicode` only appears if a Unicode-capable telephone is entered in the Station screen **Type** field. To use a user-defined file, set the **Display Language** field on the Station screen to `user-defined`.

 **Note:**

There is no uninstall option for Phone Message files. You can reload a new Phone Message file. This will overwrite existing Phone Message files.

---

### **Checking the Status of Phone Message File Loads**

To verify that a Unicode Phone Message file is loaded correctly, run `status station xxxx` on any administered station. If the Unicode Phone Message file is loaded correctly, the **Display Messages Scripts** field on the second page contains the scripts that are in this file. The General Status screen for stations contains three Unicode script-related fields. To access the General Status screen, type `status station xxxx`, where `xxxx` is the extension of the station. The General Status screen appears. Click **Next** to display page 2 of the screen.

“Scripts” are a collection of symbols used to represent text in one or more writing systems. The three script fields shown in the UNICODE DISPLAY INFORMATION section are as follows:

- **Native Name Scripts:** Scripts supported in the Unicode station name.
- **Display Messages Scripts:** The scripts used in the Unicode Display Language.
- **Station Supported Scripts:** The scripts supported in the IP station that is registered to an extension.

## Unicode Native Name support

Communication Manager supports Unicode for the “Name” associated with Vector Directory Numbers (VDNs), trunk groups, hunt groups, agent login id, vector names, station names, Invalid Number Dialed Display (Feature-Related System Parameters screen) and Restricted Number Dialed Display (Feature-Related System Parameters screen). The **Unicode Name** (also referred to as Native Name and Name 2) fields are hidden fields that are associated with the name fields you administer on the respective screens for each. These fields can only be administered using Avaya Site Administration (ASA) or MultiSite Administrator (MSA).

- The Unicode VDN name is associated with the name administered in the **Name** field on the Vector Directory screen. You must use MSA.
- The Unicode Trunk Group name is associated with the name administered in the **Group Name** field on the Trunk Group screen. You must use MSA.
- The Unicode Hunt Group Name is associated with the name administered in the **Group Name** field on the Hunt Group screen. You must use MSA.
- The Unicode Station Name is associated with the name administered in the **Name** field on the Station screen. You must use ASA or MSA.

## Script Tags and Abbreviations

The following table defines the script tags and spells out the script abbreviations.

| Script Number | Script Tag Bit (hex) | Start Code.. End Code | Script or Block Name   | SAT Screen Name |
|---------------|----------------------|-----------------------|------------------------|-----------------|
| 1             | 00000001             | 0000..007F            | Basic Latin            | Latn            |
| 2             | 00000002             | 0080..00FF            | Latin-1 Supplement     | Lat1            |
| 3             | 00000004             | 0100..017F            | Latin Extended-A       | LatA            |
| 4             | 00000008             | 0180..024F            | Latin Extended-B       | LatB            |
| 5             | 00000010             | 0370..03FF            | Greek and Coptic       | GreK            |
| 6             | 00000020             | 0400..04FF            | Cyrillic               | Cyrl            |
| 6             | 00000020             | 0500..052F            | Cyrillic Supplementary | Cyrl            |
| 7             | 00000040             | 0530..058F            | Armenian               | ArmN            |
| 8             | 00000080             | 0590..05FF            | Hebrew                 | Hebr            |
| 9             | 00000100             | 0600..06FF            | Arabic                 | Arab            |
| 10            | 00000200             | 0900..097F            | Devanagari             | Deva            |
| 11            | 00000400             | 0980..09FF            | Bengali                | Beng            |
| 12            | 00000800             | 0A00..0A7F            | Gurmukhi               | Guru            |
| 13            | 00001000             | 0A80..0AFF            | Gujarati               | Gujr            |
| 14            | 00002000             | 0B00..0B7F            | Oriya                  | Orya            |

| Script Number              | Script Tag Bit (hex)                                     | Start Code.. End Code | Script or Block Name         | SAT Screen Name                      |
|----------------------------|--|-----------------------|------------------------------|--------------------------------------|
| 15                         | 00004000   | 0B80..0BFF            | Tamil                        | Taml                                 |
| 16                         | 00008000   | 0C00..0C7F            | Telugu                       | Telu                                 |
| 17                         | 00010000   | 0C80..0CFF            | Kannada                      | Knda                                 |
| 18                         | 00020000   | 0D00..0D7F            | Malayalam                    | Mlym                                 |
| 19                         | 00040000   | 0D80..0DFF            | Sinhala                      | Sinh                                 |
| 20                         | 00080000   | 0E00..0E7F            | Thai                         | Thai                                 |
| 21                         | 00100000   | 0E80..0EFF            | Lao                          | Lao                                  |
| 22                         | 00200000   | 1000..109F            | Myanmar                      | Mymr                                 |
| 23                         | 00400000   | 10A0..10FF            | Georgian                     | Geor                                 |
| 32                         | 80000000   | 1100..11FF            | Hangul Jamo                  | Hang                                 |
| 24                         | 00800000   | 1700..171F            | Tagalog                      | Tglg                                 |
| 25                         | 01000000   | 1780..17FF            | Khmer                        | Khmr                                 |
| 27<br>28<br>29<br>30<br>31 | 04000000<br>08000000<br>10000000<br>20000000<br>40000000 | 2E80..2EFF            | CJKV Radicals Supplement     | Jpan<br>ChiS<br>ChiT<br>Korn<br>Viet |
| 27<br>28<br>29<br>30<br>31 | 04000000<br>08000000<br>10000000<br>20000000<br>40000000 | 2F00..2FDF            | Kangxi Radicals              | Jpan<br>ChiS<br>ChiT<br>Korn<br>Viet |
| 27<br>28<br>29<br>30<br>31 | 04000000<br>08000000<br>10000000<br>20000000<br>40000000 | 3000..303F            | CJKV Symbols and Punctuation | Jpan<br>ChiS<br>ChiT<br>Korn<br>Viet |
| 27                         | 04000000   | 3040..309F            | Hiragana                     | Jpan                                 |
| 27                         | 04000000   | 30A0..30FF            | Katakana                     | Jpan                                 |
| 29                         | 10000000   | 3100..312F            | Bopomofo                     | ChiT                                 |
| 32                         | 80000000   | 3130..318F            | Hangul Compatibility Jamo    | Hang                                 |
| 29                         | 10000000   | 31A0..31BF            | Bopomofo Extended            | ChiT                                 |
| 27                         | 04000000   | 31F0..31FF            | Katakana Phonetic Extensions | Jpan                                 |

| Script Number              | Script Tag Bit (hex)                                     | Start Code.. End Code | Script or Block Name                | SAT Screen Name                      |
|----------------------------|--|-----------------------|-------------------------------------|--------------------------------------|
| 27<br>28<br>29<br>30<br>31 | 04000000<br>08000000<br>10000000<br>20000000<br>40000000 | 3200..32FF            | Enclosed CJK Letters and Months     | Jpan<br>ChiS<br>ChiT<br>Korn<br>Viet |
| 27<br>28<br>29<br>30<br>31 | 04000000<br>08000000<br>10000000<br>20000000<br>40000000 | 3300..33FF            | CJKV Compatibility                  | Jpan<br>ChiS<br>ChiT<br>Korn<br>Viet |
| 27<br>28<br>29<br>30<br>31 | 04000000<br>08000000<br>10000000<br>20000000<br>40000000 | 3400..4DBF            | CJKV Unified Ideographs Extension A | Jpan<br>ChiS<br>ChiT<br>Korn<br>Viet |
| 27<br>28<br>29<br>30<br>31 | 04000000<br>08000000<br>10000000<br>20000000<br>40000000 | 4E00..9FFF            | CJKV Unified Ideographs             | Jpan<br>ChiS<br>ChiT<br>Korn<br>Viet |
| 32                         | 80000000   | AC00..D7AF            | Hangul Syllables                    | Hang                                 |
| 27<br>28<br>29<br>30<br>31 | 04000000<br>08000000<br>10000000<br>20000000<br>40000000 | F900..FAFF            | CJK Compatibility Ideographs        | Jpan<br>ChiS<br>ChiT<br>Korn<br>Viet |
|                            | 00000100   | FB50..FDFF            | Arabic Presentation Forms-A         | Arab                                 |
| 27<br>28<br>29<br>30<br>31 | 04000000<br>08000000<br>10000000<br>20000000<br>40000000 | FE30..FE4F            | CJK Compatibility Forms             | Jpan<br>ChiS<br>ChiT<br>Korn<br>Viet |
|                            | 00000100   | FE70..FEFF            | Arabic Presentation Forms-B         | Arab                                 |
| 26                         | 02000000   | FF00..FFEF            | Halfwidth and Fullwidth Forms       | Kana                                 |

### **Administering displays for QSIG trunks**

Proper transmission of QSIG name data for display requires certain settings in the Trunk Group screen, the Signaling Group screen, and the System-Parameters Country-Options screen.

1. Make the following changes to the Trunk Group screen.

- a. Set **Group Type** to `ISDN`
  - b. Set **Character Set for QSIG Names** to `iso8859-1`
  - c. Set **Outgoing Display** to `y`
  - d. Set **Send Calling Number** to `y`
  - e. Set **Send Name** to `y`
2. On the Signaling Group screen, set **Supplementary Service Protocol** to `b`.
  3. On the System-Parameters Country-Options screen, set **Display Character Set** to `Roman`.

---

## Fixing Problems

| Symptom  | Cause and Solution  |
|--|---|
| Characters that display are not what you thought you entered.                              | This feature is case sensitive. Check the table to make sure that you entered the right case.   |
| You entered <code>~c</code> , and <code>*</code> appears on the display instead.           | Lower-case "c" has a specific meaning in Avaya Communication Manager, and therefore cannot be mapped to any other character. An asterisk "*" appears in its place.  |
| You entered <code>~-&gt;</code> or <code>~&lt;-</code> and nothing appears on the display. | These characters do not exist as single keys on the standard US-English keyboard. Therefore the system is not programmed to handle them.  |
| Enhanced display characters appear in fields that you did not update.                      | If an existing display field contains a tilde (~) followed by Roman characters, and you update and submit that screen after this feature is activated, that field will display the enhanced character set.                      |
| Nothing displays on the terminal at all.   | Some unsupported terminals do not display anything if a special character is presented. Check the model of display terminal that you are using.   |
| You entered a character with a descender and part of it appears cut off in the display.    | Some of the unused characters in Group2a have descenders that do not appear entirely within the display area. These characters are not included in the character map. For these characters (g,j,p,q,y), use Group1 equivalents. |

## Related Topics

See the Telephone Displays and the Administrable Display Languages feature descriptions in the *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205 for more information.

To view the dial pad letter/number/symbol mapping tables used for the integrated directory, see Telephone Display in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

## Setting the Directory Buttons

Your Communication Manager integrated directory contains the names and extensions that are assigned on each Station screen. Display-telephone users can use a telephone button to access the directory, use the touch-tone buttons to key in a name, and retrieve an extension from the directory.

### Note:

When you assign a name beginning with two tildes (~~) to a telephone, and **Display Character Set** on the System Parameters Country-Options screen is set to Roman, the name does not appear in the integrated directory. Note that this is the only way to hide a name in the integrated directory.

The example below shows how to assign directory telephone buttons for extension 2000.

Our button assignment plan is set up so that telephone buttons 6, 7, and 8 are used for the directory. Remember, the name you type in the **Name** field on the first page of the Station screen is the name that appears when the integrated directory is accessed on a telephone display, except when the name is “hidden”, as described in the Note above.

- 
1. Type `change station 2000`.
  2. Press `Enter`.
  3. Press `Next Page` to move to the **BUTTON ASSIGNMENTS** section on Station screen (page 4).
  4. In **Button Assignment** field 6, type `directory`.
  5. In **Button Assignment** field 7, type `next`.
  6. In **Button Assignment** field 8, type `call-display`.
  7. Press `Enter` to save your changes.
-

---

## Handling Incoming Calls

### Basic Call Coverage

#### What does call coverage do?

Basic incoming call coverage:

- Provides for automatic redirection of calls to alternate destinations when the called party is not available or not accepting calls
- Provides the order in which Communication Manager redirects calls to alternate telephones or terminals
- Establishes up to 6 alternate termination points for an incoming call
- Establishes redirection criteria that govern when a call redirects
- Redirects calls to a local telephone number (extension) or an off-switch telephone number (public network)

#### Redirection

Call coverage allows an incoming call to redirect from its original destination to an extension, hunt group, attendant group, uniform call distribution (UCD) group, direct department calling (DDC) group, automatic call distribution (ACD) split, coverage answer group, Audio Information Exchange (AUDIX), or vector for a station not accepting calls.

#### Administering system-wide call coverage characteristics

This section shows you how to set up system-wide call coverage characteristics that govern how coverage is handled.

The System Parameters Call Coverage/Call Forwarding screen sets up the global parameters which direct Communication Manager how to act in certain situations.

- 
1. Leave all default settings as they are set for your system.
  2. If you desire to customize your system, carefully read and understand each field description before you make any changes.  
For more information on redirecting calls, see *Covering calls redirected to an off-site location*.  
For information on setting the Caller Response Interval before a call goes to coverage, see “Caller Response Interval” in the Call Coverage section of *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

---

#### Creating coverage paths

This section explains how to administer various types of call coverage. In general, call coverage refers to what happens to incoming calls. You can administer paths to cover all incoming calls,

or define paths for certain types of calls, such as calls to busy telephones. You can define where incoming calls go if they are not answered and in what order they reroute to other locations. For example, you can define coverage to ring the called telephone, then move to a receptionist if the call is not answered, and finally access a voice mailbox if the receptionist is not available.

With call coverage, the system redirects a call to alternate answering extensions when no one answers at the first extension. An extension can have up to 6 alternate answering points. The system checks each extension in sequence until the call connects. This sequence of alternate extensions is called a coverage path.

The system redirects calls based on certain criteria. For example, you can have a call redirect to coverage without ever ringing on the principal set, or after a certain number of rings, or when one or all call appearances (lines) are busy. You can set coverage differently for internal (inside) and external (outside) calls, and you can define coverage individually for different criteria. For example, you can decide that external calls to busy telephones can use the same coverage as internal calls to telephones with Do Not Disturb active.

 **Note:**

If a call with a coverage path is redirected to a coverage point that is not available, the call proceeds to the next coverage point regardless of the type of coverage administered in the point that was unavailable. For example, if the unavailable coverage point has a hunt group coverage path administered, the hunt group coverage path would not be used by a call coming into the hunt group through the higher-level coverage path. The hunt group coverage path would be used only for calls coming directly into the hunt group extension.

- 
1. Type `add coverage path next`.
  2. Press `Enter`.  
The system displays the Coverage Path screen. The system displays the next undefined coverage path in the sequence of coverage paths. Our example shows coverage path number 2.
  3. Type a coverage path number in the **Next Path Number** field.  
The next path is optional. It is the coverage path to which calls are redirected if the current path's coverage criteria does not match the call status. If the next path's criteria matches the call status, it is used to redirect the call; no other path is searched.
  4. Fill in the **Coverage Criteria** fields.  
You can see that the default sets identical criteria for inside and outside calls. The system sets coverage to take place from a busy telephone, if there is no answer after a certain number of rings, or if the **DND** (do not disturb), **SAC** (send all calls), or **Go to Cover** button has been pressed or corresponding feature-access codes dialed.
  5. Fill in the **Point** fields with the extensions, hunt group number, or coverage answer group number you want for coverage points.

Each coverage point can be an extension, hunt group, coverage answer group, remote number, or attendant.

6. Click **Enter** to save your changes.

 **Tip:**

If you want to see which extensions or groups use a specific coverage path, type `display coverage sender group n`, where `n` is the coverage path number. For example, you should determine which extensions use a coverage path before you make any changes to it.

---

### **Assigning a coverage path to users**

Once you create a coverage path, assign it to a user. For example, we will assign the new coverage path to extension 2045.

 **Note:**

A coverage path can be used for more than one extension.

- 
1. Type `change station 2054`.
  2. Press `Enter`.  
The system displays the Station screen for extension 2054.
  3. Type `2` in the **Coverage Path 1** field.  
To give extension 2054 another coverage path, you can type a coverage path number in the **Coverage Path 2** field.
  4. Press `Enter` to save your changes.
- 

## **Advanced call coverage**

Advanced incoming call coverage:

- redirects calls based on time-of-day.
- allows coverage of calls that are redirected to sites not on the local server running Communication Manager.
- allows users to change back and forth between two coverage choices (either specific lead coverage paths or time-of-day tables).

## Covering calls redirected to an off-site location

### Prerequisites

- On the System Parameters Customer-Options (Optional Features) screen, verify the **Coverage of Calls Redirected Off-Net Enabled** field is *y*. If not, contact your Avaya representative.
- You need call classifier ports for all situations except ISDN end-to-end signaling, in which case the ISDN protocol does the call classification. For all other cases, use one of the following:
  - Tone Clock with Call Classifier - Tone Detector circuit pack. See the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207 for more information on the circuit pack.
  - Call Classifier - Detector circuit pack.

---

You can provide coverage for calls that have been redirected to an off-site location (for example, your home). This capability, called Coverage of Calls Redirected Off-Net (CCRON) allows you to redirect calls onto the public network and bring back unanswered calls for further coverage processing.

- 
1. Type `change system-parameters coverage-forwarding`.
  2. Press `Enter`.
  3. Click **Next Page** until you see the **Coverage of Calls Redirected Off-Net (CCRON)** page of the System-Parameters Coverage-Forwarding screen.
  4. In the **Coverage of Calls Redirected Off-Net Enabled** field, type *y*.  
This instructs Avaya Communication Manager to monitor the progress of an off-net coverage or off-net forwarded call and provide further coverage treatment for unanswered calls.
  5. In the **Activate Answer Detection (Preserves SBA) On Final CCRON Cvg Point** field, leave the default as *y*.
  6. In the **Ignore Network Answer Supervision** field, leave the default as *n*.
  7. Click **Enter** to save your changes.
- 

### Defining coverage for calls redirected to external numbers

You can administer the system to allow calls in coverage to redirect to off-net (external) or public-network numbers.

Standard remote coverage to an external number allows you to send a call to an external telephone, but does not monitor the call once it leaves your system. Therefore, if the call is busy or not answered at the external number, the call cannot be pulled back to the system. With standard remote call coverage, make the external number the last coverage point in a path.

With newer systems, you might have the option to use the Coverage of Calls Redirected Off-Net feature. If this feature is active and you use an external number in a coverage path, the

system can monitor the call to determine whether the external number is busy or does not answer. If necessary, the system can redirect a call to coverage points that follow the external number. With this feature, you can have a call follow a coverage path that starts at the user's extension, redirects to the user's home telephone, and if not answered at home, returns to redirect to their voice mail box.

The call will not return to the system if the external number is the last point in the coverage path.

To use a remote telephone number as a coverage point, you need to define the number in the Remote Call Coverage Table and then use the remote code in the coverage path.

For example, to add an external number to coverage path 2:

- 
1. Type `change coverage remote`.
  2. Press `Enter`.  
The system displays the Remote Call Coverage Table screen.
  3. Type `93035381000` in one of the remote code fields.  
If you use a digit to get outside of your network, you need to add the digit before the external number. In this example, the system requires a '9' to place outside calls.
  4. Be sure to record the remote code number you use for the external number.  
In this example, the remote code is `r01`.
  5. Click **Enter** to save your changes.
  6. Type `change coverage path 2`.
  7. Press `Enter`.  
The system displays the Coverage Path screen.  
 **Tip:**  
Before making changes, you can use `display coverage sender group 2` to determine which extensions or groups use path 2.
  8. Type `r1` in a coverage **Point** field.  
In this example, the coverage rings at extension 4101, then redirects to the external number. If you administer Coverage of Calls Redirected Off-Net and the external number is not answered or is busy, the call redirects to the next coverage point. In this example, the next point is Point 3 (h77 or hunt group 77).  
If you do not have the Coverage of Calls Redirected Off-Net feature, the system cannot monitor the call once it leaves the network. The call ends at the remote coverage point.
  9. Click **Enter** to save your changes.

**Note:**

For more information on coverage, see "Call Coverage" in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

---

## Defining time-of-day coverage

The Time of Day Coverage Table on your system lets you redirect calls to coverage paths according to the time of day and day of the week when the call arrives. You need to define the coverage paths you want to use before you define the time of day coverage plan.

For example, let us say you want to administer the system so that incoming calls to extension 2054 redirect to a coworker in the office from 8:00 a.m. to 5:30 p.m., and to a home office from 5:30 p.m. to 8:00 p.m. on weekdays. You want to redirect the calls to voice mail after 8:00 p.m. weekdays and on weekends.

- 
1. Type `add coverage time-of-day next`.
  2. Press `Enter`.  
The system displays the Time of Day Coverage Table screen, and selects the next undefined table number in the sequence of time-of-day table numbers. If this is the first time-of-day coverage plan in your system, the table number is 1.  
  
Record the table number so that you can assign it to extensions later.
  3. To define your coverage plan, enter the time of day and path number for each day of the week and period of time.  
Enter time in a 24-hour format from the earliest to the latest. For this example, assume that coverage path 1 goes to the coworker, path 2 to the home, and path 3 to voice mail.  
  
Define your path for the full 24 hours (from 00:01 to 23:59) in a day. If you do not list a coverage path for a period of time, the system does not provide coverage for that time.
  4. Click **Enter** to save your changes.
  5. Now assign the time-of-day coverage to a user. For example, we use extension 2054:
    - a. Type `change station nnnn`, where `nnnn` is the extension number.
    - b. Press `Enter`.  
The system displays the Station screen.
    - c. Move your cursors to Coverage Path 1 and type `t` plus the number of the Time of Day Coverage Table.
    - d. Click **Enter** to save your changes.

Now calls to extension 2054 redirect to coverage depending on the day and time that each call arrives.

---

### Creating coverage answer groups

You can create a coverage answer group so that up to 8 telephones simultaneously ring when calls cover to the group. Anyone in the answer group can answer the incoming call.

- 
1. Enter `add coverage answer-group next`.
  2. In the **Group Name** field, enter a name to identify the coverage group.
  3. In the **Ext** field, type the extension of each group member.
  4. Select **Enter** to save your new group list.

The system automatically completes the Name field when you press Enter.

---

## Call Forwarding

This section explains how to administer various types of automatic call forwarding. To provide call forwarding to your users, assign each extension a class of service (COS) that allows call forwarding. Then assign call-forwarding buttons to the user telephones (or give them the feature access code (FAC) for call forwarding) so that they can easily forward calls. Use the Station screen to assign the COS and any call-forwarding buttons.

Within each class of service, you can determine whether the users in that COS have the following call forwarding features:

- Call Forwarding All Calls — allows users to redirect all incoming calls to an extension, attendant, or external telephone number.
- Call Forwarding Busy/Don't Answer — allows users to redirect calls only if their extensions are busy or they do not answer.
- Restrict Call Fwd-Off Net — prevents users from forwarding calls to numbers that are outside your system network.

As the administrator, you can administer system-wide call-forwarding parameters to control when calls are forwarded. Use the System Parameters Call Coverage/Call Forwarding screen to set the number of times an extension rings before the system redirects the call because the user did not answer (CFWD No Answer Interval). For example, if you want calls to ring 4 times at an extension and, if the call is not answered, redirect to the forwarding number, set this parameter to 4.

You also can use the System Parameters Call Coverage/Call Forwarding screen to determine whether the forwarded-to telephone can override call forwarding to allow calls to the forwarded-from telephone (Call Forward Override). For example, if an executive forwards incoming calls

to an attendant and the attendant needs to call the executive, the call can be made only if the **Call Forwarding Override** field is set to *y*.

### Determining extensions having call forwarding activated

- 
1. Type `list call-forwarding`.
  2. Press `Enter`.  
This command lists all the extensions that are forwarded along with each forwarding number.



#### Note:

If you have a V1, V2, or V3 system, you can see if a specific extension is forwarded only by typing `status station nnnn`, where *nnnn* is the specific extension.

For more information see “Call Forwarding” in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

---

### Setting up call forwarding for users

This section shows you how to give your users access to call forwarding.

We will change a call forwarding access code from a local telephone with a Class of Service of 1:

- 
1. Type `change feature-access-codes`.
  2. Press `Enter`.  
The system displays the Feature Access Code (FAC) screen.
  3. In the **Call Forwarding Activation Busy/DA** field, type `*70`.  
The `*70` feature access code activates the call forwarding option so incoming calls forward when your telephone is busy or does not answer.
  4. In the **Call Forwarding Activation All** field, type `*71`.  
The `*71` feature access code forwards all calls.
  5. In the **Call Forwarding Deactivation** field, type `#72`.  
The `#72` feature access code deactivates the call forwarding option.
  6. Press `Enter` to save your changes.
  7. Type `change cos`.
  8. Press `Enter`.  
The system displays the Class of Service screen.
  9. On the **Call Fwd-All Calls** line, in the 1 column, type `y`.  
This allows the user with this Class of Service to forward their calls. The 1 column is for telephones with a Class of Service of 1.

10. On the **Console Permissions** line, in the 1 column, type `y`.  
This allows the user to define call forwarding on any station, not just the dialing station.
11. On the **Restrict Call Fwd-Off Net** line, in the 1 column, type `y`.  
This restricts your users from forwarding calls off-site. If you want your users to be able to call off-site, leave this field as `n`.
12. On the **Call Forward Busy/DA** line, in the 1 column, type `y`.  
This forwards a user's calls when the telephone is busy or doesn't answer after a programmed number of rings.
13. Press `Enter` to save your changes.

---

### Allowing users to specify a forwarding destination

Now that you have set up system-wide call forwarding, have your users use this procedure if they want to change their call forwarding destination from their work (local) station.

- 
1. They dial either their Call Forwarding Activation Busy/DA or Call Forwarding Activation All feature access code. If your users have buttons assigned, they press those buttons, listen for dial tone, and dial the digits.



**Note:**

Both Call Forwarding Activation Busy/DA or the Call Forwarding Activation All cannot be active for the same telephone at the same time.

In this example, enter `*71` for Call Forwarding Activation All.

2. They dial their "forwarding-to" off-site or on-site number.  
In this example, enter `2081`. This is a local number; for off-site forwarding, include the AAR/ ARS feature access code.
3. When they hear the 3-beep confirmation tone, they hang up.

---

### Changing the forwarding destination remotely

Now that you have set up all of the required system administration for call forwarding, have your users use this procedure if they want to change their call forwarding destination from a telecommuting (off-site) telephone.

- 
1. They dial their telecommuting extension.  
In this example, enter `555-9126`.
  2. When they get dial tone, they dial either their Extended Call Forward Activate Busy/DA or the Extended Call Forward Activate All feature access code.  
In this example, enter `*61` for the Extended Call Forward Activate All number.

3. When they get dial tone, they dial their extension number. Press the #.  
In this example, enter 1014, then #.
4. Even though there is no dial tone, they dial their security code. Press #.  
In this example, enter 4196, then #.
5. When they get dial tone, they dial their "forwarding-to" off-site or on-site number.  
In this example, enter 9-555-2081.
6. When they hear the 3-beep confirmation tone, they hang up.

---

### Allowing users to change coverage remotely

This section shows you how to allow users to change their call coverage path from a local or telecommuting (off-site) telephone.

- 
1. Type `change feature-access-codes`.
  2. Press `Enter`.  
The system displays the Feature Access Code (FAC) screen.
  3. In the **Change Coverage Access Code** field, type `*85`.  
Use the `*85` feature access code to change a coverage path from a telephone or remote station.
  4. Press `Enter` to save your changes.
  5. Type `change cor`.
  6. Press `Enter`.  
The system displays the Class of Restriction screen.
  7. In the **Can Change Coverage** field, type `y`.  
This permits users to select one of two previously administered coverage paths.
  8. Press `Enter` to save your changes.
  9. Type `change station 1014`.
  10. Press `Enter`.  
The system displays the Station screen for extension 1014.
  11. In the **Security Code** field, type `4196`.  
In this example, this is your security code.
  12. In the **Coverage Path 1** and **Coverage Path 2** fields, verify that both are defined enabling your user to move from one coverage path to another.  
The `t1` and `t2` are the numbers of the Time of Day Coverage Tables.
  13. Press `Enter` to save your changes.
-

## Enhanced Call Forwarding

There are three types of Enhanced Call Forwarding:

- Use Enhanced Call Forwarding Unconditional to forward all calls
- Use Enhanced Call Forwarding Busy to forward calls when the user's line is busy
- Use Enhanced Call Forwarding No Reply to forward calls when the user does not answer the call

The user can activate or deactivate any of these three types from their phone, and can specify different destinations for calls that are from internal and external sources. Users receive visual display and audio feedback on whether or not Enhanced Call Forwarding is active.

Display messages on the phone guide the user through the process of activating and deactivating Enhanced Call Forwarding, and for viewing the status of their forwarding.

Users can choose whether they want, at any one time, Call Forwarding or Enhanced Call Forwarding activated. The regular Call Forwarding feature (called "Classic Call Forwarding" to distinguish it from Enhanced Call Forwarding) continues to be available to users and has not changed.

Each of the three types of Enhanced Call Forwarding can have different destinations based on whether a call is internal or external. Therefore, six different destinations are possible to set up:

- Enhanced Call Forwarding Unconditional - internal
- Enhanced Call Forwarding Unconditional - external
- Enhanced Call Forwarding Busy - internal
- Enhanced Call Forwarding Busy - external
- Enhanced Call Forwarding No Reply - internal
- Enhanced Call Forwarding No Reply - external.

Each of these types of call forwarding can be activated either by feature access codes or by feature button.

When Enhanced Call Forwarding is deactivated, the destination number is kept. When the user activates Enhanced Call Forwarding again, the same destination number can be used without having to type it again.

When Enhanced Call Forwarding is not activated for a call, the call will go to a coverage path, if one has been set up.

### Redirection

Call coverage allows an incoming call to redirect from its original destination to an extension, hunt group, attendant group, uniform call distribution (UCD) group, direct department calling (DDC) group, automatic call distribution (ACD) split, coverage answer group, Audio Information Exchange (AUDIX), or vector for a station not accepting calls.

## Activating Enhanced Call Forwarding Using a feature button

---

1. Press the feature button labeled cfwd-enh  
The phone goes off hook.
2. Press 1 to activate Enhanced Call Forwarding.
3. Press
  - 1 for Enhanced Call Forwarding Unconditional
  - 2 for Enhanced Call Forwarding Busy
  - 3 for Enhanced Call Forwarding No Reply
4. Press
  - 1 to forward internal calls
  - 2 to forward external calls
  - 3 to forward all calls
5. Dial the destination number to which calls will be forwarded.  
Dial # at the end of an external destination number, or wait for the timeout to expire.  
You hear a confirmation tone if the activation was successful.

## Activating Enhanced Call Forwarding Using a feature access code

---

1. Press the feature access code for activating Enhanced Call Forwarding.  
The phone goes off hook.
  2. Press
    - 1 for Enhanced Call Forwarding Unconditional
    - 2 for Enhanced Call Forwarding Busy
    - 3 for Enhanced Call Forwarding No Reply
  3. Press
    - 1 to forward internal calls
    - 2 to forward external calls
    - 3 to forward all calls
  4. Dial the destination number to which calls will be forwarded.  
Dial # at the end of an external destination number, or wait for the timeout to expire.  
You hear a confirmation tone if the activation was successful.
-

## Deactivating enhanced call forwarding using a feature button

---

1. Press the feature button labeled **cfwd-enh**.  
The phone goes off hook.
  2. Press 2 to deactivate Enhanced Call Forwarding.
  3. Press
    - 0 for all Enhanced Call Forwarding
    - 1 for Enhanced Call Forwarding Unconditional
    - 2 for Enhanced Call Forwarding Busy
    - 3 for Enhanced Call Forwarding No Reply
  4. Press
    - 1 for internal calls
    - 2 for external calls
    - 3 for all calls
- You hear a confirmation tone if the deactivation was successful.

---

## Deactivating enhanced call forwarding using a feature access code

---

1. Press the feature access code for deactivating Enhanced Call Forwarding.  
The phone goes off hook.
  2. Press
    - 0 to deactivate all Enhanced Call Forwarding
    - 1 to deactivate Enhanced Call Forwarding Unconditional
    - 2 to deactivate Enhanced Call Forwarding Busy
    - 3 to deactivate Enhanced Call Forwarding No Reply
  3. Press
    - 1 for internal calls
    - 2 for external calls
    - 3 for all calls
- You hear a confirmation tone if the deactivation was successful.
-

## Reactivating enhanced call forwarding using a feature button

---

1. Press the feature button labeled **cfwd-enh**.  
The phone goes off hook.
2. Press 1 to reactivate Enhanced Call Forwarding
3. Press
  - 1 for Enhanced Call Forwarding Unconditional
  - 2 for Enhanced Call Forwarding Busy
  - 3 for Enhanced Call Forwarding No Reply
4. Press
  - 1 to forward internal calls
  - 2 to forward external calls
  - 3 to forward all calls
5. Optionally, dial the destination number to which calls will be forwarded.  
If you do not enter a destination number, the previous destination number will be used.  
Dial # at the end of an external destination number, or wait for the timeout to expire.  
  
You hear a confirmation tone if the action was successful.

## Reactivating enhanced call forwarding using a feature access code

---

1. Press the feature access code for activating Enhanced Call Forwarding.  
The phone goes off hook.
2. Press
  - 1 for Enhanced Call Forwarding Unconditional
  - 2 for Enhanced Call Forwarding Busy
3. Press
  - 1 to forward internal calls
  - 2 to forward external calls
  - 3 to forward all calls
4. Optionally, dial the destination number to which calls will be forwarded.  
If you do not enter a destination number, the previous destination number will be used.

Dial # at the end of an external destination number, or wait for the timeout to expire.

You hear a confirmation tone if the action was successful.

---

### Displaying Enhanced Call Forwarding Status Using a Feature Button

---

1. Press the feature button labeled **cfwd-enh**.  
The phone goes off hook.
2. Press 3 to display status.  
Your phone will display the status of the different types of Enhanced Call Forwarding.

---

### Displaying Enhanced Call Forwarding Status Using a Feature Access Code

---

1. Press the feature access code for displaying Enhanced Call Forwarding status..  
The phone goes off hook.
2. Press 3 to display status.  
Your phone will display the status of the different types of Enhanced Call Forwarding.

---

### Activating Enhanced Call Forwarding from an off-network phone

---

1. Dial the remote access number, including barrier code or authentication code.
2. Press the feature access code for activating Enhanced Call Forwarding.
3. Press:
  - 1 for Enhanced Call Forwarding Unconditional
  - 2 for Enhanced Call Forwarding Busy
  - 3 for Enhanced Call Forwarding No Reply
4. Press
  - 1 to forward internal calls
  - 2 to forward external calls
  - 3 to forward all calls
5. Dial the forwarding station extension.
6. Dial the destination number to which calls will be forwarded.  
Dial # at the end of an external destination number, or wait for the timeout to expire.

You hear a confirmation tone if the activation was successful.

---

### Deactivating Enhanced Call Forwarding from an off-network phone

---

1. Dial the remote access number, including barrier code or authentication code.
2. Press the feature access code for deactivating Enhanced Call Forwarding.
3. Press:
  - 0 for all Enhanced Call Forwarding
  - 1 for Enhanced Call Forwarding Unconditional
  - 2 for Enhanced Call Forwarding Busy
  - 3 for Enhanced Call Forwarding No Reply
4. Press
  - 1 for internal calls
  - 2 for external calls
  - 3 for all calls
5. Dial the forwarding station extension.
6. Dial the destination number to which calls will be forwarded.  
You hear a confirmation tone if the activation was successful.

---

### Activating Enhanced Call Forwarding from a phone with console permissions

---

1. Press the feature access code for activating Enhanced Call Forwarding.  
The phone goes off hook.
  2. Press:
    - 1 to forward internal calls
    - 2 to forward external calls
    - 3 to forward all calls
  3. Dial the forwarding station extension.
  4. Dial the destination number to which calls will be forwarded.  
Dial # at the end of an external destination number, or wait for the timeout to expire.  
You hear a confirmation tone if the activation was successful.
-

## Deactivating Enhanced Call Forwarding from a phone with console permission

- 
1. Press the feature access code for activating Enhanced Call Forwarding.  
The phone goes off hook.
  2. Press:
    - 0 for all Enhanced Call Forwarding
    - 1 for Enhanced Call Forwarding Unconditional
    - 2 for Enhanced Call Forwarding Busy
- 

## Night Service

You can use night service to direct calls to an alternate location when the primary answering group is not available. For example, you can administer night service so that anyone in your marketing department can answer incoming calls when the attendant is at lunch or has left for the day.

Once you administer night service to route calls, your end-users merely press a button on the console or a feature button on their telephones to toggle between normal coverage and night service.

There are five types of night service:

- Night Console Night Service — directs all attendant calls to a night or day/night console
- Night Station Night Service — directs all incoming trunk or attendant calls to a night service destination
- Trunk Answer from Any Station (TAAS) — directs incoming attendant calls and signals a bell or buzzer to alert other employees that they can answer the calls
- Trunk Group Night Service — directs incoming calls to individual trunk groups to a night service destination
- Hunt Group Night Service — directs hunt group calls to a night service destination

### Setting up night station service to voice mail

The night station service (also known as Listed Directory Number (LDN) Night Service) sends calls directed to an LDN to voice mail when the system is in night service.

What is described below is a common setup; however, you can use a regular extension in this field, but it will not follow coverage.

 **Note:**

You can use a dummy hunt group (one with no members) or an exported station with a coverage path. The instructions below use a hunt group.

- 
1. Type `add hunt-group` next.
  2. Press `Enter`.  
The system displays the Hunt Group screen.  
The **Group Number** field fills automatically with the next hunt group number.
  3. In the **Group Name** field, type the name of the group.  
In our example, type `ldn nights`. There should be no members in this hunt group.
  4. Click **Enter** to save your changes.

 **Note:**

If you are using tenant partitioning, the command for the next step will be `change tenant x`. If you are using tenant partitioning, the **Night Destination** field does not appear on the Listed Directory Numbers screen. Instead, it is on the Tenant screen.

5. Type `change listed-directory-numbers`.
6. Press `Enter`.  
The system displays the Listed Directory Numbers screen.
7. In the **Night Destination** field, add the night destination on the listed directory telephone.  
In our example, type `51002`.
8. Click **Enter** to save your changes.
9. Type `change console-parameters`.
10. Press `Enter`.  
The system displays the Console Parameters screen.
11. In the **DID-LDN Only to LDN Night Ext** field, type `n`.
12. Click **Enter** to save your changes.
13. From a telephone with console permissions, dial the call forwarding feature access code, then the hunt group's extension, followed by the main number of AUDIX.  
In our example, dial `51002`.

 **Note:**

You should receive the confirmation tone (3 beeps). This step is very important as calls to the LDN night service extension do not follow coverage.

14. In voice mail, build your auto attendant with the extension of the Listed Directory Number, not the hunt group.  
The originally dialed number was the LDN. That is what Communication Manager passes to the voice mail. In the case of the INTUITY and newer embedded AUDIX

Voice Mail systems, you can use the Auto Attendant routing table to send the calls to a common Auto Attendant mailbox.

---

### Setting up night console service

Night Console Service directs all calls for primary and daytime attendant consoles to a night console. When a user activates Night Console Service, the Night Service button for each attendant lights and all attendant-seeking calls (and calls waiting) in the queue are directed to the night console.

 **Note:**

Activating night console service also puts trunk groups into night service, except those for which a night service button has been administered. See *Setting up trunk answer from any station* on page 244 for more information.

To activate and deactivate Night Console Service, the attendant typically presses the Night button on the principal attendant console or designated console.

Only the principal console can activate night service. In the absence of any console, a telephone can activate night service.

We will put the attendant console (attendant 2) in a night service mode.

- 
1. Type `change attendant`.
  2. Press `Enter`.  
The system displays the Attendant Console screen.
  3. In the **Console Type** field, type `principal`.  
There can be only one night-only or one day/night console in the system unless you administer Tenant Partitioning. Night Service is activated from the principal console or from the one station set per-system that has a **nite-serv** button.
  4. Click **Enter** to save your changes.

---

### Setting up night station service

You can use night station service if you want to direct incoming trunks calls, DID-LDN (direct inward dialing-listed directory number) calls, or internal calls to the attendant (dialed 'O' calls) to a night service destination.

Let us say your attendant, who answers extension (LDN) 8100, usually goes home at 6:00 p.m. When customers call extension 8100 after hours, you would like them to hear an announcement that asks them to try their call again in the morning.

To set up night station service, you need to record the announcement (in our example, it is recorded at announcement extension 1234).

 **Tip:**

All trunk groups that are routed through the attendant direct to this night service destination provided they already do not have a night service destination and, on the Console

Parameters screen, the **DID-LDN Only to DID-LDN Night Ext** field is *n*. See *Setting up trunk answer from any station*.

- 
1. Type `change listed-directory-numbers`.
  2. Press `Enter`.  
The system displays the Listed Directory Numbers screen.
  3. Enter `1234` in the **Night Destination** field.  
The destination can be an extension, a recorded announcement extension, a vector directory number, or a hunt group extension.
  4. Click **Enter** to save your changes.
  5. Type `change console-parameters`.
  6. Press `Enter`.  
The system displays the Console Parameters screen.
  7. In the **DID-LDN Only to LDN Night Extension** field, type *n*.
  8. Click `Enter` to save your changes.  
After you set up night station service, have the attendant use the night console button to activate and deactivate night service.

---

### Setting up trunk answer from any station

There might be situations where you want everyone to be able to answer calls when the attendant is away. Use trunk answer any station (TAAS) to configure the system so that it notifies everyone when calls are ringing. Then, you can give users the trunk answer any station feature access code so they can answer these calls.

When the system is in night service mode, attendant calls redirect to an alerting device such as a bell or a buzzer. This lets other people in the office know when they should answer the telephone.

 **Note:**

If no one answers the call, the call will not redirect to night service.

We will define a feature access code (we'll use 71) and configure the alerting device for trunk answer any station.

You need a ringing device and 1 port on an analog line circuit pack. See the *Avaya Aura™ Communication Manager Hardware Description and Reference*, 555-245-207, for more information on the circuit pack.

- 
1. Type `change feature-access-codes`.
  2. Press `Enter`,  
The system displays the Feature Access Code (FAC) screen.

3. Click **Next** until you see the **Trunk Answer Any Station Access Code** field.
4. In the **Trunk Answer Any Station Access Code** field, type 71.
5. Click **Enter** to save your changes.  
Once you set the feature access code, determine where the external alerting device is connected to the Communication Manager server (we'll use port 01A0702).  
To set up external alerting:
6. Type `change console-parameters`.
7. Press `Enter`.  
The system displays the Console Parameters screen.
8. In the **EXT Alert Port (TAAS)** field, type 01A0702.  
Use the port address assigned to the external alerting device.
9. In the **EXT Alert Port (TAAS)** field, type 01A0702.
10. Click **Enter** to save your changes.

---

### **Setting up external alerting**

- 
1. Type `change console-parameters`.
  2. Press `Enter`.  
The system displays the Console Parameters screen.
  3. In the **EXT Alert Port (TAAS)** field, type 01A0702.  
Use the port address assigned to the external alerting device.
  4. Click **Enter** to save your changes.

---

### **Setting up external alerting night service**

Calls redirected to the attendant via Call Forwarding or Call Coverage will not go to the LDN Night Station. If there is no night station specified, and the TAAS bell is being used, these calls ring the TAAS bell. A call following the coverage path rings the TAAS bell for the number of times indicated in the Coverage Don't Answer Interval for Subsequent Redirection (Rings) field. If not answered, the call proceeds to the next point in the station's coverage path. If the call was sent to the Attendant by Call Forwarding, it continues to ring the TAAS bell.

When night service is enabled, and there is a night service destination on the Listed Directory Numbers screen, calls covering to the attendant attempt to ring the night destination instead of the attendant position even if the handset is plugged in.

To send LDN calls to the attendant during the day and to a guard's desk at night:

- 
1. Type `change listed-directory-numbers`.
  2. Press `Enter`.  
The system displays the Listed Directory Numbers screen.
  3. In the **Night Destination** field, verify this field is blank.
  4. Click **Enter** to save your changes.
  5. Type `change console-parameters`.
  6. Press `Enter`.  
The system displays the Console Parameters screen.
  7. In the `EXT Alert Port (TAAS)` field, type `01A0702`.  
This is the port address assigned to the external alerting device.
  8. Click **Enter** to save your changes.  
The system is in Night Service.  
Any calls to extension 2000 now go to extension 3000 (the guard's desk).  
Any "0" seeking calls go to extension 3000 (the guard's desk).

---

### **Sending LDN calls to the attendant during the day and to the TAAS bell at night**

- 
1. Type `change console-parameters`.
  2. Press `Enter`.  
The system displays the Console Parameters screen.
  3. In the **DID-LDN Only to Night Ext?** field, type `y`.  
This allows only listed directory number calls (LDN) to go to the listed directory night service number extension.
  4. In the **Ext Alert Port (TAAS)** field, type `01A070`.  
This is the port address assigned to the external alerting device.
  5. Click **Enter** to save your changes.  
Any DNIS extension 2000 calls now go to the TAAS bell.  
Any "0" seeking calls now go to the TAAS bell.

---

### **Setting up trunk group night service**

You can use trunk group night service if you want to direct individual trunk groups to night service. The system redirects calls from the trunk group to the group's night service destination.

Trunk group night service overrides night station service. For example, we will say you activate trunk group night service, and then your attendant activates night station service. In this case,

calls to the trunk group use the trunk night service destination, rather than the station night service destination.

We will direct night calls for trunk group 2 to extension 1245.

- 
1. Type `change trunk-group`.
  2. Press `Enter`.  
The system displays the Trunk Group screen.
  3. Type `1245` in the **Night Service** field.  
The destination can be a station extension, a recorded announcement extension, a vector directory number, a hunt group extension, a terminating extension group, or `attd` if you want to direct the call to the attendant.
  4. Click **Enter** to save your changes.

---

### Setting up night service for hunt groups

You can administer hunt group night service if you want to direct hunt group calls to a night service destination.

Let us say your helpline on hunt group 3 does not answer calls after 6:00 p.m. When customers call after hours, you would like them to hear an announcement that asks them to try their call again in the morning.

To set up night service for your helpline, you need to record the announcement (in our example, the announcement is on extension 1234) and then modify the hunt group to send calls to this extension.

- 
1. Type `change hunt-group`.
  2. Press `Enter`.  
The system displays the Hunt Group screen for hunt group 3.
  3. In the **Night Service Destination** field, type `1234`.  
The destination can be an extension, a recorded announcement extension, a vector directory number, a hunt group extension, or `attd` if you want to direct calls to the attendant.  
Calls to hunt group 3 will follow the coverage path assigned to extension 1234.
  4. Click **Enter** to save your changes.
  5. Now you need to program a night service button.

---

### Related topics:

[Hunt Groups](#) on page 304

## Call Pickup

Users might need to answer a call that is ringing at a nearby desk. With Communication Manager, a user can answer a call that is ringing at another telephone in three ways:

- Use Call Pickup. With Call Pickup, you create one or more pickup groups. A pickup group is a collection, or list, of individual telephone extensions. A pickup group is the way to connect individual extensions together. For example, if you want everyone in the payroll department to be able to answer calls to any other payroll extension, you can create a pickup group that contains all of the payroll extensions.

A user extension can belong to only one pickup group. Also, the maximum number of pickup groups might be limited by your system configuration.

Using their own telephones, all members in a pickup group can answer a call that is ringing at another group member telephone. If more than one telephone is ringing, the system selects the extension that has been ringing the longest.

- Use Extended Call Pickup. With Extended Call Pickup, you can define one or more extended pickup groups. An extended pickup group is the way to connect individual pickup groups together.

There are two types of extended pickup groups: simple and flexible. You administer the type of extended pickup groups on a system-wide basis. You cannot have both simple and flexible extended pickup groups on your system at the same time.

Based on the type of extended pickup group that you administer, members in one pickup group can answer calls to another pickup group.

For more information, see *Setting up simple extended pickup groups*, *Setting up flexible extended pickup groups*, and *Changing extended pickup groups*.

- Use Directed Call Pickup. With Directed Call Pickup, users specify what ringing telephone they want to answer. A pickup group is not required with Directed Call Pickup. You must first administer Directed Call Pickup before anyone can use this feature.

For more information, see *Setting up Directed Call Pickup*.

Throughout this procedure on pickup groups and extended pickup groups, we show examples to make Call Pickup easier to understand.

### Call Pickup Alert

Members of a call pickup group know that another group member is receiving a call in two ways:

- Group members can hear the other telephone ring.
- The Call Pickup button status lamp on the telephones of all the group members flash.



**Note:**

You must activate Call Pickup Alerting in your system, and assign a Call Pickup button to the telephones of each pickup group member, before the Call Pickup button status lamps work properly.

For information how to set up Call Pickup Alerting, see Enabling Call Pickup Alerting.

If the **Call Pickup Alerting** field on the Feature-Related System Parameters screen is set to n , members of the call pickup group must rely only on ringing to know when another group member receives a call. Pickup group members must be located close enough that they can hear the ringing of the other telephones.

To answer a call, a pickup group member can either press the Call Pickup button on the telephone, or dial the Call Pickup feature access code (FAC).

For more information, see Assigning a Call Pickup button to a user telephone, and Assigning a Call Pickup feature access code.

The Call Pickup Alerting feature is enhanced to support the SIP telephones. You need to upgrade the SIP telephone firmware 2.6 to take advantage of call pickup alerting on SIP telephones. You can activate an audible and a visual alert at a SIP telephone by administering the **Call Pickup Ring Type** and **Call Pickup Indication** fields available under the Screen and Sound Options menu on the SIP telephones.

For more information on how to administer the audible and visual alerting, see the user guide for your SIP telephone.

The **Call Pickup Alerting** field on the Feature-Related System Parameters screen determines how the Call Pickup button status lamps operate.

- If the **Call Pickup Alerting** field is set to n, the Call Pickup Button status lamps on all pickup group member telephones do not flash when a call comes in. When a pickup group member hears the telephone of another group member ring and presses the Call Pickup button to answer the call, the:
  - Call Pickup button status lamp of the answering group member becomes steadily lit for the duration of the call.
  - Telephone of the called group member stops ringing.
- If the **Call Pickup Alerting** field is set to y, the Call Pickup Button status lamps on all pickup group member telephones flash when a call comes in. When a pickup group member sees the Call Pickup button status lamp flash and presses the Call Pickup button to answer the call, the:
  - Call Pickup button status lamp of the answering group member goes out.
  - Call Pickup button status lamp of the called group member goes out.
  - Call Pickup button status lamps of the other pickup group members go out.
  - Telephone of the called group member stops ringing.

If another call comes into the pickup group,

- The call will alert to the answering group member. However, the answering group member cannot answer the call using the call pickup button unless the member puts the original call on hold. Once the group member is off the original call, that member is alerted for subsequent group calls and can answer the call using the call pickup button.
- The call alerts to all other group members and can be answered by any of these other group members.

In all scenarios, the call appearance button on the telephone of the called group member:

- Stays steadily lit if the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to y. The called group member can join the call in progress by pressing the lit call appearance button. The person who picked up the call can either stay on the call or hang up.
- Goes out if the **Temporary Bridged Appearance on Call Pickup?** field on the Feature-Related System Parameters screen is set to n. The called group member cannot join the call in progress.

The system uses an algorithm to select what call is answered when multiple calls ring or alert in a call pickup group at the same time. The system searches the extensions of the call pickup group until the system finds an extension with a call that is eligible to be answered with Call Pickup. The system selects this call to be answered. The next time that a group member answers a call with Call Pickup, the system bypasses the extension that was answered most recently, and starts the search at the next extension.

For example, if a group member attempts to use Call Pickup when two calls are ringing at extension A and one call is ringing at extension B, the system selects the calls in the following order:

- One of the calls to extension A
- The call to extension B
- The remaining call to extension A

The system also determines which call that a group member answers when multiple calls ring or alert at the same telephone. The system selects the call with the lowest call appearance, which is usually the call appearance that is nearest to the top of the telephone.

For example, when calls ring or alert at the second and the third call appearances, the system selects the call on the second call appearance for the user to answer.

## Setting up Call Pickup

The first step in setting up any call pickup system is to create pickup groups and assign users to the groups. You can create one or many pickup groups, depending on your needs. A user extension can belong to only one pickup group.

In this exercise, you will:

- Add a pickup group and assign users to the pickup group.
- Enable Call Pickup alerting.

- Assign a Call Pickup button to each extension in the pickup group.
- Assign a feature access code (FAC).

### **Adding Pickup Groups**

- 
1. Type `add pickup-group` next.
  2. Press `Enter`.  
The system displays the Pickup Group screen. The system also assigns the next available Group Number for the new pickup group.

 **Note:**

The **Extended Group Number** field is not shown in this example because the system is set for none or simple extended pickup groups. For more information, see *Setting up simple extended pickup groups*. If the **Extended Group Number** field is visible on this screen, then your system is set up for flexible extended pickup groups.

For more information, see *Setting up flexible extended pickup groups*.

3. Type a name for this pickup group in the **Group Name** field.
4. Type the extension of each group member.  
Up to 50 extensions can belong to one pickup group.
5. Click **Enter** to save your changes.  
The system automatically completes the **Name** field when you click **Enter**.

---

### **Example**

This procedure shows how to set up a new pickup group 11 for Accounting. For the rest of these procedures, let us say that you also set up these pickup groups:

- 12 for Billing
- 13 for Credit Services
- 14 for Delinquency Payments
- 15 for Executives
- 16 for Finance

### **Related topics:**

[Simple extended pickup groups](#) on page 295

[Flexible Extended Pickup Groups](#) on page 297

### **Enabling Call Pickup Alerting**

Call Pickup Alerting allows members of pickup groups to know visually when the telephone of another member is ringing. Use Call Pickup Alerting if the telephones of other pickup group members are too far away to be heard. You must enable Call Pickup Alerting in your system.

- 
1. Enter `change system-parameters features`.
  2. Click **Next** until you see the **Call Pickup Alerting** field.
  3. Set the **Call Pickup Alerting** field to `y`.
  4. Select **Enter** to save your changes.
- 

**Related topics:**

[Call Pickup Alert](#) on page 287

***Assigning a Call Pickup button to a user telephone***

After you define one or more pickup groups, assign a Call Pickup button for each extension in each pickup group. Users in a pickup group can press the assigned Call Pickup button to answer calls to any other extension in their pickup group.

- 
1. Type `change station n`, where *n* is an extension in the pickup group.
  2. Press `Enter`.  
The system displays the Station screen.
  3. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.
  4. Type `call-pkup` after the button number.
  5. Press **Enter** to save your changes.  
Repeat this procedure for each member of each pickup group.
- 

***Assigning a Call Pickup feature access code***

After you define one or more pickup groups, assign and give each member the Call Pickup feature access code (FAC). Instead of using the Call Pickup button, users in a pickup group can dial the assigned FAC to answer calls to any other extension in their pickup group.

- 
1. Enter `change feature-access-codes`.
  2. In the **Call Pickup Access Code** field, type the desired FAC.  
Make sure that the FAC complies with your dial plan.
  3. Select **Enter** to save your changes.
-

### ***Removing a user from a call pickup group***

---

1. Enter `change pickup-group n`, where *n* is the number of the pickup group.
  2. Move to the extension that you want to remove.
  3. Click **Clear** or **Delete**, depending on your system.
  4. Select **Enter** to save your changes.
- 

### ***Deleting pickup groups***

Before deleting a pickup group, you must verify if the pickup group is a member of any simple or flexible extended pickup group. If so, you must first delete the pickup group from all extended pickup groups.

Follow these three steps to delete a pickup group:

- Get a list of all extended pickup groups.
- Verify and delete the pickup group from all extended pickup groups.
- Delete the pickup group.

### ***Getting a list of extended pickup groups***

---

1. Enter `list extended-pickup-group`.
  2. Print this screen or write down the existing Group Numbers so that you can check each extended pickup group.
  3. Click **Cancel**.
- 

### ***Removing a pickup group from an extended pickup group***

You must remove the pickup group from all extended pickup groups.

- If your system is set up for simple extended pickup groups, the pickup group can be a member of only one extended pickup group.
  - If your system is set up for flexible extended pickup groups, the pickup group can be a member of many extended pickup groups.
  - If your system is set up for no extended pickup groups (none) or has no extended pickup groups assigned, you can skip this section and see *Deleting a pickup group*.
- 

1. Type `change extended-pickup-group n`, where *n* is the extended pickup group that you want to check.
2. Press `Enter`.  
The system displays the Extended Pickup Group screen.
3. Perform one of the following actions:

- If the pickup group that you want to delete is not a member of this extended pickup group, Click **Cancel**.
  - If the pickup group that you want to delete is a member of this extended pickup group:
    - Select the pickup group.
    - Click **Clear** or **Delete**, depending on your system.
    - Click **Enter** to save your changes.
4. Repeat this procedure for each extended pickup group.

---

### Deleting pickup groups

Before deleting a pickup group, you must verify if the pickup group is a member of any simple or flexible extended pickup group. If so, you must first delete the pickup group from all extended pickup groups.

Follow these three steps to delete a pickup group:

- Get a list of all extended pickup groups.
- Verify and delete the pickup group from all extended pickup groups.
- Delete the pickup group.

### *Getting a list of extended pickup groups*

- 
1. Enter `list extended-pickup-group`.
  2. Print this screen or write down the existing Group Numbers so that you can check each extended pickup group.
  3. Click **Cancel**.

---

### *Removing a pickup group from an extended pickup group*

You must remove the pickup group from all extended pickup groups.

- If your system is set up for simple extended pickup groups, the pickup group can be a member of only one extended pickup group.
- If your system is set up for flexible extended pickup groups, the pickup group can be a member of many extended pickup groups.
- If your system is set up for no extended pickup groups (none) or has no extended pickup groups assigned, you can skip this section and see *Deleting a pickup group*.

- 
1. Type `change extended-pickup-group n`, where `n` is the extended pickup group that you want to check.
  2. Press `Enter`.

The system displays the Extended Pickup Group screen.

3. Perform one of the following actions:
  - If the pickup group that you want to delete is not a member of this extended pickup group, Click **Cancel**.
  - If the pickup group that you want to delete is a member of this extended pickup group:
    - Select the pickup group.
    - Click **Clear** or **Delete**, depending on your system.
    - Click **Enter** to save your changes.
4. Repeat this procedure for each extended pickup group.

---

### ***Deleting a pickup group***

- 
1. Type `remove pickup-group n`, where `n` is the number of the pickup group that you want to delete.
  2. Press `Enter`.  
The system displays the Pickup Group screen.
  3. Click **Enter**.  
The system deletes the pickup group.

---

#### **Related topics:**

[Simple extended pickup groups](#) on page 295

[Flexible Extended Pickup Groups](#) on page 297

---

### ***Changing a Call Pickup button on a user telephone***

- 
1. Type `change station n`, where `n` is the extension that you want to change.
  2. Press `Enter`.  
The system displays the Station screen.
  3. Click **Next** until you see the BUTTON ASSIGNMENTS area.
  4. Move to the existing **call-pkup** button.
  5. Click **Clear** or **Delete**, depending on your system.
  6. Move to the button number that you want to use for call pickup.

7. Type `call-pkup` after the button number.
8. Click **Enter** to save your changes.

---

### **Removing a Call Pickup button from a user telephone**

---

1. Enter `change station n`, where *n* is the extension that you want to change.
2. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.
3. Move to the existing **call-pkup** button.
4. Click **Clear** or **Delete**, depending on your system.
5. Select **Enter** to save your changes.

---

### **Simple extended pickup groups**

What if you want to have members in one pickup group be able to answer calls for another pickup group? In our example, what if you want members in the Credit Services pickup group 13 to answer calls in the Delinquency Payments pickup group 14? You can do that by setting up extended pickup groups.

If you want members of pickup group 13 to answer calls for pickup group 14, and if you want members of pickup group 14 to answer calls for pickup group 13, set your system for simple extended pickup groups.

Simple extended pickup groups allow members of two or more individual pickup groups to answer each others calls. In a simple extended pickup group, an individual pickup group can be assigned to only one extended pickup group.

All members of one pickup group can answer the calls to the other pickup groups within the simple extended pickup group.

#### **Caution:**

Before you administer what type of extended pickup group to use (none, simple, or flexible), be sure that your pickup group objectives are well thought out and defined.

In this exercise, you will:

- Set up the system for simple extended pickup groups.
- Assign a FAC so that users can answer calls.
- Add pickup groups, if needed
- Assign two pickup groups to an extended pickup group.

#### **Related topics:**

[Adding Pickup Groups](#) on page 290

[Deleting a pickup group](#) on page 294

### ***Creating simple extended pickup groups***

---

1. Enter `change system-parameters features`.
  2. Click **Next** until you see the **Extended Group Call Pickup** field.
  3. In the **Extended Group Call Pickup** field, type `simple`.
  4. Select `Enter` to save your changes.
- 

### ***Creating an extended pickup group feature access code***

Users in an extended pickup group must dial an assigned FAC, followed by a 1-digit or 2-digit Pickup Numbers, to answer calls to an extension in another pickup group. Pickup groups must be in the same extended pickup group. Users cannot use a call pickup button with Extended Call Pickup.

---

1. Type `change feature-access-codes`.
  2. Press `Enter`.  
The system displays the Feature Access Code (FAC) screen.
  3. Click **Next** until you see the **Extended Group Call Pickup Access Code** field.
  4. Perform one of the following actions:
    - If the **Extended Group Call Pickup Access Code** field contains a FAC, click **Cancel**.
    - If the **Extended Group Call Pickup Access Code** field does not contain a FAC:
      - Type the desired FAC.  
Make sure that the FAC complies with your dial plan.
      - Click **Enter** to save your changes.
  5. Communicate the FAC, the list of pickup numbers, and the pickup group to which each pickup number is associated, to each pickup group member who is part of the extended pickup group.
- 

### ***Assigning pickup groups to a simple extended pickup group***

---

1. Type `change extended-pickup-group n`, where n is a number of the extended pickup group. In this example, type `change extended-pickup-group 4`.
2. Press `Enter`.  
The system displays the Extended Pickup Group screen for extended pickup group 4

3. In the Pickup Group Number column, type the numbers of the pickup groups that you want to link together. In this example, add pickup group 13 (Credit Services) and pickup group 14 (Delinquency Payments).
4. Press Enter to save your changes.

---

### Example

Pickup groups 13 and 14 are now linked together in extended pickup group 4. In addition to answering calls to their own pickup group:

- All members of pickup group 13 can answer calls to pickup group 14.
- All members of pickup group 14 can answer calls to pickup group 13.

### Pickup Numbers

The **Pickup Number** column that is associated with the Pickup Group Number is the unique number that users must dial after dialing the Extended Group Call Pickup Access Code FAC to answer a call in that pickup group.

For example, let us say that the Extended Group Call Pickup Access Code FAC is \*39. In the above example:

- A user in pickup group 13 must dial \*391 to answer a call to pickup group 14, because pickup group 14 is assigned to Pickup Number 1.
- A user in pickup group 14 must dial \*390 to answer a call to pickup group 13, because pickup group 13 is assigned to Pickup Number 0.

#### Note:

To minimize the number of digits that a user has to dial, first assign pickup groups to Pickup Numbers 0 to 9.

- By assigning Pickup Numbers 0 to 9, all users only need to dial a single digit (0 to 9) after the FAC to answer the call.
- If you assign a number greater than 9 (10 to 24) to any pickup group, all users must dial two digits (00 to 24) after the FAC to answer the call.

### Flexible Extended Pickup Groups

If you want members of a pickup group to answer calls for another pickup group, but you do not want the other pickup group to answer your calls, set your system for flexible extended pickup groups.

Flexible extended pickup groups still allow members of one or more individual pickup groups to answer calls of another pickup group. However, the reverse scenario is not always true. With flexible extended pickup groups, you can prevent members of one or more pickup groups from answering the calls to another pickup group.

Flexible extended pickup groups allows more control over what pickup groups can answer calls for other pickup groups. Unlike simple extended pickup groups, an individual pickup group can be in multiple flexible extended pickup groups.

The system displays the **Extended Group Number** field on the Pickup Group screen only when you set the **Extended Group Call Pickup** field on the Feature-Related System Parameters screen to flexible. When you populate the **Extended Group Number** field on the Pickup Group screen, you are associating, or "pointing," that pickup group to an extended pickup group. By pointing to an extended pickup group, members of the pickup group can answer calls made to any member of that extended pickup group.

A specific pickup group does not have to be a member of the extended pickup group that the pickup group points to. To help clarify flexible extended pickup groups, see the Example in this section.

 **Caution:**

Before you administer what type of extended pickup group to use (none, simple, or flexible), be sure that your pickup group objectives are well thought out and defined.

In this exercise, you will:

- Set up the system for flexible extended pickup groups.
- Assign a FAC so that users can answer calls.
- Add or change pickup groups, and "point" a pickup group to an extended pickup group.

**Related topics:**

[Adding Pickup Groups](#) on page 290

[Deleting a pickup group](#) on page 294

***Creating flexible extended pickup groups***

- 
1. Type `change system-parameters features`.
  2. Press `Enter`.  
The system displays the Feature-Related System Parameters screen.
  3. Click **Next** until you see the **Extended Group Call Pickup** field
  4. In the **Extended Group Call Pickup** field, type `flexible`.
  5. Click **Enter** to save your changes.  
Your system is now set up for flexible extended pickup groups.  
To create an extended pickup group FAC, see *Creating an extended pickup group feature access code*.
- 

Associating individual pickup groups with an extended pickup group

- 
1. Type `change pickup-group n`, where `n` is a pickup group number.

In this example, let us change pickup group 15 (Executives). Type `change pickup-group 15`.

2. Press `Enter`.

The system displays the Pickup Group screen. Notice that the system displays the **Extended Group Number** field on the Pickup Group screen. This field appears because you set the **Extended Group Call Pickup** field on the Feature-Related System Parameters screen to flexible.

 **Important:**

If you change your system from simple to flexible extended pickup groups (see *Changing extended pickup groups*), the system automatically populates the **Extended Group Number** field on the Pickup Group screen for each pickup group member. For example, pickup groups 13 and 14 are members of extended pickup group 4. If you change the system from simple to flexible extended pickup groups, the system automatically populates the **Extended Group Number** field to 4 on the Pickup Group screen for these two pickup groups.

You are not required to keep the number that the system automatically populates in the **Extended Group Number** field. You can change the number in the **Extended Group Number** field to another pickup group number. You can also make the field blank.

3. If you want to associate, or "point" the pickup group to an extended pickup group, type the number of the extended pickup group for which this pickup group can answer calls in the **Extended Group Number** field. In this example, manually associate pickup group 15 (Executives) to extended pickup group 4. For this example, let us say that you followed the same procedure for pickup group 16 (Finance).

 **Note:**

You do not have to populate the **Extended Group Number** field. You can leave the **Extended Group Number** field blank. You can just as easily point the pickup group to a different extended pickup group. For example, you can point pickup group 13 (Credit Services) to extended pickup group 2, even though pickup group 13 is not a member of extended pickup group 2.

4. Click **Enter** to save your changes.

---

### Assigning pickup groups to a flexible extended pickup group

---

1. Type `change extended-pickup-group n`, where *n* is the number of the extended pickup group.  
In this example, type `change extended-pickup-group`.
2. Press `Enter`.  
The system displays the Extended Pickup Group screen for extended pickup group 4

3. Add pickup group 16 (Finance) to this extended pickup group.
4. Click **Enter** to save your changes.

---

### Example

Here is how flexible extended pickup groups work.

Notice that pickup groups 13, 14, and 16 are now members of extended pickup group 4. On the Pickup Group screen for pickup groups 13, 14, and 16, you also pointed each pickup group to extended pickup group 4.

Pickup group 15 (Executives) is not a member of extended pickup group 4. However, on the Pickup Group screen for group 15 (Figure 96: Pickup Group screen on page 266), you pointed pickup group 15 to extended pickup group 4.

In addition to answering calls to their own pickup group:

Notice that pickup groups 13, 14, and 16 are now members of extended pickup group 4. On the Pickup Group screen for pickup groups 13, 14, and 16, you also pointed each pickup group to extended pickup group 4.

Pickup group 15 (Executives) is not a member of extended pickup group 4. However, on the Pickup Group screen for group 15 (Figure 96), you pointed pickup group 15 to extended pickup group 4.

In addition to answering calls to their own pickup group:

- Any member of pickup group 13 can answer calls to pickup groups 14 and 16.
- Any member of pickup group 14 can answer calls to pickup groups 13 and 16.
- Any member of pickup group 16 can answer calls to pickup groups 13 and 14.
- Any member of pickup group 15 can answer calls to pickup groups 13, 14, and 16 because pickup group 15 points to extended pickup group 4.
- Any member of pickup groups 13, 14 and 16 cannot answer calls to pickup group 15 because pickup group 15 is not a member of extended pickup group 4.

### Changing extended pickup groups

You define extended pickup groups on a system-wide basis. The system cannot support both simple and flexible extended pickup groups at the same time. You can, however, change your extended pickup groups from one type to another.

#### Related topics:

[Call Pickup](#) on page 287

[Simple extended pickup groups](#) on page 295

[Flexible Extended Pickup Groups](#) on page 297

[Directed Call Pickup](#) on page 301

### Changing from simple to flexible

If you want to change all extended pickup groups from simple to flexible, you can easily make the change. See *Creating flexible extended pickup groups*. The system automatically

populates the **Extended Group Number** field on the Pickup Group screen for all pickup groups that are part of an extended pickup group.

### ***Changing from flexible to simple***

The process is more complex to change all extended pickup groups from flexible to simple. Before you can change the extended pickup group from flexible to simple, you must first delete all of the individual pickup groups from all of the extended pickup groups. Then you can change the extended pickup group from flexible to simple (see *Creating simple extended pickup groups*). After that step, you must re-administer all of the extended pickup groups again.

### **Directed Call Pickup**

If you do not want to set up pickup groups and extended pickup groups, but still want selected people to answer other telephones, use Directed Call Pickup. Before a person can use this feature, you must enable Directed Call Pickup on your system.

- Telephones that can be answered by another extension using Directed Call Pickup must have a Class of Restriction (COR) that allows this feature.
- Telephones that can answer another extension using Directed Call Pickup must have a COR that allows this feature.

In this exercise, you will:

- Determine if Directed Call Pickup is enabled on your system.
- Create one or more Classes of Restriction (COR) that allow Directed Call Pickup.
- Assign the COR to individual extensions.
- Assign a Directed Call Pickup button to each extension that is assigned the COR.
- Assign a feature access code (FAC).

### ***Ensuring Directed Call Pickup availability***

Before you can assign Directed Call Pickup to a user, you must ensure that Directed Call Pickup is available on your system.

- 
1. Type `change system-parameters features`.
  2. Press `Enter`.  
The system displays the Feature-Related System Parameters screen.
  3. Click **Next** until you see the **Directed Call Pickup?** field
  4. Perform one of the following actions:
    - a. If the **Directed Call Pickup?** field is set to `y`, your system is set up for Directed Call Pickup. Click **Cancel**.
    - b. If the **Directed Call Pickup?** field is set to `n`:
      - Type `y` in the field.

- Click **Enter** to save your changes.

---

### **Creating Classes of Restriction for Directed Call Pickup**

You must create one or more Classes of Restriction (COR) that allow Directed Call Pickup. All users to whom you assign a COR can then use Directed Call Pickup.

There are three ways to set up a COR for Directed Call Pickup. You can create a COR where users can:

- Only have their extensions answered by Directed Call Pickup. Users with this COR cannot pick up other extensions.
- Only pick up other extensions using Directed Call Pickup. Users with this COR cannot have their extensions answered by other users.
- Both have their extensions answered by Directed Call Pickup and pick up other extensions.

- 
1. Enter `change COR n`, where *n* is the COR that you want to change.
  2. Perform one of the following actions:
    - a. To create one or more CORs where the extensions can only be picked up by the Directed Call Pickup feature, but not be able to pick up other extensions:
      - Type *y* in the **Can Be Picked Up By Directed Call Pickup** field.
      - Leave the **Can Use Directed Call Pickup** field set to *n*.

Any extension to which you assign this COR can only be picked up by the Directed Call Pickup feature.
    - b. To create one or more CORs where the extensions can only use the Directed Call Pickup feature to pick up other extensions, but not be picked up by other extensions:
      - Leave the **Can Be Picked Up By Directed Call Pickup** field set to *n*.
      - Type *y* in the **Can Use Directed Call Pickup** field.

Any extension to which you assign this COR can only use the Directed Call Pickup feature to pick up other extensions.
    - c. To create one or more CORs where the extensions can use the Directed Call Pickup feature both to pick up other extensions and be picked up by other extensions:
      - Type *y* in the **Can Be Picked Up By Directed Call Pickup** field.
      - Type *y* in the **Can Use Directed Call Pickup** field.

Any extension to which you assign this COR can use the Directed Call Pickup feature both to pick up other extensions and be picked up by other extensions.

3. Select **Enter** to save your changes.

---

### ***Assigning a Class of Restriction to a user***

You must assign a COR to user extensions before anyone can use Directed Call Pickup.

- 
1. Enter `change station n`, where *n* is the extension that you want to change.
  2. In the **COR** field, type the appropriate COR that allows Directed Call Pickup capabilities.
  3. Select **Enter** to save your changes.

---

### ***Assigning a Directed Call Pickup button***

Assign a Directed Call Pickup button to all extensions that share a COR where the **Can Use Directed Call Pickup** field is set to *y*.

- 
1. Enter `change station n`, where *n* is an extension to which you have assigned the Directed Call Pickup COR.
  2. Click **Next** until you see the **BUTTON ASSIGNMENTS** area.
  3. Move to the button number that you want to use for Directed Call Pickup. You can use any of the available buttons.
  4. Type `dir-pkup` after the button number.
  5. Select **Enter** to save your changes.
- Repeat this procedure for each member of the COR who can pick up other extensions using Directed Call Pickup.

---

### ***Assigning a Directed Call Pickup feature access code***

Also assign a Directed Call Pickup feature access code (FAC). Give the FAC to each user whose extension shares a **COR where the Can Use Directed Call Pickup** field is set to *y*.

Instead of using the Directed Call Pickup button, users can dial the assigned FAC to answer calls using Directed Call Pickup.

- 
1. Enter `change feature-access-codes`.
  2. Click **Next** until you see the **Directed Call Pickup Access Code** field.
  3. Perform one of the following actions:

- a. If the **Directed Call Pickup Access Code** field already contains a code, click **Cancel**.
- b. If the **Directed Call Pickup Access Code** field does not contain a code:
  - Type a code in the field. Make sure that the code you type conforms to your dial plan.
  - Select **Enter** to save your change.

Communicate the FAC with each member of the COR that can pick up other extensions using Directed Call Pickup.

---

## Removing Directed Call Pickup from a user

---

1. Enter `change station n`, where  $n$  is the extension of the user.
  2. In the **COR** field, type a different COR that does not have Directed Call Pickup permissions.
  3. Click **Next** until you see the **BUTTON ASSIGNMENTS** section.
  4. Move to the button number that contains `dir-pkup`.
  5. Click **Clear** or **Delete**, depending on your system.
  6. Select **Enter** to save your changes.
- 

## Hunt Groups

A hunt group is a group of extensions that receive calls according to the call distribution method you choose. When a call is made to a certain telephone number, the system connects the call to an extension in the group.

Use hunt groups when you want more than one person to be able to answer calls to the same number. For example, set up a hunt group for:

- a benefits department within your company
- a travel reservations service

### Setting up hunt groups

Let us set up a hunt group for an internal helpline. Before making changes to Communication Manager, we'll decide:

- the telephone number for the hunt group
- the number of people answering calls
- the way calls are answered

Our dial plan allows 4-digit internal numbers that begin with 1. The number 1200 is not in use. So, we'll set up a helpline hunt group so anyone within the company can call extension 1200 for help with a telephone.

We will assign 3 people (agents) and their extensions to our helpline. We want calls to go to the first available person.

- 
1. Type `add hunt-group` next.
  2. Press `Enter`.  
The system displays the Hunt Group screen. The **Group Number** field is automatically filled in with the next hunt group number.
  3. In the **Group Name** field, type the name of the group.  
In our example, type `internal helpline`.
  4. In the **Group Extension** field, type the telephone number.  
We'll type `1200`.
  5. In the **Group Type** field, type the code for the call distribution method you choose.  
We'll type `ucd-loa` so a call goes to the agent with the lowest percentage of work time since login.

 **Note:**

The COS for all hunt groups defaults to 1. Therefore, any changes to COS 1 on the Class of Service screen changes the COS for all your hunt groups. A **COS** field does not appear on the Hunt Group screen.

6. Click **Next Page** to find the Group Member Assignments screen.
7. In the **Ext** field, type the extensions of the agents you want in the hunt group.  
We'll type `1011`, `1012`, and `1013`.

 **Tip:**

For a ddc group type (also known as "hot seat" selection), the call is sent to the extension listed in the first **Ext** field. The system uses this screen to determine the hunting sequence.

8. Click **Enter** to save your changes.  
The **Name** fields are display-only and do not appear until the next time you access this hunt group.

---

### ***Dynamic hunt group queue slot allocation***

The dynamic hunt group queue slot allocation feature eliminates the need to preallocate queue slots for hunt groups. The system dynamically allocates the queue slots from a common pool on an as-needed basis. All possible calls can be queued. There is no additional administration needed. This feature expands the capacities of your system by eliminating the potential of missed calls due to a full queue

When the **Queue?** field on the Hunt Group screen is set to y, this feature applies to all uses of hunt groups:

- Automatic Call Distribution (ACD) non-vector/vector splits and skills
- Non-ACD hunt group
- Voice mail

### Changing a hunt group

- 
1. Enter `change hunt-group n`, where *n* is the number of the hunt group.
  2. Change the necessary fields.
  3. Select **Enter** to save your changes.

### Setting up a queue

You can tell your server running Communication Manager how to handle a hunt-group call when it cannot be answered right away. The call waits in "queue."

We will tell Communication Manager that as many as 10 calls can wait in the queue, but that you want to be notified if a call waits for more than 30 seconds.

You also want Communication Manager to send a warning when 5 or more calls are waiting in the queue. This warning flashes queue-status buttons on telephones that have a status button for this hunt group. When the buttons flash, everyone answering these calls can see that the help-line calls need more attention.

- 
1. Type `change hunt-group n`, where *n* is the number of the hunt group to change.
  2. Press **Enter**.  
In our example, type `change hunt-group 5`.  
The system displays the Hunt Group screen.
  3. In the **Queue** field, type *y*.
  4. In the **Queue Length** field, type the maximum number of calls that you want to wait in the queue.  
In our example, type 10.
  5. In the **Calls Waiting Threshold** field, type the maximum number of calls that can be in the queue before the system flashes the queue status buttons.  
In our example, type 5.
  6. In the **Time Warning Threshold** field, type the maximum number of seconds you want a call to wait in the queue before the system flashes the queue status buttons.

In our example, type 30.

7. Click **Enter** to save your changes.

---

## Hunt groups for TTY callers

Several laws, such as the Americans with Disabilities Act (ADA) of 1990 and Section 255 of the Telecommunications Act of 1996, require that “reasonable accommodation” be provided for people with disabilities. For this reason, your company might choose to offer support for callers who use TTYs. (These devices are also known as TDDs -- “Telecommunication Device for the Deaf” -- but the term TTY is generally preferred, in part because many users of these devices are hearing-impaired, but not deaf.)

TTY callers can be accommodated by creating a hunt group that includes TTY-equipped agents. The TTY itself looks a little like a laptop computer, except that it has a one- or two-line alphanumeric display instead of a computer screen. The cost of a typical TTY is approximately three hundred dollars. Although many TTYs can connect directly with the telephone network via analog RJ-11 jacks, Avaya recommends that agents be equipped with TTYs that include an acoustic coupler that can accommodate a standard telephone handset. One reason for this recommendation is that a large proportion of TTY users are hearing impaired, but still speak clearly. These individuals often prefer to receive calls on their TTYs and then speak in response. This requires the call center agent to alternate between listening on the telephone and then typing on the TTY, a process made considerably easier with an acoustically coupled configuration.

Although TTY-emulation software packages are available for PCs, most of these do not have the ability to intermix voice and TTY on the same call.

For a TTY hunt group, you can record TTY announcements and use them for the hunt group queue. To record announcements for TTY, simply follow the same steps as with voice recordings from your telephone (see *Managing Announcements*). However, instead of speaking into your telephone to record, you type the announcement with the TTY device.

### **Note:**

For an alternative to simply creating a TTY hunt group, you can use vectors to process TTY calls. With vectors, you can allow TTY callers and voice callers to use the same telephone number. In this case, you can also record a single announcement that contains both TTY signaling and a voice recording.

## Adding hunt group announcements

You can add recorded announcements to a hunt group queue. Use announcements to encourage callers to stay on the line or to provide callers with information. You can define how long a call remains in the queue before the caller hears an announcement.

For more information on how to record an announcement, see “Announcements” in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

Let us add an announcement to our internal helpline. We want the caller to hear an announcement after 20 seconds in the queue, or after approximately 4 or 5 rings. Our announcement is already recorded and assigned to extension 1234.



**Tip:**

You can use `display announcements` to find the extensions of your recorded announcements.

- 
1. Type `change hunt-group n`, where `n` is the number of the hunt group to change.
  2. Press `Enter`.  
In our example, type `change hunt-group 5`.  
The system displays the Hunt Group screen.
  3. Click **Next Page** to find the **First Announcement Extension** field.
  4. In the **First Announcement Extension** field, type the extension of the announcement you want callers to hear.  
In this example, type `1234`.
  5. In the **First Announcement Delay (sec)** field, type the number of seconds you want the caller to wait before hearing the first announcement.  
In our example, type `20`.



**Tip:**

If you set the delay announcement interval to 0, callers automatically hear the announcement before anything else. This is called a “forced first announcement.”

6. Click **Enter** to save your changes.  
You can use the same announcement for more than one hunt group.

---

## Vectors and VDNs

This section provides an introduction to vectors and Vector Directory Numbers (VDN). It gives you basic instructions for writing simple vectors.



**Security alert:**

Vector fraud is one of the most common types of toll fraud because vectors route calls based on the Class of Restriction (COR) assigned to the VDN. See *BCS Products Security Handbook, 555-025-600* for more information.

This section references announcements, hunt groups, queues, splits, and skills, which are covered in detail in other sections of this book. You can also find information about these topics in *Avaya Call Center Call Vectoring and Expert Agent Selection (EAS) Guide, 07-600780*.



**Note:**

The **Client Room** field on the Class of Service screen will affect VDN displays. If a local station that has a COS with the **Client Room** field set to `y` calls a local VDN, the agent's

display that receives the call will look as if it is a direct station call rather than the expected VDN display of “station name to vdn name.”

### What are Vectors?

A vector is a series of commands that you design to tell the system how to handle incoming calls. A vector can contain up to 32 steps and allows customized and personalized call routing and treatment. Use call vectoring to:

- play multiple announcements
- route calls to internal and external destinations
- collect and respond to dialed information

#### **Tip:**

The vector follows the commands in each step in order. The vector “reads” the step and follows the command if the conditions are correct. If the command cannot be followed, the vector skips the step and reads the next step.

Your system can handle calls based on a number of conditions, including the number of calls in a queue, how long a call has been waiting, the time of day, day of the week, and changes in call traffic or staffing conditions.

### Putting a call in a queue

Write a vector so that calls that come into the main business number redirect to a queue.

We will use a vector-controlled hunt group for the main number queue. This hunt group was set up as main split 47. When calls first arrive, all calls to our main number should be queued as “pri 1” for low priority.

To queue calls, write the following vector (step 2). (Please note, we started our example on step 2 because step 1 is used later.)

- 
1. Keep it Blank.
  2. Type `queue-to main split 47 pri 1`.

#### **Tip:**

Remember, Communication Manager automatically fills in some of the information when you type your vector step. Press `Tab`.

### Playing an Announcement

Write a vector to play an announcement for callers in a queue. Use the announcement to ask callers to wait. You need to record the announcement before the vector can use it.

Let us play our announcement 4001, asking the caller to wait, then play music for 60 seconds, then repeat the announcement and music until the call is answered. The `goto` command creates the loop to repeat the announcement and the music. Unconditionally means under all conditions.

**+ Tip:**

Rather than loop your vectors directly back to the announcement step, go to the previous queue-to step. This way, if for some reason the call does not queue the first time, Communication Manager can attempt to queue the call again. If the call successfully queued the first time though, it merely skips the queue-to step and plays the announcement. The system cannot queue a call more than once in the exact same priority level.

To play and repeat an announcement, write this vector (steps 3-5):

- 
1. Keep it Blank.
  2. Type `queue-to main split 47 pri 1`.
  3. Type `announcement 4001 (All agents are busy, please wait...)`.
  4. Type `wait-time 60 secs hearing music`.
  5. Type `goto step 2 if unconditionally`.
- 

### **Routing Based On Time Of Day**

Write a vector for calls that come in after your office closes.

Assume that your business is open 7 days a week, from 8:00 a.m. to 5:00 p.m. When calls come in after business hours, you want to play your announcement 4002, which states that the office is closed and asks callers to call back during normal hours. Write the vector so the call disconnects after the announcement is played.

For after hours treatment, write this vector (steps 1, 6, and 7):

- 
1. Type `goto step 7 if time-of-day is all 17:00 to all 8:00`.
  2. Type `queue-to main split 47 pri 1`.
  3. Type `announcement 4001 (All agents are busy, please wait...)`.
  4. Type `wait-time 60 secs hearing music`.
  5. Type `goto step 2 if unconditionally`.
  6. Type `stop`.
  7. Type `disconnect after announcement 4002 ("We're sorry, our office is closed...")`.

If the `goto` command in step 5 fails, Communication Manager goes to the next step. The `stop` in step 6 prevents callers from incorrectly hearing the "office is closed" announcement in step 7. `stop` keeps the call in the state it was in before the command failed. In this case, if step 5 fails, the call remains in step 4 and the caller continues to hear music.

**Caution:**

Add a stop vector step only after calls are routed to a queue. If a stop vector is executed for a call not in queue, the call drops.

---

**Allowing callers to leave a message**

Write a vector that allows callers to leave messages. This type of vector uses a hunt group called a messaging split. For our example, we send after-hours calls to the voice mailbox at extension 2000 and use messaging split 99.

Once the vector routes a call to the mailbox, the caller hears a greeting (that was recorded with the voice mail for mailbox 2000) that tells them they can leave a message.

To let callers leave messages, write this vector (step 7):

- 
1. Type `goto step 7 if time-of-day is all 17:00 to all 8:00.`
  2. Type `queue-to main split 47 pri 1.`
  3. Type `announcement 4001 (All agents are busy, please wait...).`
  4. Type `wait-time 60 secs hearing music.`
  5. Type `goto step 2 if unconditionally.`
  6. Type `stop.`
  7. Type `messaging split 99 for extension 2000.`

---

**Redirecting calls during an emergency or holiday**

You can provide a quick way for a supervisor or agent to redirect calls during an emergency or holiday. Use a special mailbox where you can easily change announcements. This vector is also an alternative to making sure all agents log out before leaving their telephones.

In our example, no agents are normally logged in to split 10. We'll use split 10 for an emergency. We preset buttons on our agents' telephones so people with these telephones can log in at the touch of a button.

To quickly redirect calls:

Create a special mailbox with the appropriate announcement such as "We are unable to answer your call at this time" or "Today is a holiday, please call back tomorrow."

In our example, we recorded the mailbox greeting for extension 2001.

Insert the following steps (steps 1, 10, and 11).

See *Inserting a step*.

- 
1. **Type** goto step 10 if staff agents split 10 > 0.
  2. **Type** goto step 8 if time-of-day is all 17:00 to all 8:00.
  3. **Type** queue-to main split 47 pri 1.
  4. **Type** announcement 4001 (All agents are busy, please wait...).
  5. **Type** wait-time 60 secs hearing music.
  6. **Type** goto step 2 if unconditionally.
  7. **Type** stop.
  8. **Type** messaging split 99 for extension 2000.
  9. **Type** stop.
  10. **Type** messaging split 99 for extension 2001.
  11. **Type** stop.

When there is an emergency, fire drill, or holiday, the supervisor or agent logs into this split. When an agent logs into split 10, the system looks at vector step 1, sees that more than 0 people are logged into split 10, and sends calls to step 10 (which sends to messaging split 99). When your business returns to normal and the agent logs out of split 10, call handling returns to normal.

---

### ***Giving callers additional choices***

You can give your callers a list of options when they call. Your vector tells Communication Manager to play an announcement that contains the choices. Communication Manager collects the digits the caller dials in response to the announcement and routes the call accordingly.

We'll create a vector that plays an announcement, then lets callers dial an extension or wait in the queue for an attendant.

Please note, the following example of this "auto attendant" vector is a new vector and is not built on the vector we used in the previous example.

To let callers connect to an extension, write this kind of vector:

- 
1. **Type** wait-time 0 seconds hearing music.
  2. **Type** collect 4 digits after announcement 4004 (You have reached our company. Please dial a 4-digit extension or wait for the attendant.).
  3. **Type** route-to digits with coverage y.

4. Type `route-to number 0 with cov n if unconditionally.`
5. Type `stop.`

---

### ***Inserting a Step***

It is easy to change a vector step and not have to retype the entire vector. We will add announcement 4005 between step 3 and step 4 in vector 20.

- 
1. Type `change vector 20.` Press **Enter**.  
The system displays the Call Vector screen.
  2. Click **Edit**.
  3. Type `i` followed by a space and the number of the step you want to add.  
In our example, type `i 4`.
  4. Type the new vector step.  
We will type `announcement 4005 (Please wait...)`.
  5. Click **Enter** to save your changes.



#### **Tip:**

When you insert a new vector step, the system automatically renumbers the rest of the vector steps and all references to the vector steps. Communication Manager inserts a "\*" when the numbering needs more attention.

---

### ***Deleting a Step***

- 
1. Type `change vector 20.` Press **Enter**.  
The system displays the Call Vector screen.
  2. Click **Edit**.
  3. Type `d` followed by a space and the number of the step you want to delete.  
In our example, type `d 5`.



#### **Tip:**

You can delete a range of vector steps. For example, to delete steps 2 through 5, type `d 2-5`. Click **Enter**.

4. Click **Enter** to save your changes.



#### **Tip:**

When you delete a vector step, the system automatically renumbers the rest of the vector steps and all references to the vector steps. An asterisk (\*) is inserted when the numbering needs more attention.

---

## Variables in Vectors

Variables in Vectors (VIV) is a Call Vectoring feature that allows you to create variables that can be used in vector commands to:

- Improve the general efficiency of vector administration
- Provide increased manager and application control over call treatments
- Allow you to create more flexible vectors that better serve the needs of your customer and contact center operations

The vector variables are defined in a central variable administration table. Values assigned to some types of variables can also be quickly changed by means of special vectors, Vector Directory Numbers (VDNs), or Feature Access Codes (FACs) that you administer specifically for that purpose. Different types of variables are available to meet different types of call processing needs. Vector variables can be added to “consider location,” “messaging,” and “adjunct routing” vector steps when the Call Center Release is 3.0 or later. Depending on the variable type, variables can use either call-specific data or fixed values that are identical for all calls. In either case, an administered variable can be reused in many vectors. For a more detailed description of variable types and purposes, see *Avaya Call Center Call Vectoring and Expert Agent Selection (EAS) Guide, 07-600780*.

## Administering Vector Variables

Administering variables and implementing them in your vectors is a relatively simple process:

- 
1. First, determine how you intend to use the new variable and identify its defining characteristics. Use this information to decide on an available variable type that meets your needs.
  2. Type `change variables`.  
The Variables for Vectors screen appears.
  3. In the **Var** column, select an unused letter between A and Z. This letter is used to represent this variable in vector steps. Complete the editable fields in the row that you select. Depending on your entry in the **Type** field, some fields in the row may be pre-populated and display-only, or not applicable.
    - **Description** - a short description of your variable
    - **Type** - the variable type
    - **Scope** - local or global
    - **Length** - length of the digit string
    - **Start** - digit start position
    - **Assignment** - pre-assigned value
    - **VAC** - Variable Access Code (for value variable type only)
  4. Click **Enter** to save your changes.
-

## Handling TTY calls with vectors

Unlike fax machines and computer modems, a Tele-typewriter device (TTY) has no handshake tone and no carrier tone. A TTY is silent when not transmitting. This is why systems cannot identify TTY callers automatically. However, the absence of these special tones also means that voice and TTY tones can be intermixed in pre-recorded announcements. The ability to provide a hybrid voice-and-TTY announcement, when combined with the auto-attendant vectoring capability, can permit a single telephone number to accommodate both voice and TTY callers.

The sample vector that follows allows TTY callers to access a TTY agent. It begins with a step that plays a TTY announcement combined with a voice announcement. The announcement tells the TTY caller to enter a digit that will direct them to a TTY support person. The vector then processes the digit entered to connect the TTY caller to the TTY split (or hunt group). For more information on recording TTY announcements, see *Managing Announcements*.

In the following example, split 47 (hunt group 47) has already been established and consists of TTY-enabled agents.

If a TTY caller calls the number that connects to vector 33, the following occurs:

- 
1. After a short burst of ringing, a quick burst of TTY tones is sent to the caller telling the caller to hold, "HD". Then, a voice announcement follows for callers using a normal telephone connection. The announcement tells them to stay on the line. Finally, another burst of TTY tones is sent to the TTY caller which displays on the caller's TTY device as, "Dial 1." The TTY caller won't hear the voice announcement, but because the step collects digits, it allows the caller to enter 1 on his or her touchtone telephone.

 **Note:**

For voice callers, the burst of TTY tones lasts about one second and sounds like a bird chirping.

2. In vector step 3, since the TTY caller entered 1 in vector step 2, the TTY caller is sent to vector step 8, at which point the caller is put in queue for a TTY-enabled agent in split 47.

 **Note:**

The voice caller is sent to vector step 3 also, but a voice caller does not go to vector step 8 because the caller did not enter 1 at vector step 2. Instead, voice callers continue on to vector step 4, where they connect to split 48.

3. While the TTY caller waits in queue, he or she hears silence from vector step 9, then the announcement in vector step 10, and is then looped back to wait with silence by vector step 11.

See the *Avaya Call Center Call Vectoring and Expert Agent Selection (EAS) Guide*, 07-600780, for more information.

Automated Attendant competes with several features for ports on the Call Classifier — Detector circuit pack or equivalent. See the *Avaya Aura™ Communication*

*Manager Hardware Description and Reference*, 555-245-207 for more information on the circuit pack.

---

### **Fixing vector problems**

If there is a problem with a vector, Communication Manager records the error as a vector event. Vector events occur for a number of reasons including problems with a trunk, full queue slots, or the vector reaching the maximum 1000 steps allowed.

Use `display events` to access the Event Report screen and see the event record. Use the event record to see why the vector failed.

To view the Event Report:

- 
1. Type `display events`.
  2. Press `Enter`.  
The system displays the Event Report screen.
  3. To see all current vector events, click `Enter`.

OR

Indicate the events that you want to see by completing the **Report Period** and **Search Option** fields.

4. Click `Enter` to view the report.  
The system displays the Event Report (detail) screen.

Look at the information in the **Event Data** field to diagnose the vector event. In this example, there was a problem with:

- Vector 12, step 5
- Split 89

---

### **Vector Directory Numbers**

A VDN is an extension that directs an incoming call to a specific vector. This number is a “soft” extension number not assigned to an equipment location. VDNs must follow your dial plan.

We will create VDN 5011 for our sales department. A call into 5011 routes to vector 11. This vector plays an announcement and queues calls to the sales department.

#### **Security alert:**

Vector fraud is one of the most common types of toll fraud because vectors route calls based on the class of restriction (COR) assigned to the VDN. See the *Avaya Toll Fraud and Security Handbook*, 555-025-600 for more information.

## Adding a vector directory number

---

1. Type `add VDN 5011`.
2. Press `Enter`.
3. You enter the VDN extension you want to add.  
The system displays the Vector Directory Number screen.
4. Type a description for this VDN in the **Name** field.  
In our example, type `Sales Department`.

The information in the VDN Name field appears on a display telephone. This allows the agent to recognize the nature of the call and respond accordingly.



### Tip:

The **VDN Override** on the Vector Directory Number screen controls the operation of the display.

5. Enter the vector number.  
In our example, type `11`.
6. In the **Measured** field, indicate how you want to measure calls to his VDN.  
In our example, type `both` (for both CMS and BCMS).



### Tip:

BCMS must be enabled to use `both`. Use `display system-parameters customer-options` to see if BCMS is enabled.

7. Click **Enter** to save your changes.
- 

## Viewing vector directory numbers

---

1. Type `list VDN`.
  2. Press `Enter`.  
The system displays the Vector Directory Number screen.
  3. Each VDN maps to one vector. Several VDNs can map to the same vector.
- 

## Automatic Call Distribution

Automatic Call Distribution (ACD) is an Avaya Communication Manager feature used in many contact centers. ACD gives you greater flexibility to control call flow and to measure the performance of agents.

ACD systems operate differently from non-ACD systems, and they can be much more complex. ACD systems can also be more powerful because they allow you to use features and products

that are not available in non-ACD systems. See the *Avaya Call Center Release 4.0 Automatic Call Distribution (ACD) Guide, 07-600779*, for more information on ACD call centers.

### ACD System Enhancement

First, all call center management systems (such as Avaya's Basic Call Management System (BCMS), BCMSVu, and the sophisticated Avaya IP Agent Call Management System) require ACD. These management systems give you the ability to measure more aspects of your center's operation, and in more detail, than is possible with standard Avaya Communication Manager reports.

Call vectoring greatly enhances the flexibility of a call center, and most vectoring functions require ACD. Vectoring is a simple programming language that allows you to custom design every aspect of call processing.

Together, ACD and vectoring allow you to use Expert Agent Selection (EAS) For a variety of reasons, you might want certain agents to handle specific types of calls. For example, you might want only your most experienced agents to handle your most important customers. You might have multilingual agents who can serve callers in a variety of languages.

EAS allows you to classify agents according to their specific skills and then to rank them by ability or experience within each skill. Avaya Communication Manager uses these classifications to match each call with the best available agent. See *Avaya Call Center Call Vectoring and Expert Agent Selection (EAS) Guide, 07-600780*, for more information on call vectoring and EAS.

## Assigning a Terminating Extension Group

A Terminating Extension Group (TEG) allows an incoming call to ring as many as 4 telephones at one time. Any user in the group can answer the call.

Once a member of the TEG has answered a group call, the TEG is considered busy. If a second call is directed to the group, it follows a coverage path if one has been assigned.

The following example shows how to assign a terminating extension group to the advertising department.

For example, we will assign this TEG to extension 6725.

- 
1. Type `add term-ext-group next`.
  2. Press `Enter`.  
The system displays the Terminating Extension Group screen.
  3. In the **Group Extension** field, type `6725`.  
This is the extension for the advertising group.
  4. In the **Group Name** field, type `advertising`.

This is the name of the group.

5. In the **Coverage Path** field, type 5.

This is the number of the call coverage path for this group.

---

---

## Routing Outgoing Calls

### World Class Routing

Your system uses Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS) to direct outgoing calls.

- AAR routes calls within your company over your own private network.
- ARS routes calls that go outside your company over public networks. ARS also routes calls to remote company locations if you do not have a private network.

Automatic routing begins when a user dials a feature access code (FAC) followed by the number the user wants to call. Avaya Communication Manager analyzes the digits dialed, selects the route for the call, deletes and inserts digits if necessary, and routes the call over the trunks you specify in your routing tables. ARS and AAR can access the same trunk groups and share the same route patterns and other routing information. ARS calls can be converted to AAR calls and vice-versa.

The FAC for AAR is usually the digit 8. The FAC for ARS is usually the digit 9 in the US and 0 outside of the US. Your Avaya technician or business partner sets up AAR on your server running Communication Manager and usually assigns the AAR FAC at the same time. You can administer your own ARS FAC.

This section describes only ARS call routing.

### Calling Privileges Management

Each time you set up a telephone, you use the Station screen to assign a class of restriction (COR). You can create different CORs for different groups of users. For example, you might want executives in your company to have different calling privileges than receptionists.

When you set up a COR, you specify a Facility Restriction Level (FRL) on the Class of Restriction screen. The FRL determines the calling privileges of the user. Facility Restriction Levels are ranked from 0–7, where 7 has the highest level of privileges.

You also assign an FRL to each route pattern preference in the Route Pattern screen. When a user makes a call, the system checks the user's COR. The call is allowed if the caller's FRL is higher than or equal to the route pattern preference's FRL.

## Changing Station

Let us say we are setting up a new telephone for an executive. The current translations assign COR 1, with outward restrictions and an FRL 0, which is the lowest permission level available. We want to assign a COR with the highest level of permissions, FRL 7, to station 1234.

To change station 1234 from COR 1 to COR 7:

- 
1. Type `change station 1234`.
  2. Press **Enter**.  
The Station screen appears.
  3. In the **COR** field, type 7.
  4. Press `Enter` to save your changes.
  5. To change from FRL 0 to FRL 7, type `change cor 7`.
  6. Press **Enter**.  
The Class of Restriction screen appears.
  7. In the **FRL** field, type 7.
  8. Press **Enter** to save your changes.  
Now all users with COR 7 will have the highest level of calling permissions.
- 

## Assigning ARS FAC

### Prerequisites

Be sure the ARS feature access code (FAC) is set up on your system. In the U.S., 9 is usually the ARS FAC. Users dial 9 to make an outgoing call.

When a user dials 9 to access ARS and make an outgoing call, the ARS access code 9 is dropped before digit analysis takes place. will not be part of the digit analysis.

To assign the ARS FAC:

- 
1. Type `change dialplan`.
  2. Press **Enter**.  
The DCS to QSIG TSC Gateway appears.
  3. Move to the 9 row and type `fac` in the first column.
  4. Press `Enter` to save your changes.
  5. Type `change features`.
  6. Press **Enter**.

The Feature Access Code (FAC) screen appears.

7. Type 9 in the **ARS - access code** field.
8. Press **Enter** to save your changes.

---

### Location ARS FAC

The **Location ARS FAC** allows users in different locations to use the same “culturally significant” FAC they are accustomed to, such as dialing 9 for an outside line, and access the same feature. The Location ARS FAC is only accessible for calling numbers at locations administered with that ARS FAC (for details on setting up Location ARS FAC, see the Locations screen). If an attempt is made to use an ARS FAC at a location for which it is not valid, the attempt is denied. The ARS access code on the Feature Access Code (FAC) screen continues to be used when a location ARS does not exist. If a location ARS FAC exists, then the ARS access code on the Feature Access Code (FAC) screen is prohibited/denied from that location.

By using a local ARS code, the ability to administer two ARS codes on the Feature Access Code (FAC) screen is lost.

## Displaying ARS Analysis Information

You will want to become familiar with how your system currently routes outgoing calls. To display the ARS Digit Analysis Table that controls how the system routes calls that begin with 1:

- 
1. Type `display ars analysis 1`.
  2. Press `Enter`.  
The ARS Digit Analysis Table for dialed strings that begin with 1 appears.

 **Note:**

Communication Manager displays only as many dialed strings as can fit on one screen at a time.

 **Note:**

Type `display ars analysis` and press `Enter` to display an all-location screen. For details on command options, see online help, or *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

3. To see all the dialed strings that are defined for your system, run an ARS Digit Analysis report:
  - a. Type `list ars analysis`.
  - b. Press **Enter**.  
The ARS Digit Analysis Report appears.

You might want to print this report to keep in your paper records.

---

## ARS Analysis

With ARS, Communication Manager checks the digits in the number called against the ARS Digit Analysis Table to determine how to handle the dialed digits. Communication Manager also uses Class of Restriction (COR) and Facility Restriction Level (FRL) to determine the calling privileges.

Let us look at a very simple AAR and ARS digit analysis table. Your system likely has more defined dialed strings than this example.

The far-left column of the ARS Digit Analysis Table lists the first digits in the dialed string. When a user makes an outgoing call, the system analyzes the digits, looks for a match in the table, and uses the information in the matching row to determine how to route the call.

Let us say a caller places a call to 1-303-233-1000. Communication Manager matches the dialed digits with those in the first column of the table. In this example, the dialed string matches the "1". Then Communication Manager matches the length of the entire dialed string (11 digits) to the minimum and maximum length columns. In our example, the 11-digit call that started with 1 follows route pattern 30 as an fnpa call.

### Tip:

The first dialed digit for an external call is often an access code. If '9' is defined as the ARS access code, Communication Manager drops this digit and analyzes the remaining digits with the ARS Analysis Table.

The Route Pattern points to the route that handles the calls that match this dial string. **Call Type** tells what kind of call is made with this dial string.

**Call type** helps Communication Manager decide how to handle the dialed string.

## Examples Of Digit Conversion

### Purpose

Your system uses the AAR or ARS Digit Conversion Table to change a dialed number for more efficient routing. Digits can be inserted or deleted from the dialed number. For instance, you can tell Communication Manager to delete a 1 and an area code on calls to one of your locations, and avoid long-distance charges by routing the call over your private network.

### ARS digit conversion examples

The ARS digit conversion table reflects these values:

- ARS feature access code = 9
- AAR feature access code = 8
- Private Network Office Code (also known as Home RNX) = 222
- Prefix 1 is required on all long-distance DDD calls
- Dashes (-) are for readability only

Communication Manager maps the dialed digits to the matching pattern that most closely matches the dialed number.

Example:

If the dialed string is 957-1234 and matching patterns 957-1 and 957-123 are in the table, the match is on pattern 957-123.

ARS digit conversion examples table:

| Operation  | Actual Digits Dialed            | Matching Pattern     | Replacement String | Modified Address | Notes   |
|--|---------------------------------|----------------------|--------------------|------------------|---|
| DDD call to ETN  | 9-1-303-538-1 345               | 1-303-538            | 362                | 362-1345         | Call routes via AAR for RNX 362   |
| Long-distance call to specified carrier  | 9-10222+DD D                    | 10222                | (blank)            | (blank)          | Call routes as dialed with DDD # over private network   |
| Terminating a local DDD call to an internal station  | 9-1-201-957-5 567 or 9-957-5567 | 1-201-957-5 or 957-5 | 222-5              | 222-5567         | Call goes to home RNX 222, ext. 5567  |
| Unauthorized call to intercept treatment   | 9-1-212-976-1 616               | 1-XXX-976            | #                  | (blank)          | "#" means end of dialing. ARS ignores digits dialed after 976. User gets intercept treatment. |
| International calls to an attendant  | 9-011-91-672 5 30               | 011-91               | 222-0111#          | 222-0111         | Call routes to local server (RNX 222), then to attendant (222-0111).                          |
| International call to announcement (This method can also be used to block unauthorized IDDD calls) | 9-011-91-672 5 30               | 011-91               | 222-1234#          | 222.1234-        | Call routes to local server (RNX 222), then to announcement extension (222-1234).             |
| International call from  | 0-00-XXXXXX XX                  | 00                   | +00+               | 00+XXXX          | The first 0 denotes   |

| Operation  | Actual Digits Dialed | Matching Pattern | Replacement String | Modified Address | Notes   |
|--|----------------------|------------------|--------------------|------------------|---|
| certain European countries needing dial tone detection |                      |                  |                    |                  | ARS, the second pair of 0s denotes an international call, the pluses denote "wait" for dial tone detection. |

### Defining operator assisted calls

Here is an example of how Communication Manager routes an ARS call that begins with 0 and requires operator assistance. The user dials 9 to access ARS, then a 0, then the rest of the number.

- 
1. Type `display ars analysis 0`.
  2. Press **Enter** to view the AAR and ARS Digit Analysis Table screen starting with 0.  
 We will use the ARS digit analysis table shown above and follow the routing for an operator assisted a call to NJ.  
 We will use the ARS digit analysis table shown above and follow the routing for an operator assisted a call to NJ.
    - A user dials 9 0 908 956 1234.
    - Communication Manager drops the ARS FAC (9 in our example), looks at the ARS Digit Analysis Table for 0, and analyzes the number. Then it:
      - determines that more than 1 digit was dialed
      - rules out the plan for 00, 01, and 011
      - determines that 11 digits were dialed
    - Communication Manager routes the call to route pattern 1 as an operator assisted call.

### Defining Inter-exchange carrier calls

Here is an example of how Communication Manager routes an ARS call to an inter-exchange (long-distance) carrier (IXC). IXC numbers directly access your long-distance carrier lines. IXC numbers begin with 1010, followed by three digits, plus the number as it is normally dialed including 0, 00, or 1+ 10 digits. These numbers are set up on your default translations. Remember, the user dials 9 to access ARS, then the rest of the number.

- 
1. Type `display ars analysis 1`.
  2. Press **Enter** to view the ARS Digit Analysis Table screen starting with 1.

This table shows five translations for IXC calls.

When you use `x` in the **Dialed String** field, Communication Manager recognizes `x` as a wildcard. The `x` represents any digit, 0 - 9. If I dial 1010, the next 3 digits will always match the `x` wild cards in the dialed string.

Use the ARS digit analysis table shown above and follow the routing for an IXC call to AT&T. 1010288 is the carrier access code for AT&T.

- A user dials 9 1010288 plus a public network number.
- Communication Manager drops the ARS FAC (9 in our example), looks at the ARS Digit Analysis Table for 1010, and analyzes the number.
- Then it matches 288 with `xxx` and sends the call over route pattern 5.

---

### Restricting area codes and prefixes

Certain area code numbers are set aside in the North American Numbering Plan. These numbers are 200, 300, 400, 500, 600, 700, 800, 877, 888, 900. You need to specifically deny calls made to area codes 200 through 900 (except 800 and 888).

You can also deny access to the 976 prefix, which is set aside in each area code for pay-per call services, if you do not want to incur charges. You can block 976 or any other prefix in all NPAs with a single entry in the digit analysis table. See *Using wild cards* for more information.

- 
1. Set the 200 area code apart from other area codes 201 through 209.  
We use the digit analysis table 120 because it defines long distance calls that begin with 1 and all area codes from 200 through 209.
  2. To deny long distance calls to the 200 area code, type `change ars analysis 120`.
  3. Press **Enter** to view the ARS Digit Analysis Table screen beginning with 120.  
The table (on the screen) in this example shows two translations for calls that begin with 120.  
First, follow the routing for a long-distance call that begins with 120 and is allowed. The 120 translation handles all dial strings 1-201 through 1-209, and there are many matches.
    - A user dials 9 120 plus 8 digits (the first of the 8 digits is not 0).
    - Communication Manager drops the ARS FAC (9 in our example), looks at the **ARS Digit Analysis Table** for 120, and analyzes the number. It determines the call is long-distance and sends the call over route pattern 4

Now we will follow a call that begins with the restricted area code 200. Only one string matches this translation.

- A user dials 9 1200 plus 7 digits.
- Communication Manager drops the ARS FAC (9), and looks at the **ARS Digit Analysis Table** for 1200. It determines that the call type is deny, and the call does not go through.

---

### Using wild cards

You can use wild cards to help separate out calls to certain numbers. Remember, when you use the wild card `x` in the **Dialed String** field, Communication Manager recognizes `x` as any digit, 0 - 9. For example, you can restrict users from making calls to a 555 information operator where you might incur charges.

- 
1. Type `change ars analysis 1`.
  2. Press **Enter**.  
The ARS Digit Analysis Table screen beginning with 1 appears.
  3. Use the arrow keys to move to a blank **Dialed String** field.
  4. Enter `1xxx555` in the **Dialed String** field.
  5. Enter `11` in the **Total Min** and `11` in **Total Max** fields.
  6. Enter `deny` (denied) in the **Route Pattern** field.
  7. Enter `fnhp` in the **Call Type** field.
  8. Press **Enter** to save your changes.

---

### Defining local information calls

You can set up Communication Manager to allow calls to local information, or in this example, 411.

To allow 411 service calls:

- 
1. Type `change ars analysis 4`.
  2. Press **Enter**.  
The ARS Digit Analysis Table screen beginning with 4 appears.
  3. Use the arrow keys to move to a blank **Dialed String** field.
  4. Enter `411` in the **Dialed String** field.
  5. Enter `3` in the **Total Min** and `3` in **Total Max** fields.
  6. Enter `1` in the **Route Pattern** field.

7. Enter `svcl` (service call) in the **Call Type** field.
  8. Press **Enter** to save your changes.
- 

## Administering Call Type Digit Analysis

### Prerequisites

There must be at least one entry in the **Call Type Digit Analysis Table** for Call Type Digit Analysis to take place.

---

1. Enter `change calltype analysis`.  
The **Call Type Digit Analysis Table** appears.
  2. In the **Match** field, enter the digits the system uses to match to the dialed string.  
The dialed string contains the digits that Communication Manager analyzes to determine how to process the call.  
For example, enter `303` to match any dialed number beginning with 303.
  3. In the **length: Min Max** fields, enter the minimum and maximum number of dialed digits for the system to match.
  4. Enter up to four digit manipulations for this **Match** string.
  5. Enter the number of digits to delete, the number of digits to insert, and the call type against which to test the modified digit string.
- 

### Call Type Digit Analysis Example

In our example, this is the administered **Call Type Digit Analysis Table**.

In our example, Communication Manager analyzes 3035554927 for routing.

1. Communication Manager deletes 0 digits, inserts nothing, and searches the resulting 3035554927 against the ARS tables.
2. If there are no matching entries, Communication Manager deletes 0 digits, inserts the digit 1, and searches the resulting 13035554927 against the ARS tables.
3. If there are no matching entries, Communication Manager deletes 3 digits, inserts nothing, and searches the resulting 5554927 against numbers of **ext** type in the dial plan.
4. If there are no matching entries, Communication Manager deletes 0 digits, inserts 011, and searches the resulting 0113035554927 against the ARS tables.

## Setting up Multiple Locations

### Prerequisites

Ensure that the **Multiple Locations** field on the System Parameters Customer-Options (Optional Features) screen is set to `y`. If this field is set to `n`, contact your Avaya representative for more information. If you are setting up locations across international borders, you must ensure that the **Multinational Locations** field on the System Parameters Customer-Options (Optional Features) screen is also set to `y`.

Be sure your daylight savings rules are administered. Daylight Savings Rule numbers are located on the Daylight Savings Rules screen.

Each cabinet in a server or switch and each port network in the cabinet must be assigned a location number. See the `add-cabinet` and `change-cabinet` in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

---

You can define a location number for:

- Remote Offices
- Media gateways
- IP network regions, used by IP stations and IP trunks

You can create numbering plans and time zone and daylight savings plans that are specific for each location. Choose your main location, and offset the local time for each location relative to the system clock time. The main location is typically set to have offset 0.

For example, we will set up multiple locations for Communication Manager server with cabinets in Chicago and New York. Location 1 is assigned to the cabinet in Chicago, our main office, so Central Standard Time is used for our main location. Location 2 is assigned to the cabinet in New York. We'll define the numbering plan area (NPA) for the Chicago and New York locations, and set the time zone offset for NY to show the difference in time between Eastern Standard Time and Central Standard Time.



#### Tip:

Type `list cabinets` to see the Cabinet screen and a list of cabinets and their locations.

To define locations for cabinets in Chicago and New York:

- 
1. Type `change locations`.
  2. Press `Enter`.  
The Locations screen appears.
  3. Type `y` in the **ARS Prefix 1 required for 10-digit NANP calls** field.  
Our dial plan requires users to dial a 1 before all 10-digit (long distance) NANP calls.
  4. Type `Chicago` in the **Name** field in the **Number 1 row**.

Use this field to identify the location.

5. Type `+00:00` in the **TimeZone Offset** field in the **Number 1 row**.  
In our example, the system time and the Chicago location time are the same.
6. Type `1` in the **Daylight Savings Rule** field in the **Number 1 row**.  
In our example, daylight savings rule 1 applies to U.S. daylight savings time.



**Tip:**

Use the `display daylight-savings-rules` command to see what rules have been administered on Communication Manager.

7. Type `312` in the **Number Plan Area Code** field in the **Number 1 row**.  
In our example, 312 is the local area code for Chicago, location 1.
8. Type `New York` in the **Name** field in the **Number 2 row**
9. Type `-01:00` in the **TimeZone Offset** field in the **Number 2 row**.  
In our example, subtract one hour from the system clock in Chicago to provide the correct time for the location in New York.
10. Type `1` in the **Daylight Savings Rule** field in the **Number 2 row**.  
In our example, daylight savings rule 1 applies to U.S. daylight savings time, and both locations use the same rule.
11. Type `212` in the **NANP** field in the **Number 2 row**.  
In our example, 212 is the local area code for New York, location 2.
12. Press **Enter** to save your changes.  
See *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information on the Multiple Locations feature.

---

## Routing with multiple locations

### Prerequisites

Be sure the **Multiple Locations** field on the System Parameters Customer-Options (Optional Features) screen is set to `y`. If this field is set to `n`, contact your Avaya representative for more information.

AAR or ARS must be administered.

- For AAR, verify that either the **Private Networking** field or the **Uniform Dialing Plan** field is `y` on the System Parameters Customer-Options (Optional Features) screen.
- For ARS, verify that the **ARS** field is `y` on the System-Parameters Customer-Options (Optional Features) screen.

You can define a location number for:

- Remote Offices
- Media gateways
- IP network regions, used by IP stations and IP trunks

---

When you set up multiple locations, you can define call routing that covers all locations as well as call routing specific to each individual location. Use your routing tables to define local routing for 911, service operators, local operator access, and all local calls for each location. Leave long-distance and international numbers that apply across all locations on the routing tables with **Location** field set to all.

For example, we will use ARS to set up local call routing for two Communication Manager server locations. Our Chicago server is assigned to location 1, and our New York server is assigned to location 2.

Our example shows a simple local dialing plan. Each location already contains location-specific routing tables. We'll use route pattern 1 for local service calls and route pattern 2 for local HNPA calls in the Chicago location.



**Tip:**

Create location-specific routing by assigning different route patterns for each location

To define local calls for servers in Chicago and New York:

- 
1. Type `change ars analysis location 1`.
  2. Press **Enter**.  
The ARS Digit Analysis Table screen for location 1 appears.
  3. Type the information for local dialed strings and service calls in each row on the screen.

In our example, for location 1 (Chicago) local HNPA calls:

- a. Type the appropriate digit in the **Dialed String** field.
- b. Type 7 in the **Total Min** field.
- c. Type 7 in the **Total Max** field.
- d. Type 2 in the **Route Pattern** field.
- e. Type `hnpa` in the **Call Type** field.

In our example, for location 1 (Chicago) local service calls:

- a. Type the appropriate digits in the **Dialed String** field.
- b. Type 3 in the **Total Min** field.
- c. Type 3 in the **Total Max** field.
- d. Type 1 in the **Route Pattern** field.

- e. Type `svcl` in the **Call Type** field.
  4. Press **Enter** to save your changes.
  5. Type `change ars analysis 4 location 2`.
  6. Press **Enter**.  
The **ARS Digit Analysis Table** for location 2 appears
  7. Type in the local HNPA and service call routing information for New York.
  8. Press **Enter** to save your changes.  
See Automatic Routing in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information on ARS.  
See Multiple Locations in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205 for more information on the Multiple Locations feature.
- 

## Call routing modification

If your system uses ARS Digit Analysis to analyze dialed strings and select the best route for a call, you must change the digit analysis table to modify call routing. For example, you'll need to update this table to add new area codes or to restrict users from calling specific areas or countries.

### Adding a new area code or prefix

#### Prerequisites

A common task for system administrators is to configure their system to recognize new area codes or prefixes.

When you want to add a new area code or prefix, you look up the settings for the old area code or prefix and enter the same information for the new one.

#### Tip:

Use **display toll xxx**, where xxx is the prefix you want to add, to see if the new area code or prefix number is set up as a toll call (y) or not. Some users might not be allowed to dial toll call numbers.

We will add a new area code. When the California area code, 415, splits and portions change to 650, you will need to add this new area code to your system.

#### Tip:

If you do not need to use 1 for area code calls, omit the 1 in steps 1, 4, and 7 in our example. Also, enter 10 in the **Total Min** and **Total Max** fields (instead of 11) in step 8.

- 
1. Type `list ars route-chosen 14152223333`.
  2. Press **Enter**.  
You can use any 7-digit number after 1 and the old area code (415). We used 222-3333.  
The ARS Route Chosen Report screen appears.
  3. Write down the **Total Min**, **Total Max**, **Route Pattern**, and **Call Type** values from this screen.  
In this example, the **Total Min** is **11**, **Total Max** is **11**, **Route Pattern** is **30**, and the **Call Type** is **fnpa**.
  4. Type `change ars analysis 1650`.
  5. Press **Enter**.  
The ARS Digit Analysis Table screen appears.
  6. Move to a blank **Dialed String** field.  
If the dialed string is already defined in your system, the cursor appears in the appropriate **Dialed String** field, where you can make changes.
  7. Enter 1650 in the **Dialed String** field.
  8. Enter the **minimum** and **maximum** values from step 2 in the **Total Mn** and **Total Mx** fields.  
In our example, enter 11 in each field.
  9. Enter the `route pattern` from step 2 in the **Route Pattern** field.  
In our example, enter 30
  10. Enter `fnpa` in the **Call Type** field.
  11. Enter the node number from step 2 in the **Node Num** field.  
For our example, leave the node number blank.
  12. Press **ENTER** to save your changes.  
To add a new prefix, follow the same directions, except use a shorter dial string (such as `list ars route-chosen 2223333`, where 222 is the old prefix) and a dial type of `hnpa`.



**Tip:**

If you change an existing area code for a network with multiple locations, be sure to change the **Number Plan Area Code** field on the Locations screen.

---

### Using ARS to restrict outgoing calls

ARS allows you to block outgoing calls to specific dialed strings. For example, you can restrict users from making international calls to countries where you do not do business, or in the U.S. you can restrict access to 900 and 976 pay-per-call numbers.

 **Security alert:**

To prevent toll fraud, deny calls to countries where you do not do business. The following countries are currently concerns for fraudulent calling.

| country     | code | country  | code |
|-------------|------|----------|------|
| Colombia    | 57   | Pakistan | 92   |
| Ivory Coast | 225  | Peru     | 51   |
| Mali        | 23   | Senegal  | 221  |
| Nigeria     | 234  | Yemen    | 967  |

To prevent callers from placing calls to Colombia (57):

- 
1. Type `change ars analysis 01157`.
  2. Press **Enter**.
    - a. Enter `011` (international access)
    - b. Enter the `country code` (`57`)

The ARS Digit Analysis Table screen appears.
  3. Move to a blank **Dialed String** field.  
Skip to Step 6 to deny calls to this dialed string  
If the dialed string is already defined in your system, the cursor appears in the appropriate **Dialed String** field.
  4. Enter `01157` in the **Dialed String** field.
  5. Enter `10` in the **Total Min** and `23` in **Total Max** fields.
  6. Enter `deny` (denied) in the **Route Pattern** field.
  7. Enter `intl` in the **Call Type** field.
  8. Press **Enter** to save your changes.
- 

## Overriding call restrictions

### Prerequisites

Verify that the **Authorization Codes** field on the System Parameters Customer-Options (Optional Features) screen is set to `y`.

 **Security alert:**

You should make authorization codes as long as possible to increase the level of security. You can set the length of authorization codes on the Feature-Related System Parameters screen.

---

You can use authorization codes to enable callers to override a station's calling privileges. For example, you can give a supervisor an authorization code so they can make calls from a telephone that is usually restricted for these calls. Since each authorization code has its own COR, the system uses the COR assigned to the authorization code (and FRL assigned to the COR) to override the privileges associated with the employee's telephone.

Note that authorization codes do not override dialed strings that are denied. For example, if your ARS tables restrict users from placing calls to Colombia, a caller cannot override the restriction with an authorization code.

We will create an authorization code 4395721 with a COR of 2.

- 
1. Type `change authorization-code 4395721`.
  2. Press **Enter**.  
The Authorization Code - COR Mapping screen appears.
  3. In the **AC** field, type 4395721.
  4. In the **COR** field, enter 2.
  5. Press **Enter** to save your changes.
- 

## ARS Partitions

Most companies want all their users to be able to make the same calls and follow the same route patterns. However, you might find it helpful to provide special calling permissions or restrictions to a group of users or to particular telephones.

ARS partitioning allows you to provide different call routing for a group of users or for specific telephones.

 **Note:**

If you used partitioning on a prior release of Avaya Communication Manager and you want to continue to use partitioning, please read this section carefully. In this release of Avaya Communication Manager, partition groups are defined on the **Partition Route Table**. If you want to define routing based on partition groups, use the **Partition Route Table**. Partition groups are no longer defined on the Digit Analysis Table.

**Related topics:**

[Setting up Time of Day Routing](#) on page 336

## Setting up partition groups

### Prerequisites

- Ensure that the **Tenant Partitioning** field on the System Parameters Customer-Options (Optional Features) screen is `y`.
- Ensure that the **Time of Day Routing** field on the System Parameters Customer-Options (Optional Features) screen is `n`.

Let us say you allow your employees to make local, long distance, and emergency calls. However, you have a lobby telephone for visitors and you want to allow users to make only local, toll-free, and emergency calls from this telephone.

To restrict the lobby telephone, you modify the routing for a partition group to enable only specific calls, such as U.S. based toll-free 1-800 calls, and then assign this partition group to the lobby telephone.

To enable 1-800 calls for partition group 2:

---

1. Type `list ars route-chosen 18002221000`.

2. Press **Enter**.

You can use any 7-digit number following the 1800 to create an example of the dialed string.

The ARS Route Chosen Report screen for `partition group 1` appears.

3. Record the route pattern for the selected dialed string.

In our example, the route pattern for 1800 is `p1`. This indicates that the system uses the Partition Routing Table to determine which route pattern to use for each partition.

 **Note:**

If there was a number (with no `p`) under Route Pattern on the Route Chosen Report, then all partitions use the same route pattern. You need to use the Partition Routing Table only if you want to use different route patterns for different partition groups.

4. Press **Cancel** to return to the command prompt.

5. Type `change partition-route-table index 1`.

6. Press **Enter**.

The Partition Routing Table screen appears. In our example, partition group 1 can make 1800 calls and these calls use route pattern 30.

7. In the **PGN2** column that corresponds to Route Index 1, type `30`.

8. Press **Enter**.

This tells the system to use route pattern 30 for partition group 2 and allow partition group 2 members to make calls to 1800 numbers.

---

## Assigning a telephone to a partition group

### Prerequisites

To assign an extension to a partition group, first assign the partition group to a COR, and then assign that COR to the extension.

- 
1. Type `list cor`.
  2. Press **Enter**.
  3. The Class of Restriction Information screen appears.
  4. Choose a COR that has not been used.  
In our example, select 3
  5. Type `change cor 3`.
  6. Press **Enter**.  
The Class of Restriction screen appears.
  7. Type a name for this COR in the **COR Description** field.  
In our example, type **lobby**
  8. Enter 2 in the **Partitioned Group Number** field.
  9. Now to assign COR 3 to the lobby telephone at extension 1234:
    - a. Type `change station 1234`.
    - b. Press **Enter**.  
The Station screen for 1234 appears.
    - c. In the **COR** field, enter 3.
    - d. Press **Enter** to save your changes.
- 

## Setting up Time of Day Routing

### Prerequisites

AAR or ARS must be administered on Communication Manager before you use Time of Day Routing.

- For AAR, verify that either the **Private Networking** field or the **Uniform Dialing Plan** field is `y` on the System Parameters Customer-Options (Optional Features) screen.
  - For ARS, verify that the **ARS** field is `y` and the **Time of Day Routing** field is `y` on the System Parameters Customer-Options (Optional Features) screen.
-

Time of Day Routing lets you redirect calls to coverage paths according to the time of day and day of the week. You need to define the coverage paths you want to use before you define the time of day coverage plan.

You can route calls based on the least expensive route according to the time of day and day of the week the call is made. You can also deny outgoing long-distance calls after business hours to help prevent toll fraud. Time of Day Routing applies to all AAR or ARS outgoing calls and trunks used for call forwarding to external numbers.

As an example, we will allow our executives to make long distance calls during business hours. Let us look at the Time of Day Routing Plan before we make any changes

To display your Time of Day Routing Plan:

- 
1. Type `display time-of-day 1`.
  2. Press **Enter**.  
The Time Of Day Routing Plan screen for plan 1 appears.



**Note:**

Make a note of the routing plan that is currently in effect. In our example, this plan is for employees who can only make local calls.

You can see that in our example, two partition group numbers control time of day routing. PGN 1 begins one minute after midnight (00:01) every day of the week, and is used for after-business hours and all day Saturday and Sunday. PGN 2 is assigned to office hours Monday through Friday, not including noon (12:00) to 1:00 p.m. (13:00).

3. Press **Cancel** to clear the screen.

---

## Creating a New Time of Day Routing Plan

- 
1. Type `change time-of-day 2`.
  2. Press **Enter**.
  3. Type **1** in each field as shown on **Time of Day Routing Plan 1**.  
In our example, this is the PGN used for after hours and the lunch hour.
  4. Type **3** in all other fields.  
In our example, PGN 3 uses the route pattern for long-distance calls during business hours. We can save money by using the trunk lines provided by our new long-distance carrier.
  5. Press **Enter** to save your changes.
  6. Now assign your new Time of Day Routing Plan 2 to the COR assigned to your executives  
See *Class of Restriction* to view where to assign this field.

For this example, assume the following:

- Jim is the user at extension 1234.
- Extension 1234 is assigned a COR of 2.
- COR 2 is assigned a Time of Day Plan Number of 1.
- The Time of Day Routing Plan 1 is administered as shown in the example above.

When Jim comes into work on Monday morning at 8:30 and makes an ARS call (dials the ARS access code followed by the number of the person he is calling), the system checks the Time of Day Plan Number assigned to Jim's COR

Because Jim has a COR of 2 with Time of Day Plan Number 1, the system uses Time of Day Routing Plan 1 to route the call.

According to Time of Day Routing Plan 1, calls made between 8:00 a.m. and 11:59 a.m. route according to the route pattern set up on PGN 1.

If Jim makes a call between 12:00 p.m. and 1:00 p.m. on Monday, the Time of Day Routing Plan 1 is used again. However, this time the call is routed according to PGN 2.

---

## Setting up a Remote user by Network region and Time zone

With your system located in New York and a remote user located in Germany, to create the correct time zone settings:

- 
1. Type `change locations`.
  2. Press `Enter`.  
The Locations screen displays.
  3. In the **Name** field, enter the name of the location (for instance, Germany).
  4. In the first **Timezone Offset** field, enter `+` to indicate the time is ahead of the system time.
  5. In the second **Timezone Offset** field, enter `08` for the number of hours difference between this location and system time.
  6. In the **Daylight Savings** field, enter `1` if this country has daylight savings.
  7. Press `Enter` to save your changes.
  8. Type `change ip-network-map`.
  9. Press `Enter`.  
The IP Address Mapping screen displays.

10. In the **From IP Address** field, enter the IP address for the remote station in Germany.
  11. In the **To IP Address** field, enter the IP address of your system.
  12. In the **Subnet** or **Mask** field, enter the subnet mask value of your network
  13. In the **Region** field, enter a number that is not being used. In this example, enter 3.
  14. Press `Enter` to save your changes.
  15. Type `change ip-network-region 3`.
  16. Press **Enter**.  
The IP Network Region screen displays.
  17. In the **Name** field, enter the location name for familiarity.
  18. In the **Location** field, enter the number from the Locations screen. In this example, it was 11.
  19. Press **Next Page** until you get to page 3, the Inter Network Region Connection Management screen.
  20. Notice in the **src rgn** column that a 3 displays, and under **dst rgn** a 1, indicating that Network Region 3 (Germany) is connected to Network Region 1 (New York) using Codec Set 1.
  21. Press `Enter` to save your changes  
See *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for more information on the Multiple Locations feature.
- 

## No-cadence call classification modes and End OCM timer

Use the No-cadence call classification modes and End OCM timer feature to improve the call classification time and accuracy used for voice and answering machine call classification.

### Setting up no-cadence call classification modes

---

1. Type `change system-parameters ocm-call-classification`. Press `Enter`. The system displays the System Parameters OCM Call Classification screen.
  2. Set the **Cadence Classification After Answer** field to `n`.
  3. Press `Enter` to save your changes.
- 

### Setting up End OCM timer and announcement extension

- 
1. Type **change location-parameters**. Press `Enter`. The system displays the System Parameters OCM Call Classification screen.
  2. In the **End OCM After Answer (msec)** field, type the desired timeout value in milliseconds. Valid entries are a number from 100 to 25,000, or blank. In the **End of OCM Intercept Extension** field, type the extension number that you want to assign. The number can be a recorded announcement, a vector directory number, or a hunt group extension.
  3. Press `Enter` to save your changes.
- 

## Alerting Tone for Outgoing Trunk Calls

Use the Alerting Tone for Outgoing Trunk Calls feature to apply an alerting tone to an outgoing trunk call after an administrable amount of time.

### Setting the outgoing trunk alerting timer

- 
1. Enter `change cor n`, where *n* is the number of a specific COR.
  2. Click **Next** until you see the **Outgoing Trunk Alerting Timer (minutes)** field.
  3. In the **Outgoing Trunk Alerting Timer (minutes)** field, specify when the initial alerting tone must be applied to the call.
  4. Select **Enter** to save your changes.
- 

### Setting the trunk alerting tone interval

- 
1. Enter `change system-parameters features`.
  2. Click **Next** until you see the **Trunk Alerting Tone Interval (seconds)** field.
  3. In the **Trunk Alerting Tone Interval (seconds)** field, specify the interval at which the alerting tone must be repeated on the call.
  4. Select **Enter** to save your changes.
- 

---

## Multimedia Calling — Multimedia Applications Server Interface

The Multimedia Applications Server Interface (MASI) defines a protocol and a set of operations that are used to extend Avaya Communication Manager feature functionality to a Multimedia Communications Exchange (MMCX) system. MASI architecture fits the client/server model,

where Avaya Communication Manager functions as a server for MMCX clients. Examples of features supported by MASI include call detail recording (CDR), Communication Manager Messaging, and Automatic Alternate Routing (AAR)/Automatic Route Selection (ARS).

MMCX can make use of both MASI features and MMCX autonomous features. Autonomous features are those that MMCX provides, even if MASI is not enabled. This document does not discuss them unless there is a consideration for MASI administration.

Some autonomous MMCX features:

- Basic Call (Place/Drop)
- Call Coverage
- Conference
- Transfer

Avaya Communication Manager /MASI features:

- Basic Call (Place/Drop) - Avaya Communication Manager tracks the status of all calls placed to or from a MASI terminal.
- Call Detail Recording - Avaya Communication Manager tracks calls to and from MASI terminals and can produce call records that indicate if a call uses MASI
- Call Coverage - Avaya Communication Manager tracks MMCX calls that are sent to coverage. A Communication Manager coverage path can contain both MASI terminals and Communication Manager stations.
- Conference - Avaya Communication Manager tracks conference calls that involve MASI terminals, if a Communication Manager station originates the conference. Conferences that involve MASI terminals and Communication Manager stations are voice-only. If the Communication Manager station originates the call, the caller can use the consultative form of conference or transfer.
- World Class Routing (AAR or ARS) - Calls from MASI terminals can take advantage of Avaya Communication Manager World Class Routing capabilities.
- Voice messaging access to AUDIX/INTUITY - MMCX users can take advantage of AUDIX voice messaging, and receive message waiting indication.
- MMCX trunking - By assigning trunk access codes to interfaces from the MMCX to other MMCXs or the PSTN, Avaya Communication Manager can monitor traffic over those interfaces.

## Prerequisites— Multimedia Applications Server Interface

For purposes of administration, there are feature buttons and groups of users that you must not administer with MASI terminal extensions. There are also features that you simply cannot administer for a MASI terminal, because the software does not allow it.

### **Caution:**

Avaya Communication Manager offers a wide range of features, and MMCX users might want to take advantage of this. In some cases, these features will operate as expected. However, some features are not supported for use over the MASI link, and their behavior is unpredictable. You might cause harm to your system by attempting to use these features.

The Interactions section contains a list of features, and lists those features that are absolutely not supported for use with MASI. If you administer features on the DO NOT ADMINISTER list, Avaya cannot be responsible for the result.

Before you start to administer MASI, you should make a plan for how to do it. Among the configurations on the following pages, there is probably one that matches the configuration of your system fairly closely. You might want to either write on these pages, or draw up your own configuration. It might help you if you have already determined trunk group and signaling group numbers, unused extensions, and so on. The following are things you need to consider:

- Establish the dial plan on the MMCX to agree with that of Avaya Communication Manager. If you use Universal Dial Plan and MMCX, you might need to make adjustments for the MMCX dial plan.
- Find unused extensions and trunk group numbers. You need:
  - one trunk group number for each ISDN-PRI connection to the MMCX
  - one signaling group number for each MASI node and an unused Communication Manager extension for the signaling group
  - one unused Communication Manager extension for the Near-End Path Termination number for all MASI Paths to this ECS. You can use the same number for all MASI nodes in the domain
  - two unused MMCX extensions for the nearpath and tscnum arguments to the chgmasi command. This is the command you use to administer MASI on the MMCX.

## List of terms

This is a list of terms that are specific to MASI, or that have meanings in the context of MASI that are not standard.

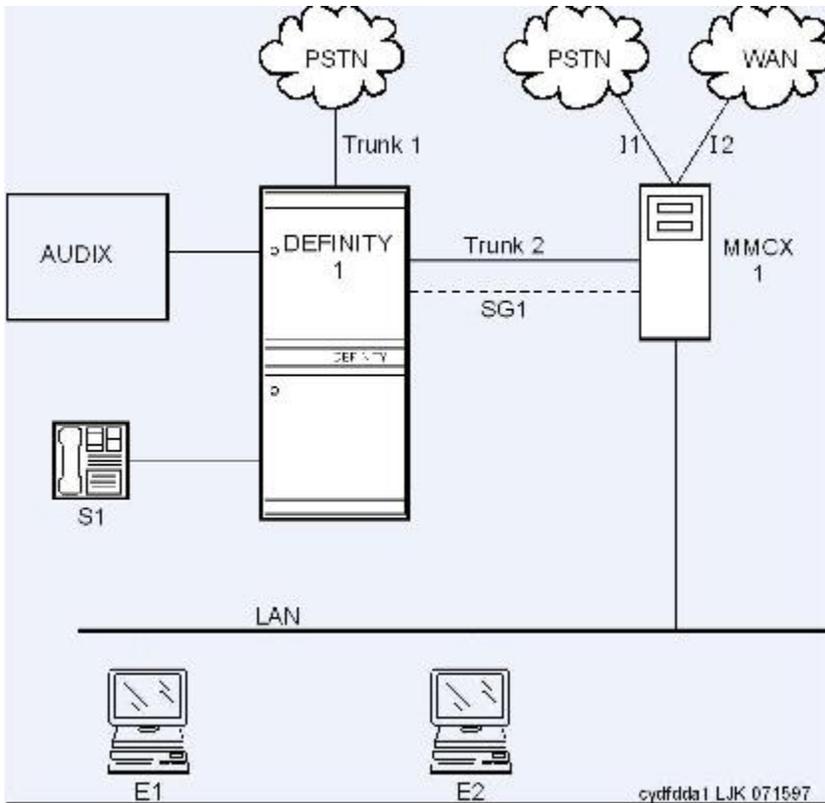
- chgmasi - The command you use to administer MASI at the MMCX administration terminal.
- Interserver - Connections between MMCX terminals on different MMCX servers/nodes.
- MASI domain - A MASI domain consists of Communication Manager and one or more MASI nodes that share the same dial plan. That is, the extension numbers on the MMCX are known to Communication Manager, and fit in the Communication Manager dial plan.
- MASI interworking - MASI interworking refers to the completion of a voice connection within Communication Manager, involving at least one MASI terminal and a MASI path.
- MASI link - The connection between the MMCX and Communication Manager.
- MASI node - A single MMCX server. You can connect more than one MASI node to a Communication Manager. Each node has a separate number. This node number needs to be consistent whenever referring to a specific MMCX server.
- MASI non-interworking - MASI non-interworking refers to the completion of a call by MMCX, not involving a MASI path.

- MASI path - The Integrated Services Digital Network (ISDN) B-channels between MMCX and Communication Manager in a MASI environment. Paths are used for voice and data connections between Communication Manager and MMCX.
- MASI signaling link - ISDN D-channel used to transport a new ISO protocol called the MASI protocol between Communication Manager and the MMCX.
- MASI terminal - The representation in Communication Manager of MMCX terminals in a MASI environment.
- MMCX interface - PRI interface for connecting an MMCX server to other public, private or wide area network (WAN) switching systems or equipment that is part of the public network. Similar to a Communication Manager trunk group. These can include non-MASI trunks connecting Communication Manager and the MMCX.
- MMCX trunk - The representation in Communication Manager of trunk or network facilities terminating on MMCX. For purposes of MASI, they are called "interfaces."

## **Configurations— Multimedia Applications Server Interface**

There are several ways to set up combinations of MASI nodes and DEFINITY servers. The following figures depict several possible configurations.

Figure 135: MASI domain of Avaya Communication Manager running on one DEFINITY Server and one MMCX



The parts of this drawing, for MASI, are as follows:

- Trunk 1 — This is any type of trunk connection to the public network
- Trunk 2 — This is the link between the Avaya Communication Manager solution and the MMCX, and requires a TN464C or later DS1 circuit pack. You administer this link as an ISDN-PRI trunk group, a MASI path and an NCA-TSC
- I1 and I2 — These are MMCX interfaces to destinations other than Avaya Communication Manager. Administer as MASI trunks
- E1 and E2 — Endpoints (terminals) belonging to the MMCX. Administer as MASI terminals
- MMCX — Determine a node number for each MMCX server. This can be any number from 1 to 15. Once the node number is established, Avaya Communication Manager informs the MMCX of its node number.
- S1 — Avaya Communication Manager station.

Figure 136: MASI domain of Communication Manager running on one DEFINITY Server and two (or more) MMCXs

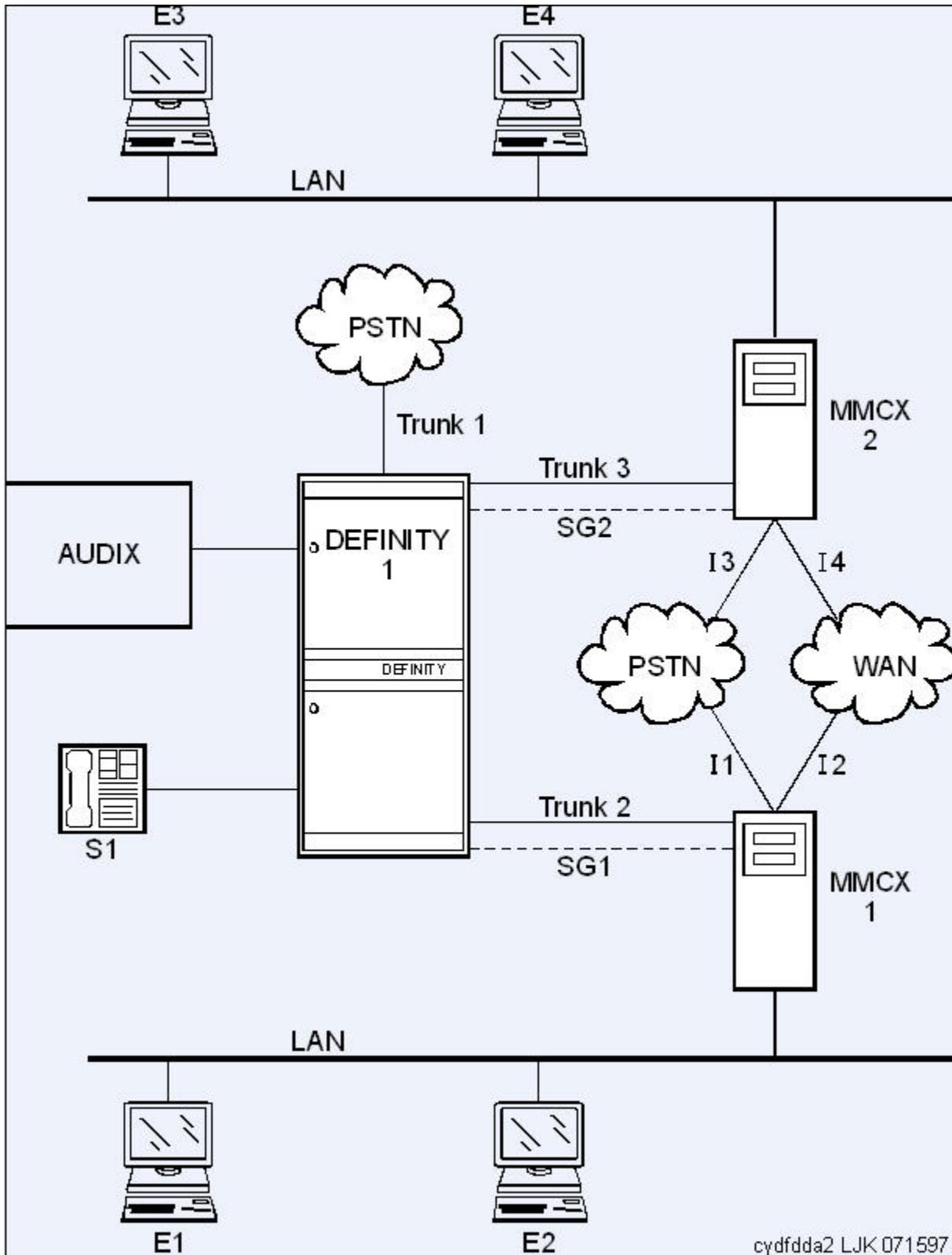


Figure 137: Two separate MASI domains

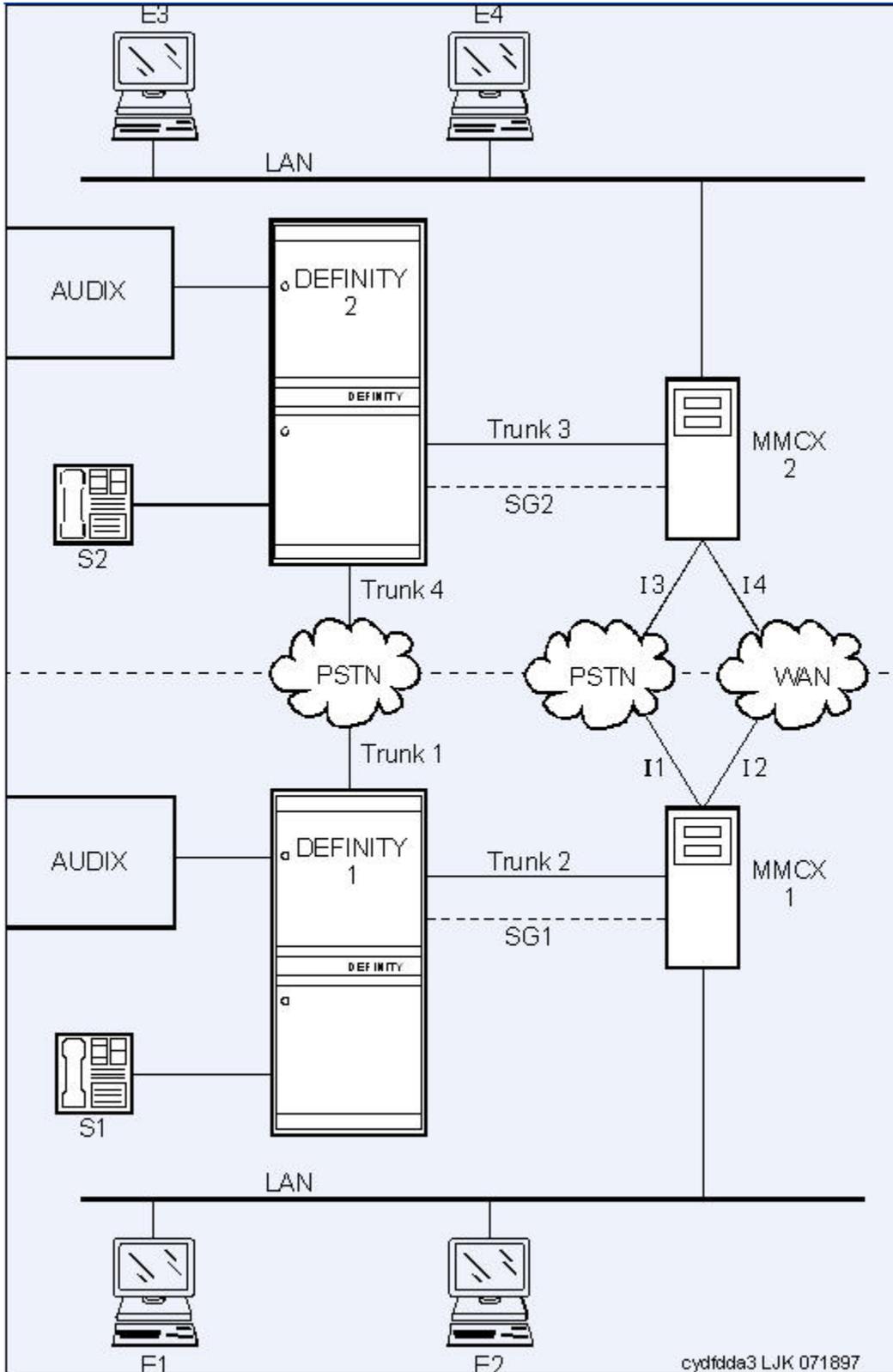
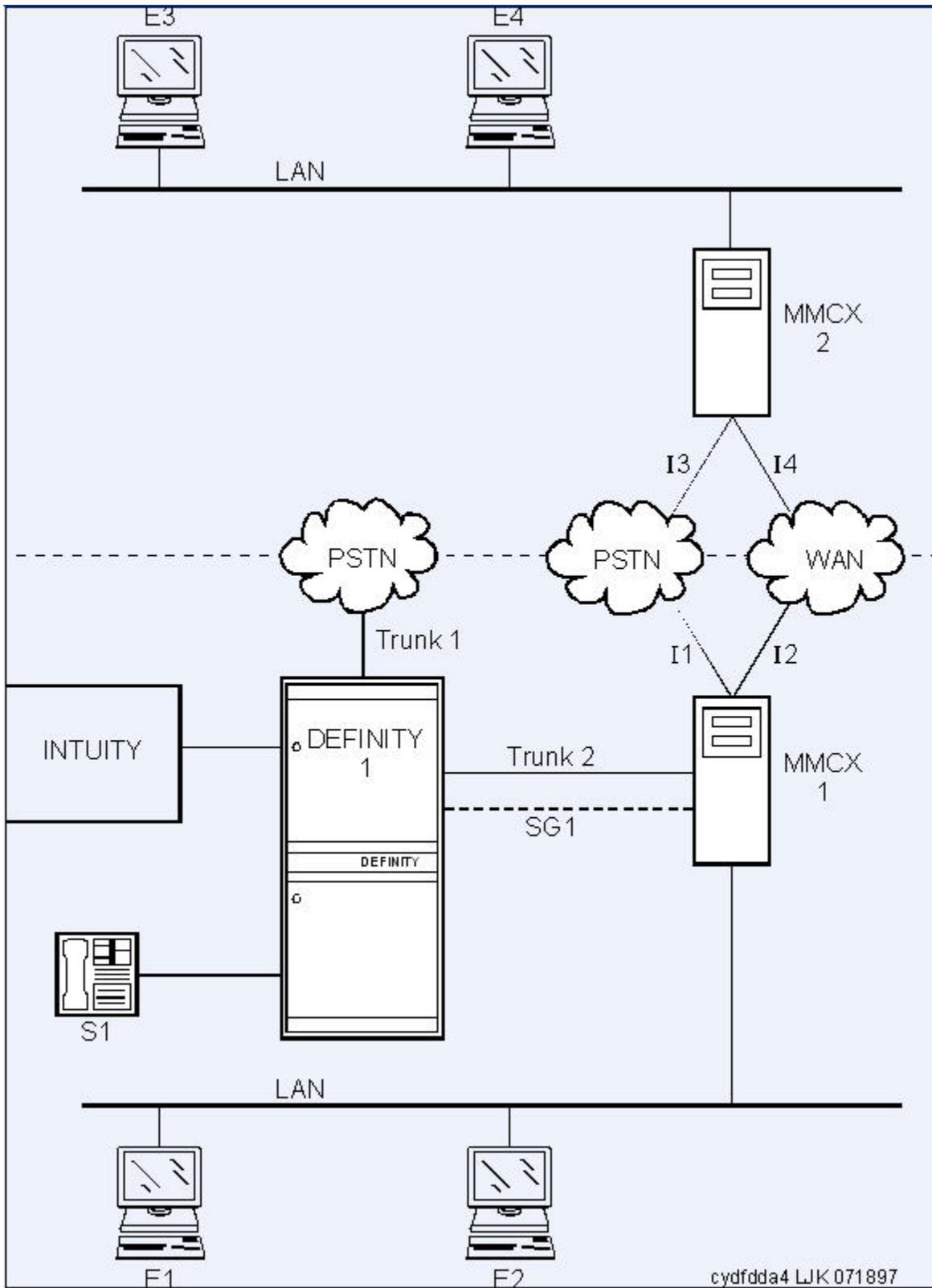


Figure 138: One MASI domain, and one non-MASI MMCX



The MASI node must be directly connected to the Avaya DEFINITY Server for MASI features to work. In this configuration, terminals that belong to MMCX 2 (E3 and E4) do not take advantage of MASI capabilities

## Multimedia Applications Server Interface Administration

This section discusses the administration required to make MASI work. You perform most of this administration from the DEFINITY Server administration terminal. However, there are a few things you must do at the MMCX administration terminal. This section sometimes refers to the `chgmasi` command. This is the command you use to administer MASI parameters on the MMCX. For more information about using the `chgmasi` command, see your MMCX documentation.

### Related topics:

[MASI with Communication Manager features](#) on page 356

## Establishing Customer Options

---

On the MMCX, MASI must be enabled using the `chgmasi` command.

An Avaya technical support representative must activate MASI using the System-Parameters Customer-Options (Optional Features) screen. The technical support representative should also verify that ISDN-PRI over PACCON (for DEFINITY Server CSI configurations), and AAR/ ARS are enabled.

## Establishing maintenance parameters and alarming options

---

Using the `set options` command (Avaya init or inads logins only), set MASI alarming options.



### Note:

Ensure that on the Maintenance-Related System Parameters screen, the **Packet Bus Activated** field is y.

For more information, see *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300432.

## Establishing the physical connection

---

Establishing the physical connection: Establish the physical connection between the Avaya DEFINITY Server and the MMCX.

---

## Administering the Circuit Pack

---

Using the DS1 Circuit Pack screen, verify that the DS1 circuit pack you use to establish the MASI link is administered as follows:

- Bit Rate = 1.544
- Line Coding = b8zs
- Line Compensation = 1
- Signaling Mode = isdn-pri
- Interface = network
- Country Protocol = 1
- Protocol Version = a

## Administering the Signaling Group

---

Administering a signaling group: For each MASI node, you need to establish a unique signaling group. Use the command `add signaling-group xxx` to access the Signaling Group screen.

For each link, establish a Non-Call Associated Temporary Signaling Connection (NCA-TSC) with the following attributes:

- **Associated Signaling** - MASI requires **Facility Associated Signaling**, so this field must be set to y.
- **Primary D-channel** - Enter a 6- to 7-character port number associated with the DS1 Interface circuit pack port. The port address of the PRI that carries D-channel signaling.

The port number is used to assign the primary D-channel in the Signaling Group. For 24-channel facilities, the 24th port is assigned as the D-channel. For 32-channel facilities, the 16th port is assigned as the D-channel.

- **Max Number of NCA TSC** - For MASI, this must be 1.
- **Max number of CA TSC** - Leave the default of 0.
- **Trunk Group For NCA TSC** - This can be left blank
- **Trunk Group for Channel Selection** - This can be left blank
- **Supplemental Service Protocol** - Values are a (AT& T) and b (Qsig).
- **Network Call Transfer?** - Values are y (yes) and n (no).
- **Service/Feature** - Leave blank.

- **As-needed Inactivity Time-out (min)** - This field only applies to as-needed NCA-TSCs. Since MASI requires a permanent connection, leave blank.
- **TSC Index** - This display-only field specifies the administered NCA-TSCs assigned
- **Local Ext** - Enter a valid, unassigned Avaya Communication Manager extension. This extension does not need a port assignment and does not need to correspond to any other administration.
- **Enabled** - Enter `y` to enable the administered NCA-TSC. You might want to wait to enable this link until all other administration is in place. If this is `y`, Avaya Communication Manager attempts to establish the connection as soon as you submit the form. This might cause your system to alarm, if other administration is not finished
- **Establish** - Used to indicate the strategy for establishing this administered NCA-TSC. Enter `permanent` for MASI.
- **Dest. Digits** - A valid MMCX extension. This must correspond to the value of the `tscnum` argument to the `chgmasi` command.

 **Note:**

These digits are sent as entered to the destination MMCX; no routing or other digit manipulation is performed

- **Appl.** - Specifies the application this administered NCA-TSC is going to be used for. Enter `masi`.
- **Machine ID** - Used to indicate the MASI node to which this administered NCA-TSC is connected. This number should be the same as the MASI node number found on other screens.

Listing or determining status of TSCs To determine which TSCs are designated for MASI, use the `list masi tsc` command.

This command displays the following:

- **Sig Grp** — The number of the signaling group to which this TSC belongs
- **Primary D-Channel** — Port location of the Primary D-channel
- **TSC Index** — The number of the MASI TSC within the signaling group
- **Local Ext.** — Communication Manager extension associated with the TSC
- **Enabled** — Indicates the state of the connection - enabled (y/n)
- **Established** — Value of established flag (as-needed/permanent)
- **Dest. Digits** — The MMCX extension that indicates the TSC destination
- **Mach. ID** — MASI node number

 **Note:**

Once you establish and enable the signaling group, you need to verify that it is active. Use the command `status signaling-group signaling-group#` or `status`

`tsc-administered signaling-group# [/tsc-index] [print]` to determine if the link is active.

---

## Administering ISDN-PRI Trunk Group

---

Use the command `add trunk-group xxx` to access the Trunk Group screen. For a more detailed description of the ISDN-PRI trunk group, see the documentation on *Trunk Group*.

Establish an ISDN-PRI trunk group with the following attributes:

- Group Type = isdn-pri
- TAC = valid TAC that conforms to your existing dial plan
- Direction = two-way
- Service Type = tie
- CDR Reports = n

You must also administer the PRI link from the MMCX to the ECS, using the MMCX administration terminal. See your *MMCX documentation* for information on the `addpri` command.

---

## Administering MASI Path Parameters

---

Use the `change masi path-parameters` command to access the MASI Path Parameters screen.

Establish a MASI Path with the following attributes:

- **Near-End Path Extension** — An unassigned Communication Manager extension. When using the `chgmasi` command to administer the MMCX, this is the `farpath` extension. See your *MMCX documentation* for more information.
  - **MASI Node** — The node number for the MMCX. For each MMCX/MASI node, this number must be the same everywhere it occurs (Signaling Group, MASI Trunk Group, and MASI Terminal screens).
  - **Trunk Group** — This is the trunk group number in Communication Manager for the ISDN-PRI trunk that will be used to establish call paths.
  - **Far-End Path Termination Number** — This is an unassigned MMCX extension. When using the `chgmasi` command to administer the MMCX, this is the `nearpath` extension. See your *MMCX documentation* for more information.
-

## Administering MASI Trunk Groups

---

1. Use the MASI Trunk Group screen to define MMCX interfaces that interconnect MASI nodes, or that connect MMCX nodes to another private switch or central office. Examples of MMCX interfaces include:
  - PRI trunks linking MMCX servers
  - PRI trunks linking MMCX to the PSTN
  - PRI trunks from MMCX to Avaya Communication Manager that are used for purposes other than MASI
  - LAN interfaces linking MMCX servers
2. Use the command `add masi trunk-group xxx` (or 'next') to access the MASI Trunk Group screen. The trunk group number must not be assigned, and you cannot exceed the maximum total trunks for your system. Valid values for xxx are unused trunk group numbers in Avaya Communication Manager between 1 to 96 for DEFINITY Server CSI configurations.
  - **Group Number** - This field displays the MASI trunk group number. This is the number assigned when executing the `add masi trunk-group` command.
  - **CDR Reports** - Valid entries are y, n, and r. Default is y.
    - If you enter y, Call Detail Recording (CDR) records will be generated by completed outgoing calls terminated on this trunk group. If incoming calls are being recorded (the **Record Outgoing Calls Only** field on the CDR System Parameters screen is set to n), then a single CDR record will be generated for answered calls with the call duration.
    - If you enter n, no CDR records will be generated by calls originated by or terminated on this trunk group.
  - **Group Name** - Enter a unique name that identifies the trunk group. Up to 27 characters can be used; default is INCOMING CALL.
  - **COR** - Enter a Class of Restriction (COR) number (0 to 995) that reflects the desired restriction; default is 1.
  - **TN** - This field displays the Tenant Partition number. All MASI trunks are associated with Tenant 1.
  - **TAC** - Enter the trunk access code (TAC) that identifies the trunk group on CDR reports. You must assign a different TAC to each MMCX interface. Valid entries conform to the dial plan (1 to 4 digits, \* and # are valid first digits).
  - **MASI Node Number** — The node number assigned to this MMCX machine.
  - **Remote Group Number** — This is the number of the remote trunk group. For ISDN-PRI interfaces, valid values are any number 1 to 8; for local area network (LAN) or WAN calling interfaces, the value must be 9. The combination of MASI

Node Number and Remote Group Number must be unique. Remote group number corresponds to the group number on the MASI node.

#### Viewing a list of all MASI trunk groups

To view a list of all the MASI trunks administered on the ECS, use the command `list masi trunk-group`.

#### Determining the status of MASI trunk groups

To determine the status of a specific MASI trunk, use the command `status masi trunk-group xxx`, where `xxx` is the trunk group number. This command provides descriptive information about the trunk, and the number of currently active trunk calls.

---

#### Related topics:

[1-number access](#) on page 389

### Administering MASI Terminals

---

Use the `add masi terminal xxxxx` or `next` command to administer each MASI terminal as a MASI terminal. You use available extensions on the ECS, so they need to conform to the Avaya Communication Manager dial plan. The extension must match the Communication Manager dial plan, and for the `add` command, the extension must not already be in use. The extension of the MASI terminal must match the number of the MASI terminal. Avaya Communication Manager users dial the MASI Terminal Extension to reach MMCX users

#### Note:

Anytime you add a terminal or other extension to the MMCX, you must administer a corresponding MASI terminal on Avaya Communication Manager. If you do not, you will not be able to dial this extension from Avaya Communication Manager.

- **Extension** — This field displays the extension that you entered on the command line.
- **BCC** — This field displays the bearer capability class of the terminal, and identifies the type of traffic the terminal supports. For MASI, this is always 0, for voice or voice-grade data.
- **MASI Node Number** — The number of the node on which this terminal resides.
- **TN** — The tenant partition in which this terminal resides. At present, all MASI terminals must reside within tenant 1. This field is display-only, and always 1.
- **COR** — The class of restriction associated with this terminal.
- **Name** — The name associated with the terminal. This can be any alphanumeric string up to 27 characters.

- **Send Display Info** — Indicates whether Avaya Communication Manager should forward display information associated with a call. Set to *y*.
- **LWC Reception** — This field indicates whether the terminal can receive Leave Word Calling (LWC) messages. Valid values are none, audix, and mas-spe (for DEFINITY Server CSI configurations). SPE-based LWC is not supported for MASI terminals. However, if embedded AUDIX is used without a Data Control Link, you must administer MASI terminals to receive SPE-based LWC messages. For such cases, the LWC feature is used by AUDIX messaging systems to activate and deactivate message waiting lamps on MASI terminals.
- **CDR Privacy** – Indicates whether CDR Privacy is supported for this terminal. See Call Detail Recording in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205 for more information.
- **Room** - Enter up to 10 characters to identify the MASI terminal location. This field can be blank.
- **Jack** - Enter up to 5 characters to identify the location where the MASI terminal is connected. This field can be left blank.
- **Cable** - Enter up to 5 characters to identify the cable that connects the MASI terminal to the system. This field can be left blank.
- **Floor** - Enter up to 7 characters to identify the floor where the MASI terminal is located.
- **Building** - Enter up to 7 characters to identify the building where the MASI terminal is located. Valid entries are listed in the site table.
- **BUTTON ASSIGNMENTS** — This field contains a call appearance button and is display only.

---

### ***Duplicating MASI Terminals***

---

Once you have one MASI terminal administered to your liking, you can use the `duplicate masi terminal` command to administer other stations with the same characteristics.

---

### ***Listing MASI Terminals***

1. To view a list of all the MASI terminals administered on a server, use the command `list masi terminals`.

This command only lists terminals within the domain of the Avaya DEFINITY Server from whose SAT you issue the command.

2. To view the active or idle status of a specific MASI terminal, use the command `status masi terminal(extension)`.
3. To determine which extension you assigned as the MASI Near-End Path Termination extension, use the command `list extension-type`.

This command displays the extension number and type (attendant, masi-terminal, etc.), as well as other information about the extension.

---

## Administering Features

---

1. AAR/ARS: To verify that this feature is enabled, use the command `display system-parameters customer-options`.

AAR/ARS is an optional feature on Avaya Communication Manager, and you need to purchase this option to use it with MMCX. If it is not enabled, contact your Avaya representative.

- a. The MMCX dial plan must use the same feature access codes as Avaya Communication Manager. If this is not already the case, modify the MMCX dial plan using the `chgdp` command.

See your MMCX documentation for more information.

- b. Include this feature access code in the `chgmasi` command.

2. CDR: To get call detail records for calls over MMCX interfaces, set CDR Reports = `y` on the MASI Trunk Group screen.
  - a. To get call records for calls over the ISDN-PRI trunk group, set CDR Reports = `y` on the ISDN-PRI Trunk Group screen.
  - b. To track calls between a MASI terminal and other MASI terminals or Communication Manager stations, enter the MASI terminal extension on the Intra-switch CDR screen.
  - c. Enter `n` in the **Record Non-Call Assoc TSC** field on the CDR System Parameters screen.

 **Note:**

If you use the same PRI trunks for MASI and non-MASI calls, Avaya strongly recommends that you do not enable CDR for these calls. Establish a separate trunk group for non-MASI calls and set CDR Reports = `n`.

3. Coverage: To establish coverage from a MASI terminal to AUDIX:, use the MMCX user interface to enter the AUDIX hunt group extension as the coverage point. You cannot use Avaya Communication Manager coverage administration for MASI terminals.

- a. If AUDIX ports are not administered in Avaya Communication Manager, you must administer them.
  - b. Set up the MASI terminal as an AUDIX subscriber. Enter the MASI terminal extension in the **Extension** field on the Subscriber Administration screen.
4. To establish coverage from a MASI terminal to another MMCX terminal or Avaya Communication Manager station, use the MMCX user interface to enter the desired extension as the coverage point for the MASI terminal.
- You cannot use Avaya Communication Manager coverage administration for MASI terminals.

---

### **Verifying Administration**

You should make test calls from Avaya Communication Manager to MMCX, to ensure that you can indeed place and receive calls

- 
1. Call an unattended MASI terminal.
  2. Verify that the call goes to AUDIX..
  3. Retrieve the call from the MASI terminal.
  4. Verify that all works as expected.

---

### **Setting MASI command permissions**

If you are the super-user for your system, you can restrict other administrative logins from changing MASI administration.

- 
1. To do this, use the `change permissions(login-ID)` command.
  2. Enter `y` in the **Additional Restrictions** field, then move to the Restricted Object List page of the screen.

You can restrict the following MASI-related objects:

- masi-path-parameters
- masi-terminal
- masi-trunk-group
- masi-tsc

---

### **MASI with Communication Manager features**

- AAR/ARS — MMCX can take advantage of advanced routing features for voice-only calls to the public switched telephone network (PSTN) or an Avaya private network. Users must enter the AAR/ ARS access code before the rest of the dialed digits. MASI will route the call over the Communication Manager private network (AAR) or the public network (ARS), based on digits supplied by the MMCX user. Routing patterns must contain only trunk

groups that actually terminate to Avaya Communication Manager. Calls from one MMCX to another MMCX do not use AAR/ARS. Authorization codes are not supported.

- Call Detail Recording — Using the MASI link, Avaya Communication Manager is able to track call detail information for calls made using MMCX terminals and interfaces. CDR records all calls originating from or terminating at a MASI terminal. MASI CDR does not record ineffective call attempts when all MASI paths are busy.

The Resource Flag value of 8 indicates a MASI call. This field appears in unformatted, int-isdn, expanded and customized CDR formats. For formats other than these, you can determine that a call involves a MASI terminal or trunk by the trunk access code (TAC), dialed number or calling number fields. The following are the CDR capabilities of MASI. Administration information is under the heading *How to administer MASI*.

- Incoming/Outgoing Trunk Call Splitting: Call splitting does not produce separate records for MMCX calls that are transferred or conferenced.
  - intra-switch CDR: You can administer intra-switch CDR to monitor MASI terminals. To do this, simply add the MASI terminal extension on the Intra-switch CDR screen. Avaya Communication Manager then monitors calls from MASI terminals to other MASI terminals, and calls between MASI terminals and Communication Manager stations.
  - CDR Privacy: You can administer a MASI terminal for CDR Privacy.
  - Account Code Dialing and Forced Entry of Account Codes: This is not supported for MASI terminals. Therefore, make sure the COR you assign does not force entry of account codes.
  - Trunk CDR: You can get call detail records for all incoming and outgoing calls made over MMCX interfaces.
- Call redirection / Voice-messaging access — MMCX users can enter an Avaya Communication Manager extension, including an AUDIX hunt group, Callmaster agent, attendant console or telephone as their coverage point. If AUDIX is established as the MASI terminal's coverage point, the MASI terminal receives message waiting indication, and dials the AUDIX hunt group extension to retrieve messages. Once connected to AUDIX, operation for the MMCX user is the same as for a Communication Manager station user, including use of # to identify the extension, if desired.

 **Note:**

It is not possible to determine the call coverage status of a MASI terminal.

Avaya Communication Manager tracks calls to MASI terminals that follow the autonomous coverage path from the MASI terminal. MMCX calls redirected to Communication Manager stations contain display information

MASI terminals that dial AUDIX directly, or that place calls to MASI terminals that cover to AUDIX, do not receive ringback if all AUDIX ports are busy. Instead, these callers see a message the called party is busy, and the call drops.

- Transfer — MASI terminals cannot transfer calls to Communication Manager stations, and cannot transfer a call to another MASI terminal if the call involves a Communication Manager station.

- Conferencing — Conferences can involve both MASI terminals and Avaya Communication Manager stations, and either one can initiate the conference. Communication Manager stations participate in such conferences in voice-only mode. If an MMCX user initiates a conference that involves Communication Manager stations, the conference will drop when the initiator drops from the call. If a Communication Manager station initiates the conference, that station can drop without affecting the other conferees.
- Status tracking - terminals and trunks — Avaya Communication Manager tracks the active/idle status of all MASI terminals, and monitors traffic over MMCX interfaces.
- Trunk groups — For MASI purposes, there are two kinds of trunk groups: the ISDN-PRI trunk groups that serve as paths for establishing calls between Avaya Communication Manager stations or trunks and MASI terminals or interfaces, and the remote trunks that are interfaces from the MMCX to other entities. Each MASI remote trunk group appears to Communication Manager as a single unit, with no concept of members within the group.



**Note:**

You cannot test, busy out, or release MASI remote trunk groups, since you cannot dial a MASI remote trunk TAC from the Avaya DEFINITY Server. The TAC merely identifies the trunk to Avaya Communication Manager for purposes of status and CDR records.

You cannot administer MASI trunks as part of Communication Manager route patterns.

**Related topics:**

[Multimedia Applications Server Interface Administration](#) on page 348

**Unsupported Communication Manager features**

We can generalize feature interactions to some extent. For example, since there are no buttons available to a MASI terminal, any feature that requires a button is also not available. MASI cannot support features that require the user to dial a trunk access code for a MASI remote trunk, or a feature access code other than AAR/ARS. The MMCX dial plan can contain only those feature access codes that are supported



**Caution:**

DO NOT ADMINISTER the following features! The following features are not supported for use over the MASI link, and Avaya cannot be responsible for the results if you attempt to administer them.

**Unsupported Call Center features**

- ASAI — You must not administer a MASI terminal in an ASAI domain. MASI terminals and MMCX trunks are not monitored by ASAI. It might be possible for a MASI terminal to place a call to a Communication Manager station that is part of an ASAI domain. ASAI will not be blocked from controlling this call, but there can be unpredictable results. The same is true for calls originating from an ASAI domain terminating at MASI terminals, and for ASAI-monitored hunt groups that contain MASI terminals.
- Automatic Call Distribution — You must not include a MASI terminal extension as part of an ACD hunt group. You must not mix MASI administration with anything related to ACD, including Outbound Call Management and PASTE.
- Call Vectoring — You must not include MASI terminal extensions in any step of a vector.

## Unsupported Basic features

- Bridged Call Appearances — You must not administer a bridged appearance that involves a MASI terminal
- Call Coverage — You must not administer a MASI terminal in the coverage path of an Avaya Communication Manager station
- Call Forwarding — You must not forward a Communication Manager station to a MASI terminal
- Call Pickup — You must not administer a MASI terminal as part of a pickup group
- Intercom — You must not administer MASI terminals as members of any type of intercom group.
- Manual Message Waiting — You must not administer a manual message waiting button (man-msg-wt) with a MASI terminal as the referenced extension
- Manual Signaling — You must not administer a manual signaling button (signal) with a MASI terminal as the referenced extension.
- Night Service — You must not administer a MASI terminal as a night service destination
- Pull transfer — MASI terminals cannot perform a pull transfer operation. You must not administer this feature on an Avaya DEFINITY Server where MASI is active. This applies only in Italy.
- Station Hunting — You must not administer a MASI terminal as part of a station hunting path.
- Terminating Extension Groups — You must not administer a MASI terminal as part of a TEG.

## Constraints with other Communication Manager Features

The following section describes feature behaviors that might not be as expected, but that are not likely to be destructive.

### Attendant Features

| Features                             | Constraints   |
|--------------------------------------|---|
| Dial Access to the Attendant         | MASI terminals will be able to dial the attendant access code, if it is administered in the MMCX dial plan.   |
| Attendant Direct Extension Selection | Attendants are able to access MASI terminals via DXS buttons and busy lamp indicates status of the MASI terminal.   |
| Emergency Access to the Attendant    | MASI terminals have emergency access using the attendant access code, if it is administered in the MMCX dial plan. However, off-hook alerting is not administrable. |
| Attendant Intrusion                  | Attendants are able to activate intrusion towards MASI terminals.   |
| Attendant Override                   | Attendants are not able to activate override towards MASI terminals..   |

| <b>Features</b>                                | <b>Constraints</b>  |
|--|---|
| Attendant Recall                               | MASI terminals cannot activate attendant recall.  |
| Attendant Remote Trunk Group Select            | Attendants cannot use this feature to select MASI remote trunks   |
| Attendant Return Call                          | Operates normally if a MASI terminal is the called party.   |
| Attendant Serial Call                          | Serial calls are denied if the calling party is an MMCX interface.  |
| Attendant Straightforward Outward Completion   | The attendant is able to complete calls to Communication Manager trunks for MASI terminals.   |
| Attendant Through Dialing                      | The attendant can use Through Dialing to pass dial tone to MASI terminals.  |
| Attendant Timers                               | Attendant timers work the same no matter what kind of terminal is involved..  |
| Attendant Trunk Group Busy/ Warning Indicators | You cannot administer Busy/Warning indicators for MASI trunks because they are not standard Avaya Communication Manager trunks. However, you can administer these indicators for the trunk group administered for MASI paths. |
| Attendant Trunk Identification                 | The attendant is not able to identify the trunk name via button pushes.   |

Basic features

| <b>Features</b>                           | <b>Constraints</b>  |
|---|---|
| Abbreviated Dialing                       | A Communication Manager station can enter an MMCX extension in an AD list. However, MASI terminals cannot use AD.         |
| Administered Connections                  | MASI terminals must not be the originator nor the destination of an administered connection.                              |
| Automatic Callback                        | Automatic callback does not work towards a MASI terminal.   |
| Automatic Circuit Assurance               | You must not administer a MASI terminal as an ACA referral destination. You cannot administer ACA for MASI remote trunks. |
| Busy Verification of Terminals and Trunks | You cannot use Busy Verification for MASI terminals or remote trunks.   |
| Call Detail Recording                     | CDR Account Code Dialing and Forced Entry of Account Codes are not supported for MASI terminals.                          |

| <b>Features</b>          | <b>Constraints</b>  |
|--------------------------|---|
| Call Park                | The attendant can park calls at the extension of a MASI terminal, but users can only retrieve these calls from a Communication Manager station, since MASI terminals cannot dial the Answer Back FAC.   |
| Data Call Setup          | Avaya Communication Manager users cannot place data calls to MASI terminals.  |
| Facility Busy Indication | You can use FBI to track the status of MASI terminals. The FBI button and indicator lamp must be on a Communication Manager station. You cannot use FBI to track MMCX interfaces.                       |
| Facility Test Calls      | Avaya Communication Manager users cannot make test calls to MMCX interfaces.  |
| Go to Cover              | MASI terminals cannot activate this feature.  |
| Leave Word Calling       | The only valid LWC destination for a MASI terminal is AUDIX. You cannot administer SPE-based LWC. MASI terminals cannot send LWC messages to Avaya Communication Manager stations or to MASI terminals. |
| Loudspeaker paging       | You can administer a MASI terminal as a code calling extension.   |
| Malicious Call Trace     | MASI terminals cannot initiate malicious call trace.  |
| Message Retrieval        | MMCX users can only retrieve messages through AUDIX messaging.  |
| Music on Hold            | Music on hold will only be available if an Communication Manager station has placed the call on hold.   |
| Override                 | Executive override does not work towards MASI terminals.  |
| Priority Calling         | Priority calling is not supported for calls to or from MASI terminals.  |
| Ringback Queueing        | Ringback Queueing is not supported for MASI terminals.  |
| Send All Calls           | MMCX has an autonomous SAC function   |
| Tenant Partitioning      | All MASI terminals exist in tenant 1, and you cannot change the tenant number.  |
| Time of Day coverage     | As with all coverage, Communication Manager does not control coverage of the MASI terminal.   |
| Transfer out of AUDIX    | A MASI terminal cannot use *T to transfer from AUDIX to another MASI terminal.  |

### Hospitality Features

| <b>Features</b> | <b>Constraints</b>                             |
|-----------------|--|
| Do Not Disturb  | MASI terminals cannot activate Do Not Disturb. |

Multimedia Features

| Features                 | Constraints   |
|--------------------------|---|
| Multimedia Call Handling | Avaya MMCH users are not able to make H.320 calls to MASI terminals over the MASI link. Calls between MMCX terminals and MMCH terminals are voice only. |

**Troubleshooting**

Verify proper operation using the following commands and follow normal escalation procedures to resolve any failures detected by the demand test.

- 
1. Verify the DS1 trunk using the `test board <board location> long` command
  2. Verify the ISDN Signaling Group using the `test signaling-group <group number>` command.
  3. Also verify proper administration.
  4. Verify the temporary signaling connection using the `test tsc-administered <group number>` command
  5. Also verify proper administration.
- 

**Common Error Conditions**

=

| Error condition   | Resolution   |
|---|--|
| If the cable from an Avaya DEFINITY Server to the MMCX becomes disconnected | You should see alarms raised against ISDN-SGRP and UDS1-BD. In particular, you should observe ISDN-SGRP errors such as 769, 1793, and 257. To resolve, reconnect the cable and follow normal test procedures.  |
| If the far-end path termination number is incorrect                         | You should observe MASI-PTH error 513. To resolve, correct administration using the MASI Path Parameters screen.   |
| If the Layer 3 TSC is not administered properly or is out of service        | You should observe errors (but no alarms) raised against TSC-ADM. Verify the signaling group administration and follow normal escalation procedures for TSC-ADM.   |
| If the TSC fails to come up even through Layer 2                            | you can run <code>test tsc-administered &lt;group number&gt;</code> to force a server heartbeat test, or simply wait 5 to 10 minutes for the link to recover. This situation might occur if the server running |

| Error condition                      | Resolution   |
|--------------------------------------|--|
| Signaling Group and below pass tests | Communication Manager is rebooted or if the MASI interface is administered before the MMCX is properly administered. |
| if features are not working.         | You might want to use the <code>busy port</code> and <code>release port</code> commands to unlock things             |

## Video Telephony Solution

Use the Avaya Video Telephony Solution (AVTS) to enable videoconferencing for your desktop and group video communications.

### Note:

AVTS is Avaya's newest, and currently available H.323 video solution. Some older systems may still use the older technology H.320 video solution, Multi-Media Call Handling (MMCH). For more information on MMCH, see *Multimedia Call Handling*.

The Avaya Video Telephony Solution enables Avaya Communication Manager to merge a set of enterprise features with Polycom's videoconferencing adjuncts. It unifies Voice over IP with video, web applications, Avaya's video enabled IP softphone, third party gatekeepers and other H.323 endpoints.

The following components are part of the Avaya Video Telephony Solution feature:

- Polycom VSX3000, VSX7000 and VSX8000 conferencing systems with Release 8.03 or later
- Polycom V500 video calling systems
- Polycom MGC video conferencing bridge platforms with Release 8.0.1. Release 7.5 of the MGC is not supported.
- Third party gatekeepers, including Polycom Path Navigator

You also need a system running Avaya Communication Manager Release 3.0.1, and Avaya IP Softphone release 5.2 with video integrator.

Starting with Communication Manager Release 3.1.2, you can use cumulative bandwidth management to set video bandwidth for the Avaya Video Telephony Solution. The Audio Call Admission Control (CAC) capability allows you to set maximum bandwidth between multiple network regions for audio calls. Video bandwidth can also be controlled in a similar way.

For more information, see also:

- *Avaya Video Telephony Solution Release 3.0 Networking Guide, 16-601423, Issue 1*
- *Video Telephony Solution Release 3.0 Quick Setup, 16-300310, Issue 3*
- *IP Softphone and Video Integrator Getting Started, 16-600748, Issue 2*

 **Note:**

To configure the Polycom MGC-25 Video Conferencing Bridge Platforms with Avaya S8300D and S8510 Servers, see the procedures stated in the *Video Telephone Solution R3.0 Quick Set Up Guide, 16-300310, Issue 3, February 2007*

**Related topics:**

[Multimedia Call Handling](#) on page 375

## Communication Manager SIP Video Infrastructure Enhancements

 **Note:**

Communication Manager 6.0 as a SIP feature server implies that Communication Manager is configured with IMS enabled SIP signaling interfaces that are connected to the Session Manager 6.0. The H.323 calls are not routed via the feature server and therefore, only SIP requirements impact feature server operation. From Release 6.0 Communication Manager is supported as an Access Element as well.

- Communication Manager 6.0 supports SIP video and audio shuffling optimization.
- Communication Manager reduces the total memory footprint of each SIP call leg that has video enabled by no longer storing a duplicate copy of far-end caps in the SIP user manager.
- Communication Manager does not allocate video structures internally when only audio media is present in the SDP for the initial dialog.
- Communication Manager indicates when the called party is a video enabled endpoint and hence allows video to be added when a called party is transferred or conferenced via sending a re-INVITE (no SDP) to trigger renegotiation of capabilities by both endpoints in the new call topology.
- Communication Manager has its capacity for SIP video calls set to 1/3 of the capacity for all SIP calls. This is the equivalent ratio of audio/video users with the current H.323 solution. This change ensures that SIP video capacity increases along with SIP audio capacity in a defined manner and as the work to increase audio calls is completed, additional video calls are supported.
- Communication Manager initiates video OLCs to H.323 MCUs on behalf of SIP endpoints.
- All existing Communication Manager H.323 functionality and compatibility with both Polycom and Meeting Exchange must be maintained. Versions of Polycom firmware as tested for CM 5.2 need to be verified against the Communication Manager 6.0 . The existing H.323 functionality also need to be verified against new One X Communicator 6.0 and Meeting Exchange firmwares.
- Communication Manager as a feature server supports negotiation between endpoints of a video fast-update mechanism using RTCP feedback as specified in RFC4585 and RFC5104.
- Communication Manager as a feature server supports negotiation between endpoints of a video flow-control (Temporary Maximum Media Bitrate Request) mechanism using RTCP feedback as specified in RFC4585 and RFC5104.

- Communication Manager implements simplified SIP call flows by removing the need to “black hole” video media in the initial SIP INVITE when direct media is enabled.
- Communication Manager as a feature server passes through any media sessions which it does not explicitly handle to tandem dialogs.

## Administering the Avaya Video Telephony Solution

### Prerequisites

You must complete the following actions before you can administer the Avaya Video Telephony Solution:

1. Type `display system-parameters customer-options` to view the System Parameters Customer-Options (Optional Features) screen. Page down till you see the Maximum Video Capable Stations field and the **Maximum Video Capable IP Softphones** field. These two fields show up only if your system is licensed for the Avaya Video Telephony feature. Your Avaya license file must contain the RTUs that were purchased for **Maximum Video Capable Stations** field and the **Maximum Video Capable IP Softphones** fields



#### Note:

You must make sure that the value of the Maximum Video Capable Stations field allows for each station that you use. In addition, each single-point VSX system is considered to be one station, and each multipoint VSX system is considered to be three stations.

2. Type `change ip-network-region #` to view the IP Network Region screen. The following fields must be set to `y` on this screen:

- **Intra-region IP-IP Direct Audio**
- **Inter-region IP-IP Direct Audio**
- **IP Audio Hairpinning**

The following steps are part of the administration for the Avaya Video Telephony Solution:

- Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems
- Configuring Polycom PathNavigator Gatekeepers
- Configuring video trunks between two Communication Manager systems
- Configuring the Maximum Bandwidth for Inter-Network Regions
- Checking bandwidth usage
- Administering Ad-hoc Video Conferencing

### Related topics:

[Configuring Video-Enabled Avaya IP Softphone Endpoints](#) on page 366

[Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems](#) on page 367

[Configuring Polycom PathNavigator Gatekeepers](#) on page 370

[Configuring video trunks between two Communication Manager systems](#) on page 371

[Configuring the Maximum Bandwidth for Inter-Network Regions](#) on page 373

[Checking bandwidth usage](#) on page 374

## Configuring Video-Enabled Avaya IP Softphone Endpoints

---

1. Type the `display system-parameters customer-options` command and verify number on the **Maximum Video Capable IP Softphones**. This number is provided by the Communication Manager license file.
  2. Type `change ip-codec-set x` command (where x is the chosen IP codec set) to set the following parameters:
    - a. Allow **Direct-IP Multimedia** to `y`.
    - b. **Maximum Call Rate for Direct-IP Multimedia** - the Call Rate is the combined audio and video transmit rate or receive rate. You can use this setting to limit the amount of bandwidth used for calls.  
If you select 768 Kbits, a maximum of 768 Kbits will be used to transmit and to receive audio and video.
    - c. **Maximum Call Rate for Priority Direct-IP Multimedia** allows you to set the maximum call rate per call for priority users
    - d. Repeat this step for each IP codec set that will be used for video.
  3. Type `change cos` and scroll down till you find the **Priority IP Video** field. This must be set to `y` for each class of station that is given a Priority status.
  4. Type `change ip-network-region x` command (where x is the chosen IP network region) to set the following parameters:
    - a. **Intra-region IP-IP Direct Audio** to `yes`.
    - b. **Inter-region IP-IP Direct Audio** to `yes`.
    - c. **Security Procedures 1** to `any-auth`
    - d. Repeat this step for each IP network region that will be used for video.
  5. Type `add station` command to add an Avaya IP Softphone station, and set the following parameters for that station
    - a. **IP Softphone** to `y`.
    - b. **IP Video Softphone** to `y`.
    - c. **IP Audio Hairpinning** to `y`.
    - d. Repeat Step 5 for each video-enabled Avaya IP Softphone endpoint you want to configure.
-

**Related topics:**

[Administering the Avaya Video Telephony Solution](#) on page 365

[Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems](#) on page 367

[Configuring Polycom PathNavigator Gatekeepers](#) on page 370

[Configuring video trunks between two Communication Manager systems](#) on page 371

[Configuring the Maximum Bandwidth for Inter-Network Regions](#) on page 373

[Checking bandwidth usage](#) on page 374

## Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems

### Prerequisites

You must know the following information:

- Maximum number of VSX and V500 systems on your network
- PIN for each VSX/V500 system. The default is the unit's serial number
- Polycom software key for each system
- Avaya option key for each system
- Whether the VSX system has the multipoint option or IMCU option
- IP address of the voice system

- 
1. Use the `display system-parameters customer-options` command to verify the **Maximum Video Capable Stations**.

This number is provided by the Communication Manager license file. The **Maximum Video Capable Stations** is determined by using the following criteria

- Each V500 system is considered to be one station
  - Each single-point VSX system is considered to be one station
  - Each VSX multipoint system is considered to be three stations
2. Use the `change ip-codec-set x` command (where x is the chosen IP codec set) to define the following wideband codecs
    - SIREN14-S96K (1 fpp, 20 ms)
    - G722.1-32K (1 fpp, 20 ms)
    - G.726A-32K (no silence suppression, 2 fpp, 20 ms)
    - G.711MU (no silence suppression, 2 fpp, 20 ms)
    - G.729A (no silence suppression, 2 fpp, 20 ms)
    - Set **Allow Direct-IP Multimedia** to `y`
    - Set **Maximum Call Rate for Direct-IP Multimedia** - the Call Rate is the combined audio and video transmit rate or receive rate. You can use this setting to limit the amount of bandwidth used for calls. For example, if you

select 768 Kbits, a maximum of 768 Kbits will be used to transmit and receive audio and video. Repeat this step for each IP codec set that will be used for video.

- **Maximum Call Rate for Priority Direct-IP Multimedia** allows you to set the maximum call rate per call for priority users

3. Use the `change ip-network-region x` command (where x is the chosen IP network region) to set the following parameters:
  - **Intra-region IP-IP Direct Audio** to `yes`
  - **Inter-region IP-IP Direct Audio** to `yes`
  - **Security Procedures 1** to `any-auth`
  - Repeat this step for each IP network region that will be used for video.
4. Use the `add station` command to add a station for the Polycom system to set the following parameters
  - **Type** to `H.323`
  - **Security Code** to the `pin` on the VSX or V500 system
  - **IP Video** to `y`
  - **IP Audio Hairpinning** to `y`.
5. If the VSX system has the multipoint option or IMCU option, perform the following steps:
  - a. Use the **add station** command to add a second station for the Polycom system.
  - b. Set **Type** to `H.323`.
  - c. Set **Security Code** to the `pin` on the VSX.  
Make sure the security code is the same as the previous station. All three stations must have the same security code.
  - d. Set **IP Video** to `y`.
  - e. Repeat Steps a through e to create the third consecutive station
  - f. Use the `change station xx` command (where xx is the first station you added for the Polycom system) to set Hunt-to Station to the second station you added for the Polycom system.
  - g. Use the `change station xx` command (where xx is the second station you added for the Polycom system) to set Hunt-to Station to the third station you added for the Polycom system.
  - h. Use the `change station xx` command (where xx is the third station you added for the Polycom system) to set Hunt-to Station to the first station you added for the Polycom system. All three stations must be in a circular hunt.
6. Install the Polycom system and connect it to your network.

7. Upgrade the Polycom system software.
8. Using a web browser, access the Polycom home page for the unit, and select **Admin Settings>Network>IP Network**.
9. Select the **Enable IP H.323** check box.
10. Select the **Display H.323 Extension** check box.
11. In the **H.323 Extension (E.164)** box, enter the station number you specified for this system on the Avaya Communication Manager system.
12. From the **Use Gatekeeper** box, select *Specify with PIN*.
13. In the **Gatekeeper IP Address** box, enter the IP address of the CLAN or PCLAN followed by `:1719` to specify the correct port that must be used.
14. In the **Authentication PIN** box, enter the security code you entered in Step 3.
15. In the **Number** box in the Gateway area, enter the extension you specified in Step 9.
16. In the **Type of Service** box in the Quality of Section area, select *IP Precedence*.
17. In the **Type of Service Value** boxes (Video, Audio, and Far End Camera Control), enter the QoS values for the IP Network Region settings in which the VSX station belongs.
18. Select the **Enabled PVEC** check box.
19. Select the **Enable RSVP** check box.
20. Select the **Dynamic Bandwidth** check box.
21. From the **Maximum Transmit Bandwidth** box, select the setting that matches the **Maximum Call Rate for Direct-IP Multimedia** setting you specified for the Avaya Communication Manager system.
22. From the **Maximum Receive Bandwidth** box, select the setting that matches the **Maximum Call Rate for Direct-IP Multimedia** setting you specified for the Avaya Communication Manager system.
23. Complete the **Firewall** and **Streaming** sections as necessary.
24. When finished, click the **Update** button.
25. Repeat the steps for each Polycom system.

---

**Related topics:**

[Administering the Avaya Video Telephony Solution](#) on page 365

[Configuring Video-Enabled Avaya IP Softphone Endpoints](#) on page 366

[Configuring Polycom PathNavigator Gatekeepers](#) on page 370

[Configuring video trunks between two Communication Manager systems](#) on page 371

[Configuring the Maximum Bandwidth for Inter-Network Regions](#) on page 373

[Checking bandwidth usage](#) on page 374

## Configuring Polycom PathNavigator Gatekeepers

---

1. Use the `change ip-codec-set 1` command to set the following parameters.
    - Allow **Direct-IP Multimedia** to `y` (page 2 of screen).
    - **Maximum Call Rate for Direct-IP Multimedia**. This setting is the combined audio and video transmit rate or receive rate for non-priority (normal) video calls. You can use this setting to limit the amount of bandwidth used for normal video calls. For example, if you select 384 Kbits, a maximum of 384 Kbits will be used to transmit and to receive audio/ video.
    - **Maximum Call Rate for Priority Direct-IP Multimedia**. This setting is the combined audio and video transmit rate or receive rate for priority video calls. You can use this setting to limit the amount of bandwidth used for priority video calls. For example, if you select 384 Kbits, a maximum of 384 Kbits will be used to transmit and to receive audio/ video.
  2. Use the `change ip-network-region x` command (where `x` is the chosen IP network region) to set the following parameters:
    - **Intra-region IP-IP Direct Audio** to `no`
    - **Inter-region IP-IP Direct Audio** to `no`
    - **Security Procedures 1** to `any-auth` (page 2 of screen).
    - **Video Norm** (page 3 of screen) to the amount of bandwidth that you want to allocate for the normal video pool to each IP network region.
    - **Video Prio** (page 3 of screen) to the amount of bandwidth that you want to allocate for the priority video pool to each IP network region.
    - **Video Shr** (page 3 of screen). Specify whether the normal video pool can be shared for each link between IP network regions.
-  **Note:**  
If one of the video bandwidth limits is in Kbits, and another video bandwidth limit is in Mbits, all of the video bandwidth limits will be converted to the same unit (that is, Kbits or Mbits).
3. Use the `change node-names ip` command to add an entry for the Polycom PathNavigator gatekeeper. Be sure to enter the IP address of the IP board for the gatekeeper.
  4. Use the `add signaling-group` command to add a signaling group for the gatekeeper. Set the following parameters:
    - **Group Type** to `h.323`
    - **IP Video** to `y`

- **Near-end Listen Port** to 1719.
  - **LRQ Required** to *y*.
  - **Incoming Priority Video**. If you want all incoming calls to receive priority video transmissions, select *y*.
  - **Far-end Node Name** to the name you entered for the gatekeeper in Step 3.
  - **Far-end Listen Port** to 1719.
  - **Far-end Network Region** to the IP network region you specified in Step 2.
  - **Direct IP-IP Audio Connections** to *y*.
  - **IP Audio Hairpinning** to *y*.
5. Use the add trunk-group command to add a trunk group for the gatekeeper. Set the following parameters:
    - **Group Type** to *isdn*.
    - **Carrier Medium** to *H.323*.
    - Add members to this trunk group.
  6. Use the `change signaling-group xx` command (where *xx* is the signaling group you added in Step 4) to set **Trunk Group** for **Channel Selection** to the trunk group you added in Step 5.
  7. Create a route pattern to the gatekeeper.
  8. Configure the gatekeeper.

---

#### Related topics:

- [Administering the Avaya Video Telephony Solution](#) on page 365
- [Configuring Video-Enabled Avaya IP Softphone Endpoints](#) on page 366
- [Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems](#) on page 367
- [Configuring video trunks between two Communication Manager systems](#) on page 371
- [Configuring the Maximum Bandwidth for Inter-Network Regions](#) on page 373
- [Checking bandwidth usage](#) on page 374

### Configuring video trunks between two Communication Manager systems

---

1. Use the `change ip-codec-set 1` command to set the following parameters.
  - a. Set **Allow Direct-IP Multimedia** to *y* (page 2 of screen).
  - b. Set **Maximum Call Rate for Direct-IP Multimedia** - the Call Rate is the combined audio and video transmit rate or receive rate.  
You can use this setting to limit the amount of bandwidth used for calls

- c. **Maximum Call Rate for Priority Direct-IP Multimedia** allows you to set the maximum call rate per call for priority users
  2. Type `display route-pattern xxx`, where xxx is the number for the route pattern  
To enable multimedia, the **M** field under BCC value must be set to y. This will allow you to send multimedia calls over a specific trunk.  
It is possible to have video over trunks that do not have M field set for the BCC. Setting **M** on the BCC enables you to select the route that the route pattern that you should use.
  3. Use the `change node-names ip` command to add an entry for the trunk.  
Be sure to enter the IP address of the CLAN or PCLAN of the other Communication Manager system
  4. Use the `add signaling-group` command to add a signaling group for the video trunk. Set the following parameters:
    - **Group Type** to `h.323` or `sip`
    - **Priority Video** to `y`
    - **IP Video** to `y`.
    - **Near-end Listen Port** .
    - **LRQ Required** to `y`.
    - **Far-end Node Name**
    - **Far-end Listen Port**
    - **Far-end Network Region**
    - **Calls Share IP Signaling Connection** to `n`.
    - **Direct IP-IP Audio Connections** to `y`.
    - **IP Audio Hairpinning** to `y`.
  5. Use the `add trunk-group` command to add a trunk group for the video trunk. Set the following parameters
    - **Group Type** to `isdn`.
    - **Carrier Medium** to `H.323`.
    - Add members to this trunk group.
  6. Use the `change signaling-group xx` command (where xx is the signaling group you added in Step 3) to set **Trunk Group** for Channel Selection to the trunk group you added in Step 4.
  7. Create a route pattern for the trunk group.
-

**Related topics:**

- [Administering the Avaya Video Telephony Solution](#) on page 365
- [Configuring Video-Enabled Avaya IP Softphone Endpoints](#) on page 366
- [Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems](#) on page 367
- [Configuring Polycom PathNavigator Gatekeepers](#) on page 370
- [Configuring the Maximum Bandwidth for Inter-Network Regions](#) on page 373
- [Checking bandwidth usage](#) on page 374

**Configuring the Maximum Bandwidth for Inter-Network Regions**

- 
1. Type `change ip-network region 1`.  
The system displays the IP Network Region screen
  2. Page down till you see the page titled Inter Network Region Connection Management.
  3. In the column named **Total**, you can specify the bandwidth across the network regions. In the column named **Video**, you specify how much of the total bandwidth is to be used by video calls. The following are the available options:
    - a. To support audio only and no video, set the **Video** field to 0 and audio to a very high number.
    - b. To support audio and video with no bandwidth management, set both the **Total** and **Video** fields to `No Limit`.
    - c. To restrict audio bandwidth, and allow unlimited video bandwidth, set the **Total** field to the desired bandwidth. Set the **Video** field to `No Limit`.
    - d. To control both audio and video bandwidth, set the **Total** field to the total bandwidth available between network regions. Set the **Video** field to the maximum bandwidth that can be used by video.  
The **Video** field must be set to a value less than or equal to the **Total**
    - e. Set priority video to the maximum bandwidth that can be used exclusively by priority video users.
- 

**Related topics:**

- [Administering the Avaya Video Telephony Solution](#) on page 365
- [Configuring Video-Enabled Avaya IP Softphone Endpoints](#) on page 366
- [Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems](#) on page 367
- [Configuring Polycom PathNavigator Gatekeepers](#) on page 370
- [Configuring video trunks between two Communication Manager systems](#) on page 371
- [Checking bandwidth usage](#) on page 374

## Checking bandwidth usage

---

Type `status ip-network-region`.

The system displays the Inter Network Region Bandwidth Status screen for a call that is up.

You can view the audio bandwidth usage on the first row.

You can view the normal video bandwidth usage on the second row.

You can view the priority video bandwidth usage on the third row.

---

### Related topics:

[Administering the Avaya Video Telephony Solution](#) on page 365

[Configuring Video-Enabled Avaya IP Softphone Endpoints](#) on page 366

[Configuring the Polycom VSX Video Conferencing Systems and V500 Video Calling Systems](#) on page 367

[Configuring Polycom PathNavigator Gatekeepers](#) on page 370

[Configuring video trunks between two Communication Manager systems](#) on page 371

[Configuring the Maximum Bandwidth for Inter-Network Regions](#) on page 373

## Administering Ad-hoc Video Conferencing

Administer the Ad-hoc Video Conferencing feature to allow users to create video conference calls. From a two-party video call, a user can press the **Conference** button on their telephone, dial the number of a third party, and press **Conference** again to add the party to the video conference call. Additional parties, up to a maximum of six, can be added in the same way. If the originator or any party who joins the conference call has administered COS permissions for Ad-hoc Video Conferencing, the video feature is enabled for the call. The call is moved from a Communication Manager hosted audio-only conference to an external bridge multimedia conference

- 
1. On page 2 of the *System Parameters Customer-Options (Optional Features)* screen, ensure that the **Maximum Administered Ad-hoc Video Conferencing Ports** field is set to the number of ports available for Ad-hoc Video Conferencing.
  2. On the *Class of Service* screen, ensure that Ad-hoc Video Conferencing is set to `y` for each class of user with Ad-hoc Video Conferencing privileges. Then assign the COS on the Station screen for the appropriate users.
  3. On the *Video Bridge* screen, configure video bridges for Ad-hoc Video Conferencing. For more detailed information on Ad-hoc Video Conferencing, see *Avaya Video Telephony Solution Networking Guide, 16-601423*.
-

## Multimedia Call Handling

Multimedia Call Handling (MMCH) enables users to control voice, video, and data transmissions using a telephone and PC. Users can conduct video conferences and route calls like a standard voice call. They can also share PC applications to collaborate with others working from remote sites

 **Note:**

MMCH is Avaya's older technology H.320 video solution. Avaya Video Telephony Solution is Avaya's newer, and preferred H.323 video solution. For more information on AVTS, see *Avaya Video Telephony Solution*.

 **Note:**

There are two distinct levels of functionality: Basic and Enhanced. The Basic mode of operation treats a standard-protocol H.320 multimedia call as a data call. If the call is redirected, it is converted to a voice call. As a voice call, certain features are enabled, such as coverage, voice mail, and multiparty video conferencing.

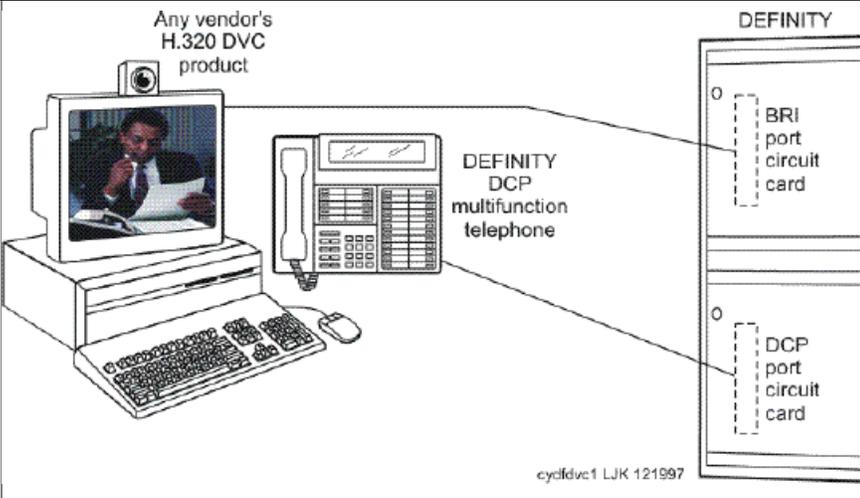
The Enhanced mode of operation allows a multifunction telephone to control a multimedia call as if it were a standard voice call. Spontaneous video conferencing, call forwarding, coverage, hold, transfer and park, along with many routing features, are available to multimedia calls. Both modes of operation allow data collaboration between multiple parties using the T.120 standard protocol.

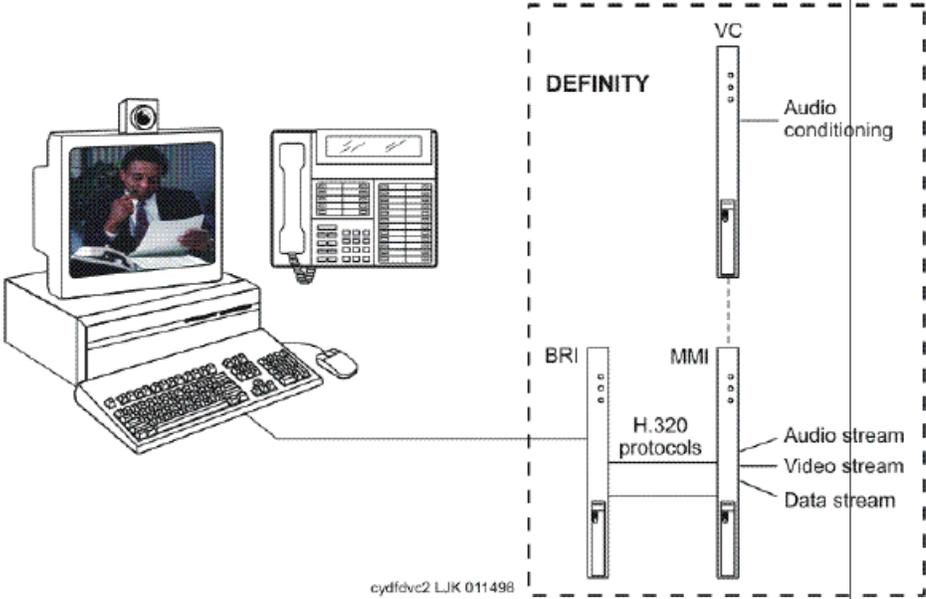
**Related topics:**

[Video Telephony Solution](#) on page 363

**Definitions: MMCH features and components**

| Features        | Meanings   |
|-----------------|--|
| Multimedia call | <p>A multimedia call, for MMCH, is one that conforms to the H.320 and T.120 suite of protocol standards. These standards allow video-conferencing packages from different vendors to communicate with one another. The capabilities of the individual multimedia-endpoint package can vary, however.</p> <ul style="list-style-type: none"> <li>• An H.320 call can contain voice, video and data.</li> <li>• The bandwidth for MMCH calls is limited to 2 B-channels</li> </ul> |

| Features                           | Meanings  |
|------------------------------------|---|
|                                    |  <p>The diagram illustrates a multimedia endpoint setup. On the left, a PC is equipped with a camera and a microphone, labeled as 'Any vendor's H.320 DVC product'. This PC is connected to a 'DEFINITY DCP multifunction telephone'. The telephone is further connected to a 'DEFINITY' rack, which contains two types of circuit cards: a 'BRI port circuit card' and a 'DCP port circuit card'. The rack is labeled 'DEFINITY' at the top. A small reference code 'cylfidvc1 LJK 121997' is located at the bottom right of the diagram area.</p> |
| <p>Basic multimedia complex</p>    | <p>A Basic multimedia complex consists of a BRI-connected multimedia-equipped PC and a non-BRI-connected multifunction telephone administered in Basic mode. With a Basic multimedia complex, users place voice calls at the multifunction telephone and multimedia calls from the multimedia equipped PC. Voice calls will be answered at the multifunction telephone and multimedia calls will alert first at the PC and, if unanswered, will next alert at the voice station. A Basic multimedia complex provides a loose integration of the voice station and H.320 DVC system.</p>   |
| <p>Enhanced multimedia complex</p> | <p>An Enhanced multimedia complex consists of a BRI-connected multimedia-equipped PC and a non-BRI-connected multifunction telephone administered in Enhanced mode. The Enhanced multimedia complex acts as though the PC were directly connected to the multifunction telephone. Thus, voice call control, multimedia call control and call status are enabled at the telephone. An Enhanced multimedia complex provides a tight integration of the voice station and H.320 DVC system.</p>  |
| <p>Multimedia endpoint</p>         | <p>The multimedia endpoint is a user's PC that has been equipped with an H.320 multimedia package. The PC is physically connected to Avaya Communication Manager with a BRI line.</p>   |

| Features                   | Meanings   |
|----------------------------|--|
|                            |  <p>The diagram illustrates the connection between a multimedia endpoint and a DEFINITY server. On the left, a PC with a camera and a telephone are shown. On the right, a DEFINITY server is depicted with several components: a VC (Video Conferencing) unit, an Audio conditioning unit, an H.320 protocols unit, a Video stream unit, a Data stream unit, and an MMI (Multimedia Interface) unit. A BRI (Basic Rate Interface) line is also shown. The server components are connected to the endpoint, and the H.320 protocols unit is connected to the Video stream and Data stream units. The VC unit is connected to the Audio conditioning unit. The MMI unit is connected to the H.320 protocols unit. The BRI line is connected to the DEFINITY server. The diagram is labeled 'cydfvvc2 LJK 011498'.</p> |
| Enhanced mode service link | <p>The service link is the combined hardware and software multimedia connection between the user's multimedia endpoint and the Avaya DEFINITY Server which terminates the H.320 protocol. The service link provides video, data, and, optionally, voice streams to augment the capabilities of the telephone and PC. A service link only applies to an Enhanced multimedia complex, never to a Basic multimedia complex. The service link is administered on the Station screen and can be either permanent or as-needed.</p>  |

### Basic Mode Operation

MMCH's two levels of functionality for a multimedia complex, Basic and Enhanced mode, are enabled either by administration on Communication Manager or by an mm-basic feature button or FAC.

- All voice-only calls originate at the voice station.
- All multimedia calls originate with the H.320 DVC system
- All incoming voice calls attempt to alert at the voice station and receive all standard voice call treatment.
- All incoming H.320 multimedia calls attempt to alert on the H.320 DVC system initially. If answered, a 2-way video call will result. The Basic multimedia complex voice station will not be involved in the call in any way.

If the H.320 multimedia call is not answered at the H.320 DVC system and the Basic multimedia complex voice station has the **H.320** field administered to  $y$ , the call will:

- Time out at the DVC system.
- Alert at the associated voice station set as a voice-only call.
- Receive all standard voice call treatment

- Call control depends on what type of call is being originated.
  - Video is received and controlled at the PC.
  - Voice is received and controlled at the telephone set.
- The voice station of a Basic multimedia complex must manually add their multimedia endpoint to a multimedia conference. There is limited support for multimedia feature interactions. A specific set of voice features work for multimedia calls.
- Service Links are not used by Basic mode complexes.
- A single number can be used to reach the Basic multimedia complex for voice or H.320 multimedia calls.

**Related topics:**

[MMCH Settings Administration](#) on page 383

**Enhanced Mode Operation**

The Enhanced multimedia complex provides a much more tightly coupled integration of the complex voice station and H.320 DVC system. In Enhanced Mode:

- Both multimedia and voice calls must originate at the telephone set.
- Voice and multimedia calls can be controlled at the telephone set.
- Conferencing is spontaneous and established just like a voice-only conference call.
- There is extensive support for multimedia feature interaction. Most voice features work the same for multimedia calls.
- Service Links can be either “permanent” or “as-needed”

**Related topics:**

[MMCH Settings Administration](#) on page 383

**Physical Installation**

The physical components necessary to utilize MMCH capabilities include:

- H.320 DVC systems that are BRI connected to the Avaya DEFINITY Server.
- Non-BRI multifunction telephones.
- Avaya TN787 MultiMedia Interface (MMI) and TN788 Voice Conditioner (VC) boards.
- A T.120 Extended Services Module (ESM) server (necessary only if you plan to do T.120 data collaboration). Connectivity of the ESM requires an additional TN787 along with a TN2207 DS1 circuit pack.

**Dual Port Desktop**

Both Basic and Enhanced multimedia complexes are dual-port desktops that consist of:

- A BRI-connected multimedia-equipped PC that supports the H.320 protocol.
- A non-BRI-connected multifunction telephone set.

The PC and the multifunction telephone are individually wired to the Avaya DEFINITY Server. These two pieces of equipment can be administratively associated to form a Basic or ENHANCED multimedia complex

MMCH works with any H.320 system that is fully H.320 compliant and operates at the 2B or 128K rate.

 **Note:**

If you intend to share applications among users or whiteboard capabilities, the endpoint software you choose must also support the T.120 protocol.

The following endpoint-software packages have been tested:

- PictureTel PCS 50 & PCS 100, Release 1.6T.
- Proshare 2.0a, 2.1.
- Zydacron Z250 Ver. 2.02, Z350 Ver. 1.2 (With Netmeeting 2.0).

### **MMI & VC hardware**

The MMCH feature requires the use of two additional circuit packs:

- Multi Media Interface (MMI) TN787J.
- Voice Conditioner (VC) TN788B.

The TN787 and TN788 are service circuit packs. The TN787 supports simultaneous operation of 16 2B H.320 calls. The TN788 supports the voice processing for 4 H.320 endpoints.

- These service circuit packs can be located in any Port Network.
- These packs do not require any translations as part of their implementation
- The MMI and VC circuit packs are resource circuit packs akin to the Tone Detector circuit packs.
- These circuit packs require no administration on Communication Manager and can be located in multiple port networks.

### **T.120 Data Collaboration Server**

The Extended Services Module (ESM) provides T.120 data collaboration capability on a MMCH multipoint H.320 video conference.

- Each person in the conference who wants to participate in the data collaboration session, must have a personal computer with an H.320 video application that supports the T.120 protocol.
- The Avaya DEFINITY Server must have an ESM installed.

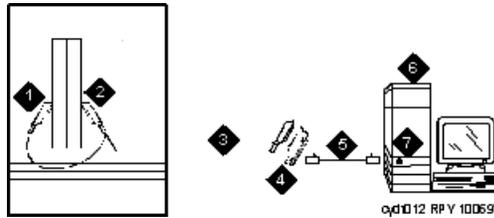
### **Installing ESM**

Use the following procedure and *Typical Multimedia Call handling ESM Connections* to connect to the ESM equipment:

1. Install the TN2207 primary rate interface (PRI) circuit pack and the TN787 multimedia interface (MMI) circuit pack in the port carrier of the server for Avaya Communication Manager.

 **Note:**

These two circuit packs should be co-located in the cabinet since they must be connected by a Y-cable on the back plane of the Avaya DEFINITY Server.



Typical Multimedia Call handling ESM Connections

- a. Port B Y-cable connector to a TN787 multimedia interface (MMI) circuit pack
  - b. Port A Y-cable connector to a TN2207 PRI circuit pack
  - c. 25-pair Y-cable
  - d. 356A adapter
  - e. D8W cord connected to 356A adapter S/B port 8
  - f. Extended services module (ESM)
  - g. Port B on compatible primary rate interface (PRI) card
2. Record the circuit pack locations.
  3. Connect the ESM Y-cable as shown.
  4. Administer the DS1 Circuit Pack screen and the Signaling Group screen for the ESM (see *ESM T.120 Server Administration*).
  5. Configure the ESM adjunct.

## Planning MMCH

### Prerequisites

Questions that help you use Avaya Communication Manager for multimedia

- How many MMCH users are you going to have?
- How many multimedia calls do you expect to have at any given time?

With the information above you can determine how many Voice Conditioner (VC) and Multimedia Interface (MMI) circuit packs you need.

- Will users need data collaboration capabilities? If so, you need to install the Extended Services Module (ESM).
- Which stations, hunt groups or vectors need early answer?
- Do you have ISDN-PRI trunks? It is possible to use separate DS1 trunks for data, but ISDN-PRI trunks are recommended.

- 
1. Purchase MMCH right-to-use.
  2. Avaya — enable MMCH on System Parameters Customer-Options (Optional Features) screen.
  3. Administer default multimedia outgoing trunk parameter selection on the Feature-Related System-Parameters Features screen.
  4. Administer MMCH related feature access codes on the Feature Access Code (FAC) screen.
  5. Install and administer hardware:
    - a. Install MMIs, VCs and the ESM.
    - b. Administer the ESM to ECS connection — DS1 Circuit Pack and Signaling Group screens.
    - c. Establish maintenance parameters — Maintenance-Related System Parameters screen.
  6. Administer multimedia complexes:
    - a. Administer data modules — Data Module screen, or Data Module page of the Station screen.
    - b. Administer stations as part of a multimedia complex, assign associated data module extension, multimedia mode, service link mode and appropriate multimedia buttons — Station screen
  7. Administer early answer and H.320 flag for stations, the early answer flag for hunt groups, and the multimedia flag for vectors as appropriate.
  8. Train end users.
  9. Monitor traffic and performance.

---

### Related screens

| Screen Name                        | Settings  |
|------------------------------------|---|
| System Parameters Customer-Options | Multimedia Call Handling (Basic)<br>Multimedia Call Handling (Enhanced) |

| Screen Name                           | Settings   |
|---------------------------------------|--|
| (Optional Features)                   |  |
| Feature Related System-Parameters     | Default Multimedia Outgoing Trunk Parameter Selection (p.2)  |
| Maintenance-Related System Parameters | Packet Bus Activated = y<br>Minimum Maintenance Thresholds - MMIs, VCs   |
| Data Module (type = 7500 or WCBRI)    | Multimedia (p. 1) = y<br>XID (p. 2) = n<br>MIM Support (p. 2) = n  |
| Station                               | MM Complex Data Ext (p. 1)<br>H.320 Conversion (p. 2)<br>Multimedia Early Answer (p. 2)<br>Multimedia Mode (p.2)<br>Service Link Mode (p.2)<br>Feature Buttons (p.3) (optional)  |
| Hunt Group                            | MM Early Answer (optional)   |
| Call Vector                           | Multimedia (optional)  |
| Feature Access Code (FAC)             | Basic Mode Activation (p.5)<br>Enhanced Mode Activation (p.5)<br>Multimedia Call Access Code (p.5)<br>Multimedia Data Conference Activation & Deactivation (p.5)<br>The Multimedia Data Conference Deactivation FAC must be entered after you are active on a multimedia call. To enter the FAC:<br><br><ol style="list-style-type: none"> <li>1. Select Transfer</li> <li>2. Receive a dialtone</li> <li>3. Dial the FAC</li> <li>4. Receive a confirmation tone.</li> <li>5. Re-select the call appearance for the held multimedia call <ul style="list-style-type: none"> <li>• Multimedia Multi-Address Access Code (p.5)</li> <li>• Multimedia Parameter Access Code (p.5)</li> </ul> </li> </ol> |
| DS1 Circuit Pack (ESM Only)           | Bit Rate=2.048.<br>Line Coding=hdb3<br>Signaling Mode=isdn-pri<br>Connect=pbx.<br>Interface=network.<br>Country Protocol=1<br>CRC=y.<br>MMI Cabling Board  |

| Screen Name                | Settings          |
|----------------------------|-------------------|
| Signaling group (ESM Only) | Primary D-Channel |

## MMCH Settings Administration

### System Parameters Customer-Options (Optional Features) screen

Ensure that the **Multimedia Call Handling (Basic)** field is y. This feature is provided via license file. To enable this feature, contact your Avaya representative

### Feature-Related System Parameters screen

The default bandwidth for MMCH calls is defined on the Feature-Related System Parameters screen.

#### Note:

Originating a multimedia call with the mm-call button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen.

- This default parameter will be either 2x56 or 2x64.
- The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

### Data Module screen

The H.320 DVC system should contain a BRI interface. You must connect this BRI interface to a port on a TN556 BRI circuit pack and administer it as a BRI data module.

- You can administer the data endpoint type as 7500 (recommended) or WCBRI.
- The fields for multimedia are the same on either screen.
- The administration for a Basic mode and an Enhanced mode data module are exactly the same.
- **Type** — Set the data module type to 7500 or WCBRI.
- **Multimedia** — This field appears on the Data Module screen only if MM is set to y on the System-Parameters Customer-Options (Optional Features) screen. Enter y to enable this data module to be multimedia compliant
- **MM Complex Voice Ext:** (display only) — This field contains the number of the associated telephone in the complex. This is a display-only field, and is blank until you enter the data module extension in the Station screen **MM Complex Data Ext** field. Once you have done that, these two extensions are associated as two parts of a multimedia complex.
- **XID and MIM Support** — Valid entries are y (default) and n. These fields must be set to n.

### Station screen

After you have administered the BRI data module, use the Station screen to associate it with a voice station to screen a multimedia complex. This is a one-to-one relationship: you can

administer only one station and one data endpoint per multimedia complex. Neither the voice station, nor the data endpoint can be a member of another multimedia complex.

 **Note:**

A BRI station cannot be part of a multimedia complex

**H.320 Conversion** — Valid entries are y and n (default). This field is optional for non-multimedia complex voice stations and for Basic multimedia complex voice stations. It is mandatory for Enhanced multimedia complex voice stations. Because the system can only handle a limited number of conversion calls, you might need to limit the number of telephones with H.320 conversion. Enhanced multimedia complexes must have this flag set to y.

For non-multimedia complex voice stations, setting this field to y allows H.320 calls to convert to voice and alert at the stand-alone voice station. If the call is unanswered at the voice station, the call will follow standard voice treatment. Any subsequent station that is reached in the routing of this call, that is, coverage points, forwarded destinations, call pickup members, and so forth, do not need to have the **H.320** field enabled. The **H.320** field is only needed at the first station that might receive the H.320 call.

For Basic multimedia complex voice stations, setting this field to y allows H.320 calls to convert to voice and alert at the Basic multimedia complex voice station after an attempt has been made to offer the call to the H.320 DVC system. If the call is unanswered at the H.320 DVC system, the call will alert at the voice station after 5 seconds or after the administered number of rings as specified in the voice station's coverage path. If the call is unanswered at the voice station, the call will follow standard voice treatment. Any subsequent station that is reached in the routing of this call, that is, coverage points, forwarded destinations, call pickup members, and so forth, do not need to have the **H.320** field enabled. The **H.320** field is only needed at the first station that might receive the H.320 call.

**Service Link Mode** - The service link is the combined hardware and software multimedia connection between an Enhanced mode complex's H.320 DVC system and the Avaya DEFINITY Server which terminates the H.320 protocol. A service link is never used by a Basic mode complex H.320 DVC system. Connecting a service link will take several seconds. When the service link is connected, it uses MMI, VC and system timeslot resources. When the service link is disconnected it does not tie up any resources. The Service Link Mode can be administered as either as-needed or permanent as described below:

- **As-Needed** - Most non-call center multimedia users will be administered with this service link mode. The as-needed mode provides the Enhanced multimedia complex with a connected service link whenever a multimedia call is answered by the station and for a period of 10 seconds after the last multimedia call on the station has been disconnected. Having the service link stay connected for 10 seconds allows a user to disconnect a multimedia call and then make another multimedia call without having to wait for the service link to disconnect and re-establish.
- **Permanent** - Multimedia call center agents and other users who are constantly making or receiving multimedia calls might want to be administered with this service link mode. The permanent mode service link will be connected during the station's first multimedia call and will remain in a connected state until the user disconnects from their PC's multimedia application or the Avaya DEFINITY Server restarts. This provides a multimedia user with a much quicker video cut-through when answering a multimedia call from another permanent mode station or a multimedia call that has been early answered.

**Multimedia Mode** - There are two multimedia modes, Basic and Enhanced, as described below:

- **Basic** - A Basic multimedia complex consists of a BRI-connected multimedia-equipped PC and a non-BRI-connected multifunction telephone set. When in Basic mode, users place voice calls at the multifunction telephone and multimedia calls from the multimedia equipped PC. Voice calls will be answered at the multifunction telephone and multimedia calls will alert first at the PC and if unanswered will next alert at the voice station if it is administered with H.320 = y. A Basic mode complex has limited multimedia feature capability as described in *Basic Mode Operation*.
- **Enhanced** - An Enhanced multimedia complex consists of a BRI-connected multimedia-equipped PC and a non-BRI-connected multifunction telephone. The Enhanced mode station acts as though the PC were directly connected to the multifunction telephone; the service link provides the actual connection between the Avaya DEFINITY Server and the PC. Thus, voice and multimedia calls are originated and received at the telephone set. Voice and multimedia call status are also displayed at the telephone set. An Enhanced mode station allows multimedia calls to take full advantage of most call control features as described in *Enhanced Mode Operation*.

**Multimedia Early Answer** — Valid entries are y and n (default). This field lets you set this telephone for early answer of multimedia calls. The system will answer the incoming multimedia call on behalf of the station and proceed to establish the H.320 protocol. After audio path has been established to the caller, the call will then alert at the voice station.

The station can then answer by going off-hook and will have immediate audio path. No hourglass tone will be heard by the answering party (see *Hourglass Tone*).

Example: An administrative assistant who does not have a multimedia PC, but might get multimedia mode calls from forwarding or coverage, might want to set the H.320 flag to y and the early answer flag to y on their voice station. This allows any multimedia call to be presented to the station with immediate voice path rather than hourglass tone. The answered call could then be transferred as voice to voice mail or transferred as multimedia to a user equipped with a multimedia endpoint.

#### Related topics:

[Basic Mode Operation](#) on page 377

[Enhanced Mode Operation](#) on page 378

[Hourglass Tone](#) on page 394

### Assigning Multimedia Buttons

There are six new multimedia specific buttons that can be added to a voice station. Most of them can be placed on any voice station, whether it is part of a Basic multimedia complex, an Enhanced multimedia complex or not part of any multimedia complex. Two feature buttons, **mm-basic** and **mm-pcaudio**, can only be placed on stations which are part of an Enhanced multimedia complex. All of the multimedia specific feature buttons have a corresponding feature access code except **mm-pcaudio** and **mm-cfwd**.

- 
1. Use the **mm-pcaudio** feature via the button.
  2. Use the **mm-cfwd** button to replace the standard `call forward` FAC followed by the `multimedia call` FAC.
  3. Press the **mm-call** button followed by the destination extension digits. If the user has a speakerphone the user can simply press the **mm-call** button, which preselects an idle call appearance, followed by the destination extension digits.  
This **mm-call** button can exist on any voice station. Most multimedia enabled users will want an **mm-call** button. This button (or its corresponding FAC) must be used to indicate that the user is placing a multimedia mode call. To place a multimedia mode call the user would go off-hook, select an idle call appearance.

The **mm-call** button lamp lights when you press this button during call origination. The lamp also lights to indicate that the selected call appearance is a multimedia mode call.

4. Toggle between Basic and Enhanced mode to change the station's administered Multimedia mode.  
This **mm-basic** button is only allowed on the voice station of a multimedia complex. The **mm-basic** button toggles a station between Basic and Enhanced modes. This button can NOT be used to change the station's multimedia mode when the station has an active multimedia call appearance.

When in Basic mode this field on the Station screen will show basic. When in Enhanced mode this field on the Station screen will show enhanced. The current station Multimedia mode will be saved to translation when a save translation command is executed.

5. To switch the audio path to the PC while active on a call, press the **mm-pcaudio** button (if off-hook you can now hang up the handset).  
This **mm-pcaudio** button only works for an Enhanced multimedia complex voice station. When originating or receiving a multimedia call, the audio path is connected to the voice station's handset or speakerphone device. The **mm-pcaudio** button allows a user to switch the audio portion of any call to their PC's audio input/output device (if available).

The **mm-pcaudio** button's status lamp will light up when the button is pushed to move the audio path to the PC and remain lit while the audio path is at the PC device.

 **Note:**

If you are on a voice only call, the voice path will switch to the PC device but you will get muted or loopback video depending on the multimedia endpoint software

As a user you can simply go off-hook on your voice station or press the speakerphone button to move the audio path of a multimedia call from the PC back to the voice station. Pressing the **mm-pcaudio** button while the status lamp is lit and the voice station's handset is on-hook will disconnect the user from the active call.

6. Press the **mm-datacnf** button from any voice station that is participating in a multimedia call and the status lamp will light up and alert the Avaya DEFINITY Server that you want to enable T.120 data collaboration with the other parties on the call.  
The button status lamp will also light for other participants in the multimedia call who have **mm-datacnf** buttons. Pressing this button from the voice station that enabled data collaboration on a multimedia mode call will deactivate the data session and revert to a voice and video call. If you are participating on a multimedia call with data collaboration, but did not initiate the data collaboration, and you press this button, the status lamp led will flash momentarily and the T.120 data services will not be terminated, (only the station that activated the collaboration session can deactivate it). This button only works for stations connected to an Avaya DEFINITY Server equipped with an ESM adjunct.
7. Press the **mm-cfwd** button to allow a user to indicate that multimedia mode calls will be forwarded as multimedia mode calls to a specific forwarded-to destination. If voice call forwarding is active and multimedia call forwarding is not active then multimedia calls going off of the Avaya DEFINITY Server will be forwarded as voice only calls. The **mm-cfwd** button status lamp will be lit to indicate that multimedia call forwarding is activated. Pressing the **mm-cfwd** button when the lamp is lit will deactivate multimedia call forwarding.

**Note:**

Pressing the **mm-cfwd** button is the same as dialing the regular call-fwd FAC followed by the mm-call button or FAC followed by the desired forwarded-to extension digits.

8. Press the **mm-multinbr** button to allow origination of a multimedia call from any voice station.  
The **mm-multinbr** call button is similar to the **mm-call** button. It is used when the destination being dialed requires a different address for each of the 2 B-channels. An example of this is Central Office provided ISDN-BRI. This type of BRI line is provisioned with separate listed directory numbers for each B-channel. In order to make a 2B multimedia call to such a device, two sets of address must be entered. Originating a multimedia call with the **mm-multinbr** button will originate a call according to the Default Multimedia Parameters selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

---

## Administering the ESM T.120 Server

From the system administration terminal:

- 
1. Type `list configuration all.`

A list of the installed carriers, circuit packs, and ports appears.

2. Record the location (board number) of the MMI board cabled to the TN2207 slot and verify that all other required circuit packs are present.
  3. Enter `add DS1 xxxxxx`, (where xxxxx is the location of the TN2207 PRI circuit pack recorded in step 2).  
The DS1 Circuit Pack screen appears.
  4. Set the **Name** field to `ESM DS1`.
  5. Set the **Bit Rate** field to `2.048`  
The TN2207 DS1 must have a bit rate of 2.048, even if all other DS1 boards in the system are operating at 1.544. Verify the 24/32 channel switch on the circuit pack is in the 32 channel position
  6. Set the **Line Coding** field to `hdb3`
  7. Set the **Signaling Mode** field to `isdn-pri`.
  8. Set the **Connect** field to `pbx`.
  9. Set the **Interface** field to `network`.
  10. Set the **Country Protocol** field to `1`.
  11. Set the **CRC** field to `y`.
  12. The **Idle Code** default is `11111111`.
  13. The **DCP/Analog Bearer Capability** default is `3.1` kHz.
  14. Set the **MMI Cabling Board** field to `xxxxxx` (where xxxxx is the location of the TN787 MMI circuit pack recorded in step 2).  
This must be the slot for port B of the Y-cable.  
The **MMI Interface** field `ESM` appears.
  15. Enter `add signaling-group next`.  
The Signaling Group screen appears.
  16. Set the **Associated Signaling** field to `y`.
  17. Set the **Primary D-Channel Port** field to `xxxxx16` (where xxxxx is the address of the TN2207 PRI circuit pack).  
for example: `1B0516`
  18. The **Max Number of NCA TSC** default is `0`.
  19. The **Max Number of CA TSC** default is `0`.
  20. **Trunk Group for NCA TSC** \_\_\_\_\_ (leave blank).
  21. **Trunk Group for Channel Selection** \_\_\_\_\_ (leave blank).
  22. Logoff the terminal and then log back on the terminal to view your changes.
-

## Troubleshooting ESM

To determine ESM link status, enter the following commands from the system administration terminal:

- `Status esm`
- `Status signaling-group`
- `List MMI`

### Note:

When you move ESM circuit packs, you **MUST** remove the DS1 and signaling group translations. You cannot use the `change circuit pack` command.

When a vector is used to route video (56K/64K) calls to a hunt group comprised of data extensions, the vector must have the **Multimedia** field set to n. This field causes multimedia calls routed through the vector to receive early answer treatment prior to processing the vector steps. This provides a talk path to the caller for announcements or immediate conversation with an agent and starts network billing for the incoming call when vector processing begins.

## Understanding the Multimedia Complex

### 1-number access

1-number access permits originating users to make voice or multimedia calls to a Basic multimedia complex by dialing the same number for either type of call. The number might be the voice station extension or the data module extension. If the incoming call is a voice call, Avaya Communication Manager directs it to the telephone. If the incoming call is 56K or 64K data call, Avaya Communication Manager recognizes it as such and sends it to the multimedia endpoint. Likewise, if a voice call is addressed to the data extension, the system recognizes this and directs the call to the voice station.

Calls originating on the same server as the Basic mode complex destination can always use 1-number access for voice or video. In order to take advantage of 1-number access for calls originating from a remote location, the incoming calls must arrive over ISDN-PRI trunks. If the system is setup with separate data non-PRI digital facilities multimedia calls must be made to the data extension.

AVD (alternate voice/data) trunk groups cannot be used to provide 1-number access with MMCH. If the AVD trunk group has a BCC of 0, all calls arriving over the AVD trunk to the Basic mode complex will be assumed to be voice calls. If the AVD trunk group has a BCC of 1 or 4, all calls arriving over the AVD trunk to the Basic mode complex will be assumed to be multimedia calls.

### Related topics:

[Administering ISDN-PRI Trunk Group](#) on page 351

[Administering MASI Trunk Groups](#) on page 352

### Originating voice calls

All voice calls are originated at the voice station.

## Originating multimedia calls

For a Basic mode complex, multimedia calls are normally originated at the user's multimedia equipped PC. These multimedia calls use the associated station's COR/COS.

The voice station of a Basic multimedia complex can also use the mm-call button or FAC, and the mm-multinbr button or FAC to originate multimedia calls. When these methods are used, a multimedia call is originated from the voice station. In order for the Basic multimedia complex to receive video, the user must make a call from the H.320 DVC system to the voice station of the complex or must make a multimedia call from the voice station to the H.320 DVC. This allows the station to spontaneously add themselves or other parties to a multimedia conference.

1. **H.320 DVC system GUI.** The normal way for a Basic multimedia complex endpoint to originate a multimedia call is through the vendor provided user interface. Generally, digits to dial are entered, speed is selected and the call originates from the DVC system. The voice station is not involved in such as origination.

Any voice station can use the following mechanisms to originate a multimedia call from the voice station. For stations that are not part of a multimedia complex, video cannot be provided. For voice stations that are part of a Basic multimedia complex, video is not provided until a multimedia call is made from the complex's H.320 DVC system to the voice station or a multimedia call is made from the voice station to the H.320 DVC system. Video is automatically included for Enhanced multimedia complexes.

2. **mm-call (Multimedia Call) button.** If the station has an **mm-call** button administered, the user goes off-hook and selects the **mm-call** button. The user can select the mm-call button and then go off-hook. If the user has a speakerphone on the station, the user can originate the call simply by selecting the **mm-call** button. The speakerphone will automatically be placed off-hook and dialtone will be heard. Upon selection of the **mm-call** button, the mm-call status lamp (green LED) should become solid.

The user now dials the destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, station busy indicators, etc. Originating a multimedia call with the **mm-call** button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

For calls with a bandwidth of 2B, use of the **mm-call** button to originate will cause the same destination address to be used for both channels of the 2B call. The section below on the mm-multinbr button/FAC provides information on originating a 2B call where the destination has a different address for each B-channel.

 **Note:**

The mm-call feature button is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a multimedia call.

3. **Multimedia Call feature access code.** For stations that do not have an administered **mm-call** button, the Multimedia call feature access code can be used instead. The user goes off-hook on the station, waits for dialtone, then dials the

MM-call FAC, receives dialtone again and then dials the call normally. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, station busy indicators, etc. Originating a multimedia call with the **mm-call** button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels. For calls with a bandwidth of 2B, use of the **mm-call** button to originate will cause the same destination address to be used for both channels of the 2B call. The section below on the mm-multinbr button/FAC provides information on originating a 2B call where the destination has a different address for each B-channel.

 **Note:**

The mm-call feature access code is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a multimedia call.

4. **mm-multinbr** (Multimedia Multi-number) button. The **mm-multinbr** button is similar to the **mm-call** button. It allows origination of a multimedia call from a voice station. It is used when the destination being dialed requires a different address for each of the 2 B-channels. An example of this is Central Office provided ISDN-BRI. This type of BRI line is provisioned with separate listed directory numbers for each B-channel. In order to make a 2B multimedia call to such a device, two sets of addresses must be entered.

The user goes off-hook and selects the **mm-multinbr** button. The user can select the **mm-multinbr** button and then go off-hook. If the user has a speakerphone on the station, the user can originate the call simply by selecting the mm-multinbr button. The speakerphone will automatically be placed off-hook and dialtone will be heard. Upon selection of the **mm-multinbr** button, the mm-multinbr and mm-call (if present) status lamp (green led) should light steadily. The user now dials the first destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc. The system will provide dialtone after the first address has been completed. The user now dials the second destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc. After the 2nd address has been collected the mm-multinbr status lamp will go off.

Originating a multimedia call with the **mm-multinbr** button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

 **Note:**

The mm-multinbr feature button is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a dual address multimedia call.

5. **Multimedia Multi-number Call feature access code.** For stations that do not have an administered **mm-multinbr** button, the Multimedia Multi-number call feature access code can be used instead. It allows origination of a multimedia call from a

voice station. It is used when the destination being dialed requires a different address for each of the 2 B-channels. An example of this is Central Office provided ISDN-BRI. This type of BRI line is provisioned with separate listed directory numbers for each B-channel. In order to make a 2B multimedia call to such a device, two sets of addresses must be entered.

The user goes off-hook and dials the MM-multinbr feature access code. Upon dialing of the MM-multinbr FAC, the mm-call (if present) status lamp (green led) should become solid. The user now dials the first destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc. The system will provide dialtone after the first address has been completed. The user now dials the second destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc.

Originating a multimedia call with the MM-multinbr FAC will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

 **Note:**

The mm-multinbr FAC is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a dual address multimedia call.

6. **Multimedia parameter selection feature access code.** This FAC is used to originate a multimedia call that wishes to use a different bearer and bandwidth than the system default. For example, if the system has a default multimedia parameter of 2x64 and the user wishes to make a call to a destination that is known to only have 56K digital facilities, the MM parameter selection FAC can be used to select a bearer and bandwidth of 2x56 for this specific call.

The MM parameter selection FAC can be used in conjunction with the mm-multinbr button or FAC to make a single or dual address multimedia call at the desired bearer and bandwidth. The user goes off-hook and dials the MM-parameter selection feature access code. Dialtone is returned. The user enters a single digit, 1 or 2, where 1 = 2x64, 2 = 2x56. All other digits will produce reorder. Dialtone is returned. Upon dialing of the MM-parameter selection FAC, the mm-call (if present) status lamp (green led) should become solid. The user can indicate a dual-address call at this point with the **mm-multinbr** button or FAC. The user now dials one or two sets of destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc

 **Note:**

The mm-parameter selection FAC is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a dual address multimedia call.

7. Dialing sequences that include TACs, AAR, ARS, Authorization codes, CDR account codes, FRLs

- a. Single address with TAC
  - i. Dial **mm-call** button or FAC, Hear dialtone
  - ii. Dial TAC, Dial destination digits
- b. Dual address with TAC
  - i. Dial **mm-multinbr** button or FAC, Hear dialtone
  - ii. Dial TAC, Dial 1st dest. digits, Hear dialtone
  - iii. Dial TAC, Dial 2nd dest. digits
- c. Single address with AAR/ARS
  - Dial **mm-call** button or FAC, Hear dialtone
  - Dial AAR/ARS, Dial destination digits
- d. Dual address with AAR/ARS
  - i. Dial **mm-multinbr** button or FAC, Hear dialtone
  - ii. Dial AAR/ARS, Dial 1st dest. digits, Hear dialtone
  - iii. Dial AAR/ARS, Dial 2nd dest. digits
- e. Single address with AAR/ARS and authorization code
  - i. Dial **mm-call** button or FAC, Hear dialtone
  - ii. Dial AAR/ARS FAC, Dial destination digits, Hear stutter dialtone
  - iii. Dial authorization code
- f. Dual address with AAR/ARS and authorization code
  - i. Dial **mm-multinbr** button or FAC, Hear dialtone
  - ii. Dial AAR/ARS FAC, Dial 1st dest. digits, Hear dialtone
  - iii. Dial AAR/ARS FAC, Dial 2nd dest. digits, Hear stutter dialtone
  - iv. Dial authorization code
- g. Single address with TAC or AAR/ARS and CDR account code
  - i. Dial **mm-call** button or FAC, Hear dialtone
  - ii. Dial CDR FAC, Hear dialtone
  - iii. Dial CDR account code, Hear dialtone
  - iv. Dial TAC or AAR/ARS, Hear destination digits
- h. Dual address with TAC or AAR/ARS and CDR account code
  - i. Dial **mm-multinbr** button or FAC, Hear dialtone
  - ii. Dial CDR FAC, Hear dialtone
  - iii. Dial CDR account code, Hear dialtone

- iv. Dial TAC or AAR/ARS, Dial 1st dest. digits
- v. Dial TAC or AAR/ARS, Dial 2nd dest. digits

### Receiving voice calls

Any voice calls directed to the voice or data extension of a Basic multimedia complex will ring at the voice station.

### Receiving multimedia calls

Any data calls directed to the voice or data extension of a Basic multimedia complex will ring at the multimedia equipped PC if it is available. You can answer the multimedia call at the PC and voice and video will connect to the PC. If the data endpoint is unavailable, the system verifies that the telephone of the complex is administered with the H.320 field set to y. If so, the system converts the call to voice and sends it to the telephone of the multimedia complex, where the call then alerts.

### Hourglass Tone

When a voice station answers a converted multimedia call, the answering party might hear different things depending on the nature of the originator. If the origination is directly from an H.320 DVC system or if the originator is an Enhanced mode complex on a remote server, an immediate audio path will not exist between the two parties. This is because the H.320 protocol must be established after the call is answered. It takes several seconds for the H.320 protocol to establish an audio path. During this interval the answering party will hear special ringback. When the audio path exists the special ringback will be removed and replaced with a short incoming call tone indicating that audio now exists. The combination of special ringback followed by incoming call tone is referred to as "hourglass tone." Hourglass tone is an indication to the answering party that they should wait for the H.320 call to establish audio.

#### Related topics:

[MMCH Settings Administration](#) on page 383

### Early Answer

The answering party can administer their station to avoid hearing hourglass tone. With the Station screen **Early Answer** field set to y, the system answers the incoming multimedia call on behalf of the station and establishes the H.320 protocol. After audio path has been established, the call will then alert at the voice station of the Basic complex destination. The station can then answer by going off-hook and will have immediate audio path. No hourglass tone will be heard by the answering party.

If the **H.320** field is not set to y for the telephone of a Basic multimedia complex, H.320 calls alert at the multimedia endpoint until the caller drops. If an H.320 call is directed to a telephone with **H.320** set to n, the system denies the call.

You can assign H.320 conversion to any voice station.

### Authorization

Multimedia complexes require the same types of authorization (COR/COS) as standard telephones. If a call is addressed to the voice extension, the system checks the COR/COS of the telephone, whether the call is voice-only or multimedia. If a call is addressed to the data extension, the system checks the COR/COS of the data endpoint. If the call is subsequently redirected to the voice station, the system does a second COR/COS check for the authorization of the voice station. Calls originated from the PC use the COR/COS of the voice station.

## Adjunct Switch Applications Interface

ASAI is not expected to support call-association for data calls. Therefore Avaya does not recommend that you use ASAI for multimedia.

## Administered Connection

Screen path: change administered-connection

This screen assigns an end-to-end Administered Connection (AC) between two access endpoints or data endpoints. The AC is established automatically by the system whenever the system restarts or the AC is due to be active. For information on how to access the endpoints, see *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

## Authorization and Barrier Codes

Basic Mode multimedia users or off-premises PC users might not be able to respond to prompts for authorization or barrier codes. Multimedia endpoints do not recognize the prompts.

An on-premises user might be able to use Remote Access and enter the entire digit string at once before launching the call, but it would be better to eliminate the need for such codes for multimedia users who need to call off premises.

## Bridged Appearances

Voice users can bridge onto a call if the user has a bridged appearance of a voice member of the call.

## Call Redirection

Calls directed to either member of the Basic multimedia complex are subject to redirection (coverage, forwarding). Avaya Communication Manager converts calls to voice before sending them to coverage. Calls redirected through call forwarding maintain multimedia status if forwarded from the data endpoint.

## Conferencing

A multimedia conference can consist of multimedia and voice-only conferees. All multimedia conferees are added to a multimedia conference by a voice-terminal user on Communication Manager, who acts as the controller of the multimedia conference. When the controller is a Basic complex voice station, the controller must remain on the conference until all parties have joined. Once all endpoints are on the conference, the voice-terminal user can put the call on hold or drop, if the user wishes.

Video conferees can see only their local video and one other party. If more than two people are involved in a video conference, the person who is speaking is the one whose video appears to other conferees. The speaker's video shows the previous speaker. This changes dynamically as the speaker changes.

## Creating a multi-party video conference

All multimedia conferences must be controlled by a voice telephone. Multimedia conferees can be added by calling the voice telephone or by having the voice telephone make a multimedia call to other DVC endpoints. The controller can then conference together individual parties to create a multimedia conference.

- 
1. Determine who is going to be the conference controller.
  2. At the appointed time, the conference controller calls his or her telephone from the multimedia endpoint by dialing the 1-number extension. Once this call is established, the controller conferences in other calls as if this were a voice conference. The controller continues to add conferees in this manner until all conferees have joined, or until the number of conferees reaches the administered limit.
  3. The conference controller can also add voice or multimedia parties to the conference spontaneously. The controller presses **CONFERENCE**, makes a voice or multimedia call to a new party. To make a multimedia call, the controller must originate a call using the mm-call button or FAC or the **mm-multinbr** button or FAC. After the new party begins alerting, the controller can press **CONFERENCE** to add the party to the existing conference call on hold.

---

## Coverage

Multimedia calls to a Basic mode complex are subject to the same coverage criteria as voice calls and follow the coverage path administered for the voice station of the Basic multimedia mode complex.

If a plain voice station or a Basic mode complex is the covering party, the answering voice station will receive audio only. If all voice stations in the coverage path have the Station screen Early Answer field set to n and the originator of the multimedia call was not a local Enhanced mode complex, the answering station will hear hourglass tone. If an Enhanced mode complex is the covering party, the answering voice station will receive voice and video.

If all voice stations in the coverage path have the Station screen **Early Answer** field set to n and the originator of the multimedia call was not a local Enhanced mode complex, the answering station will hear hourglass tone.

### **Coverage: Multimedia calls and off-net call coverage**

If the principal station's coverage path include a remote coverage point, the multimedia call will cover off-switch as voice only. If the call is unanswered off-switch and proceeds to the next coverage point on-switch, the multimedia nature of the call is preserved.

### **Coverage: Multimedia calls and coverage to voice mail**

Voice mail systems such as AUDIX are typically the last point in a coverage path and are usually implemented as a hunt group. In order to guarantee that the originator of an H.320 multimedia call hears the voice mail greeting, the hunt group that defines the list of voice mail ports should have the **Early Answer** field on the hunt group set to y. This field will have no effect on voice calls to the voice mail system.

## **Call Detail Recording**

Each channel of a 2-channel call generates a separate CDR record.

## Data Collaboration

Once you have established a multi-point video conference, multi-point T.120 data collaboration can be enabled for that call. This will allow all video parties on the current conference to collaborate.

T.120 Data conferencing is made possible through the Extended Services Module (ESM) server, which is an adjunct to Avaya Communication Manager. Up to six parties can participate in a single data conference, and up to 24 parties can use the ESM facilities for data collaboration at any given time.

### *Adding data sharing to a video conference*

- 
1. Set up a multimedia conference.
  2. Once a multimedia call is active, any voice station in the conference, can initiate data collaboration by pressing the **mm-datacnf** button. Or, to use the feature access code to initiate a data conference, press the **Transfer** button.  
A second line-appearance becomes active and you hear the dial tone.
  3. Dial the multimedia data conference feature access code.  
Confirmation tone is heard and the system automatically reselects the held call appearance of the multimedia conference. Avaya Communication Manager will select a data rate which is acceptable to all H.320 DVC systems in the current call. If the system does not have sufficient ESM server resources available for all parties currently in the call, the activation of T.120 data sharing will be denied. The mm-datacnf status lamp will flash denial or the mm-datacnf FAC will produce reorder.

 **Note:**

Each H.320 DVC system in the conference call is joined to the data conference. On many DVC systems, the provided GUI can prompt the user with a dialog box, requesting the user to select a specific conference to join. With MMCH, there should only be one conference available to select.

4. You must now use the PC's GUI to begin application sharing.  
The method for beginning application sharing or file transfer is different for each H.320 multimedia application. One of the H.320 DVC systems activates data sharing from the H.320 DVC vendor provided GUI. See your H.320 DVC system documentation for details.  
  
The same H.320 DVC system as in step 4, opens an application, whiteboard, etc. to share and the image of the application is displayed on all H.320 DVC systems in the conference. For details on how multiple users can control the shared application, see the vendor provided documentation for your specific H.320 DVC system.
5. To end the data collaboration session and retain the voice/video conference, the station that selected the **mm-datacnf** button or FAC can press the **mm-datacnf** button or hit transfer and dial the mm-datacnf deactivation FAC.

 **Note:**

As of this writing, many endpoints do not respond correctly to ending the data collaboration session and retaining voice/video. Some H.320 DVC systems drop

the entire call. Avaya recommends that once T.120 data sharing has been enabled for a conference, that it remain active for the duration of the conference call. When all endpoints have dropped from the call, the T.120 resources will be released.

---

### ***Joining a multimedia conference after T.120 data sharing has been enabled***

If a multimedia conference with T.120 data sharing is already active and it is desired to conference in a new video endpoint, the new video endpoint can be conferenced into the existing call. The new endpoint will be allowed into the data conference if there exists sufficient ESM server resources for the new endpoint. The new endpoint will get voice/video and data sharing if the new endpoint supports the multi-layer protocol (MLP) data rate chosen by the system when T.120 data collaboration was activated. If the endpoint does not support the pre-existing MLP data rate, the new endpoint will only receive voice and video.

### ***Single server or switch data collaboration***

When all parties involved in data collaboration conference are located on the same physical Avaya S8XXX Server, there is no restriction on the type of user. The parties can be any combination of Enhanced multimedia complexes, Basic multimedia complexes, or stand-alone H.320 DVC systems.

### ***Multi-switch data collaboration***

When all parties involved in data collaboration conference are not located on the same physical Avaya S8XXX Server, the parties located on the Avaya server hosting the data conference (i.e. the server which activated **mm-datacnf**) can be any combination of Enhanced multimedia complexes, Basic multimedia complexes or stand-alone H.320 DVC systems.

#### **Note:**

All parties on remote servers must not be Enhanced multimedia complexes: they must be Basic multimedia complexes or stand-alone H.320 DVC systems.

Prior to originating or receiving a multimedia mode call, the **mm-basic** feature button or feature access code can be used to dynamically change an Enhanced mode complex into a Basic mode complex and back again.

### **Forwarding voice/multimedia calls**

In Basic mode you can forward calls from either the telephone or the multimedia endpoint.

- 
1. At the PC's multimedia application, enter the call-forwarding feature access code (FAC).
  2. Enter the forward-to number in the `Dialed Number` field on the endpoint software.
  3. Click the **Dial** button (or equivalent)

#### **Note:**

The PC multimedia software will probably respond with a message that the call failed, since it does not recognize the FAC. In fact, Avaya Communication Manager does receive the message, and forwards all multimedia calls addressed to the 1-number.

If a call is forwarded from the telephone, the call converts to voice first. If using the multimedia endpoint to forward, the calls arrive at the forwarded-to extension as a

data call. Such calls continue to ring until answered or abandoned, rather than follow a coverage path.

Users can forward calls from the multimedia endpoint using the call forward FAC. You can also assign a call-forward button at the voice station to forward calls for the data endpoint. If a Basic multimedia complex has console permissions, that user can forward calls for others by dialing the FAC, the data extension, and then the forwarded-to number.

---

## Call Park

A voice-terminal user can park any active call, voice or multimedia, and unpark the call from another telephone. Users cannot park or unpark calls using multimedia endpoints.

## Call Pickup

Users might need to answer a call that is ringing at a nearby desk. With Communication Manager, a user can answer a call that is ringing at another telephone in three ways:

- Use Call Pickup. With Call Pickup, you create one or more pickup groups. A pickup group is a collection, or list, of individual telephone extensions. A pickup group is the way to connect individual extensions together. For example, if you want everyone in the payroll department to be able to answer calls to any other payroll extension, you can create a pickup group that contains all of the payroll extensions.

A user extension can belong to only one pickup group. Also, the maximum number of pickup groups might be limited by your system configuration.

Using their own telephones, all members in a pickup group can answer a call that is ringing at another group member telephone. If more than one telephone is ringing, the system selects the extension that has been ringing the longest.

- Use Extended Call Pickup. With Extended Call Pickup, you can define one or more extended pickup groups. An extended pickup group is the way to connect individual pickup groups together.

There are two types of extended pickup groups: simple and flexible. You administer the type of extended pickup groups on a system-wide basis. You cannot have both simple and flexible extended pickup groups on your system at the same time.

Based on the type of extended pickup group that you administer, members in one pickup group can answer calls to another pickup group.

For more information, see *Setting up simple extended pickup groups*, *Setting up flexible extended pickup groups*, and *Changing extended pickup groups*.

- Use Directed Call Pickup. With Directed Call Pickup, users specify what ringing telephone they want to answer. A pickup group is not required with Directed Call Pickup. You must first administer Directed Call Pickup before anyone can use this feature.

For more information, see *Setting up Directed Call Pickup*.

### **Consult**

After a call is converted to voice, consult can be used when transferring or conferencing the call.

### **COR / COS**

The Class of Restriction and Class of Service for H.320 calls originated from a 1-number complex are the same as those of the telephone in the complex.

### **Data Call Setup**

Basic complex multimedia endpoints are BRI data endpoints, and can use data call-setup procedures as provided by the software vendor.

### **Data Hotline**

Data Hotline provides for automatic-nondial placement of a data call preassigned to an endpoint when the originating server goes off-hook. Use for security purposes.

If endpoint software allows users to select the dial function without entering a number, the endpoint can be used for hotline dialing.

### **Dial Access to Attendant**

Access to Attendant is blocked for a data call from a Basic mode multimedia endpoint.

### **Data Trunk Groups**

Data trunk groups can be used to carry H.320 calls of a fixed (administered) bearer capability.

### **Hold**

The voice station and multimedia endpoint of a Basic complex are each independent devices with respect to call control. When a Basic multimedia complex voice station executes hold only the voice station is held. If the user has conferenced their multimedia endpoint into a multimedia conference, activating hold will not disconnect the multimedia endpoint from the conference, it will only disconnect the Basic multimedia complex voice station. Executing hold with an Enhanced mode complex will fully disconnect voice and video from the current active call.

### **Hunt Groups using Basic Mode complexes**

Since Basic mode complexes can receive point to point multimedia calls at the DVC system and voice calls to the station simultaneously, the voice station extension can be placed in any normal voice hunt group or ACD skill and the data extension can be placed in a simple hunt group made up of only data extensions.

Basic mode complex data extensions or stand-alone data extensions can be used to create simple data hunt groups. Data extensions are not allowed in ACD hunt groups. Avaya recommends that you do not mix voice and data stations in a hunt group.

If you want multimedia calls to hunt to multimedia endpoints (i.e. 2B point to point data hunting), put the data extension in the hunt group. If you place the voice extension in a hunt group, only voice calls hunt to that extension. Multimedia calls to a hunt group with a Basic mode voice station as the hunt group member will not be offered to the DVC system of the Basic mode complex. If either the voice or data extension of a Basic mode complex is busy, the entire complex is considered busy for hunting purposes.

In order to guarantee that all members of a voice hunt group or skill can receive voice or multimedia calls, all members should have the H.320 field on the Station screen set to y. Simple voice stations and Basic complex mode voice stations will receive voice only. Enhanced mode stations will receive voice and video.

The **MM Early Answer** field (on the Hunt Group screen) tells the system to answer the incoming multimedia call and establish audio before it reaches the first member of the hunt group. Thus, when the talk path is established, the caller is able to speak with an agent immediately. This is not necessary for hunt groups comprised of data extensions.

### Hunting, Other considerations

Agents that are part of a Basic mode complex can dial a feature access code to remove themselves from availability (and to indicate that they are available again) from both the multimedia endpoint and the telephone independently. This allows the voice member or the data member to be individually made unavailable. To make the data extension unavailable, the agent must dial the FAC from the DVC system. CMS measurements can indicate unusually slow ASA, because of the time required for the system to establish early-answer before offering the call to an agent.

### Hunting Call association (routing)

Typically incoming voice calls consist of 2 B-channel calls to the same address, to provide greater bandwidth and better video resolution. Avaya Communication Manager attempts to correctly pair up incoming calls and offer them as a unit to a single agent. MMCH uses call association to route both calls to the extension that answered the first call, regardless of how the call was routed internally.

Two 56K/64K data calls with the same calling party number to the same destination number are considered to be associated. The system makes every attempt to route both calls of a 2-channel call to the same answering party. If the first call terminates at a member of a hunt group, the second call does not have to hunt, but goes directly to the same member. In order for 2B multimedia calls to be correctly given to a single agent, incoming calls to the hunt group must have ANI information. The ANI information can be in the form of ISDN calling party number or DCS calling party number. Multimedia calls made on the same Avaya S8XXX Server as the hunt group are easily associated. If multimedia calls into a hunt group have incorrect ANI information (i.e. all calls from server X to server Y include the LDN for server X), then as the volume of calls increases, the number of mis-associated calls will increase. If multimedia calls into a hunt group have no ANI information, Communication Manager will never associate pairs of calls and all calls will be treated independently and routed to separate agents. This is not a recommended configuration.

### Hunting with Multimedia vectors

Calls are often routed to hunt groups or skills via a vector. The existing VDNs and vectors which exist for routing voice calls can be used to route multimedia calls.

In order to use a vector for multimedia calls that will terminate to voice stations, you must set the **Multimedia** field on the Call Vector screen to y. This field has no effect on voice calls routing through the vector. This field will cause multimedia calls routed through the vector to receive early answer treatment prior to processing the vector steps. This provides a talk path to the caller for announcements or immediate conversation with an agent.

#### Note:

Vectors which have the **Multimedia** field set to y must eventually route to hunt groups, skills or numbers which are voice extensions. A vector with the **Multimedia** field set to y should never be set up to route to a hunt group or number which is a data extension.

When a vector is used to route video (56K/64K) calls to a hunt group comprised of data extensions, the vector must have the **Multimedia** field set to n.

### **Intercept Treatment**

H.320 calls that receive intercept treatment are treated like other data calls. H.320 calls cannot be directed to an attendant for service because the attendant cannot have H.320 conversion service.

### **ISDN Trunk Groups**

Avaya highly recommends that you use ISDN trunks for multimedia calls. ISDN PRI trunks allow complete 1-number access for an Enhanced multimedia complex. ANI provided over PRI trunks allows correct routing of multiple bearer channels to the correct destination device. ISDN also provides the bearer capability on a call by call basis which can be used to distinguish voice calls from multimedia calls.

### **Malicious Call Trace**

If a malicious call terminates at a Basic multimedia complex endpoint, the user can dial the feature access code from the telephone to activate malicious call trace, followed by the extension of the multimedia endpoint. If the user does not dial the multimedia extension, MCT traces any call held on the telephone.

### **Message Waiting**

Message Waiting indication is handled at the telephone. Because H.320 calls are converted to voice before going to coverage, all messages are voice only.

### **Night Service**

You can use night service to direct calls to an alternate location when the primary answering group is not available. For example, you can administer night service so that anyone in your marketing department can answer incoming calls when the attendant is at lunch or has left for the day.

Once you administer night service to route calls, your end-users merely press a button on the console or a feature button on their telephones to toggle between normal coverage and night service.

There are five types of night service:

- Night Console Night Service — directs all attendant calls to a night or day/night console
- Night Station Night Service — directs all incoming trunk or attendant calls to a night service destination
- Trunk Answer from Any Station (TAAS) — directs incoming attendant calls and signals a bell or buzzer to alert other employees that they can answer the calls
- Trunk Group Night Service — directs incoming calls to individual trunk groups to a night service destination
- Hunt Group Night Service — directs hunt group calls to a night service destination

### **Remote Access**

Communication Manager does not prevent Basic multimedia complexes from attempting to use remote access. However, these Basic mode endpoints will most likely not be able to dial the necessary codes.

**Station Hunting**

Basic mode data calls to endpoints that have an extension administered in the **Hunt-to-station** field hunt based on established hunting criteria. The call is converted to voice before station hunting.

**Tenant Partitioning**

Permission to make multimedia calls or add parties of any type to a conference is subject to standard tenant-partitioning restrictions.

**Terminating Extension Groups**

Basic mode data calls to a TEG are converted to voice and can terminate only at a voice endpoint. Effectively, Communication Manager treats the multimedia-complex extension as a voice-only endpoint.

**Telephone Display**

Display information for calls to or from a Basic multimedia complex contains the 1-number.

**Enhanced Mode Operation**

The Enhanced multimedia complex provides a much more tightly coupled integration of the complex voice station and H.320 DVC system. In Enhanced Mode:

- Both multimedia and voice calls must originate at the telephone set.
- Voice and multimedia calls can be controlled at the telephone set.
- Conferencing is spontaneous and established just like a voice-only conference call.
- There is extensive support for multimedia feature interaction. Most voice features work the same for multimedia calls.
- Service Links can be either “permanent” or “as-needed”

**Related topics:**

[MMCH Settings Administration](#) on page 383

**Enhanced Mode MM Complex**

The Enhanced multimedia complex provides a much greater unified and integrated interface for control of voice and multimedia calls. The multifunction voice station is used to control all calls, whether voice or multimedia. The H.320 desktop video system is used to present the video stream, data stream and (optionally) audio stream to the user. The H.320 desktop video system is not used for call control. The Enhanced multimedia complex allows the multifunction voice station to handle voice or multimedia calls in an almost identical manner. Each call appearance on the voice station can represent a voice or multimedia call, allowing multiple voice or multimedia calls to be present simultaneously on the station. The user can manage the separate call appearances without regard to the voice or multimedia nature of the specific call. The standard HOLD/TRANSFER/CONFERENCE/DROP actions can be applied to any call, without regard to the voice or multimedia nature of the call.

**Originating Multimedia calls**

The basic call sequence from an Enhanced mode complex is to originate a multimedia call and alert the destination. When the destination answers the call, the originating station’s H.320 desktop video system will be alerted (that is, called by Communication Manager to establish the service link). If the H.320 DVC is not configured for auto-answer, the user must answer the

H.320 calls via the DVC GUI. If the H.320 DVC is configured for auto-answer, no action is needed via the DVC GUI.

 **Note:**

Avaya recommends, but does not require, that Enhanced mode complexes place their desktop video system into an auto-answer mode of operation.

If the far-end is providing a video signal, the 2-way video will be observed. If the destination is not providing a video signal (call was answered by a simple voice telephone), then loopback video will be provided at the Enhanced mode complex originator. The audio signal will exist at the handset of the voice telephone. The audio signal can be moved to the H.320 DVC system via activation of a **mm-pcaudio** button on the voice telephone.

### Hourglass tone

The originating party might hear different things when the incoming multimedia call is answered depending on the nature of the answering party. If the call is being answered directly by an H.320 DVC system or if the answering party is an Enhanced mode complex on a remote server, an immediate audio path will not exist between the two parties. This is because the H.320 protocol must be established after the call is answered. It takes several seconds for the H.320 protocol to establish an audio path. During this interval the originating party will hear special ringback. When the audio path exists the special ringback will be removed and replaced with a short incoming call tone indicating that audio path now exists. The combination of special ringback followed by incoming call tone is referred to as "hourglass tone." Hourglass tone is an indication to the originating party that they should wait for the H.320 call to establish audio.

### Originating voice calls

Voice calls are originated from the voice station of an Enhanced mode complex in the normal manner as for any voice station.

### Originating multimedia calls

STATION, NOT the H.320 desktop video system. All multimedia originations require the user to indicate the multimedia nature of the call prior to providing any address digits. There are several different ways to originate a multimedia call from the voice station.

1. **mm-call** (Multimedia Call) button. If the station has an **mm-call** button administered, the user goes off-hook and selects the **mm-call** button. The user can select the **mm-call** button and then go off-hook. If the user has a speakerphone on the station, the user can originate the call simply by selecting the **mm-call** button. The speakerphone will automatically be placed off-hook and dialtone will be heard. Upon selection of the **mm-call** button, the mm-call status lamp (green LED) will light steadily, indicating a multimedia call. The user now dials the destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, station busy indicators, etc. Originating a multimedia call with the mm-call button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels. For calls with a bandwidth of 2B, use of the **mm-call** button to originate will cause the same destination address to be used for both channels of the 2B call. The

section below on the **mm-multinbr** button/FAC provides information on originating a 2B call where the destination has a different address for each B-channel.

 **Note:**

The mm-call feature button is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a multimedia call.

2. Multimedia Call feature access code. For stations that do not have an administered **mm-call** button, the Multimedia call feature access code can be used instead. The user goes off-hook on the station, waits for dialtone, then dials the MM-call FAC, receives dialtone again and then dials the call normally. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, station busy indicators, etc.

Originating a multimedia call with the **mm-call** button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

For calls with a bandwidth of 2B, use of the mm-call button to originate will cause the same destination address to be used for both channels of the 2B call. The section below on the mm-multinbr button/FAC provides information on originating a 2B call where the destination has a different address for each B-channel.

 **Note:**

The mm-call feature access code is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a multimedia call.

3. **mm-multinbr** (Multimedia Multi-number) button. The mm-multinbr button is similar to the mm-call button. It allows origination of a multimedia call from a voice station. It is used when the destination being dialed requires a different address for each of the 2 B-channels. An example of this is Central Office provided ISDN-BRI. This type of BRI line is provisioned with separate listed directory numbers for each B-channel. In order to make a 2B multimedia call to such a device, two sets of addresses must be entered.

The user goes off-hook and selects the **mm-multinbr** button. The user can select the **mm-multinbr** button and then go off-hook. If the user has a speakerphone on the station, the user can originate the call simply by selecting the **mm-multinbr** button. The speakerphone will automatically be placed off-hook and dialtone will be heard. Upon selection of the **mm-multinbr** button, the **mm-multinbr** and **mm-call** (if present) status lamp (green led) should become solid. The user now dials the first destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc. The system will provide dialtone after the first address has been completed. The user now dials the second destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc. After the second address has been collected, the mm-multinbr status lamp will go off.

Originating a multimedia call with the **mm-multinbr** button will originate a call according to the **Default Multimedia Parameters** selected on the Feature-

Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

 **Note:**

The mm-multinbr feature button is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a dual address multimedia call.

4. Multimedia Multi-number Call feature access code. For stations that do not have an administered **mm-multinbr** button, the Multimedia Multi-number call feature access code can be used instead. It allows origination of a multimedia call from a voice station. It is used when the destination being dialed requires a different address for each of the 2 B-channels. An example of this is Central Office provided ISDN-BRI. This type of BRI line is provisioned with separate listed directory numbers for each B-channel. In order to make a 2B multimedia call to such a device, two sets of addresses must be entered.

The user goes off-hook and dials the MM-multinbr feature access code. Upon dialing of the MM-multinbr FAC, the mm-call (if present) status lamp (green led) should become solid. The user now dials the first destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc. The system will provide dialtone after the first address has been completed. The user now dials the second destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc.

Originating a multimedia call with the MM-multinbr FAC will originate a call according to the **Default Multimedia Parameters** selected on the Feature-Related System Parameters screen. This default parameter will be either 2x56 or 2x64. The bearer capability of the multimedia calls will either be 56K or 64K and the bandwidth will be 2B channels.

 **Note:**

The mm-multinbr FAC is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a dual address multimedia call.

5. Multimedia parameter selection feature access code. This FAC is used to originate a multimedia call that wishes to use a different bearer and bandwidth than the system default. For example, if the system has a default multimedia parameter of 2x64 and the user wishes to make a call to a destination that is known to only have 56K digital facilities, the MM parameter selection FAC can be used to select a bearer and bandwidth of 2x56 for this specific call.

The MM parameter selection FAC can be used in conjunction with the **mm-multinbr** button or FAC to make a single or dual address multimedia call at the desired bearer and bandwidth. The user goes off-hook and dials the MM-parameter selection feature access code. Dialtone is returned. The user enters a single digit, 1 or 2, where 1 = 2x64, 2 = 2x56. All other digits will produce reorder. Dialtone is returned. Upon dialing of the MM-parameter selection FAC, the mm-call (if present) status lamp (green led) should become solid. The user can indicate a dual-address call at this point with the mm-multinbr button or FAC. The user now

dials one or two sets of destination address digits. The destination address can be provided by dialing digits, using abbreviated dial entries, last number dialed, etc.



**Note:**

The mm-parameter selection FAC is generally used by stations that are part of an Enhanced multimedia complex, but can be used by any station to originate a dual address multimedia call.

6. Dialing sequences that include TACs, AAR, ARS, Authorization codes, CDR account codes, FRLs
  - a. Single address with TAC
    - Dial **mm-call** button or FAC, Hear dialtone
    - Dial TAC, Dial destination digits
  - b. Dual address with TAC
    - Dial **mm-multinbr** button or FAC, Hear dialtone
    - Dial TAC, Dial 1st dest. digits, Hear dialtone
    - Dial TAC, Dial 2nd dest. digits
  - c. Single address with AAR/ARS
    - Dial **mm-call** button or FAC, Hear dialtone
    - Dial AAR/ARS, Dial destination digits
  - d. Dual address with AAR/ARS
    - Dial **mm-multinbr** button or FAC, Hear dialtone
    - Dial AAR/ARS, Dial 1st dest. digits, Hear dialtone
    - Dial AAR/ARS, Dial 2nd dest. digits
  - e. Single address with AAR/ARS and authorization code
    - Dial mm-call button or FAC, Hear dialtone
    - Dial AAR/ARS FAC, Dial destination digits, Hear stutter dialtone
    - Dial authorization code
  - f. Dual address with AAR/ARS and authorization code
    - Dial **mm-multinbr** button or FAC, Hear dialtone
    - Dial AAR/ARS, Dial 1st dest. digits, Hear dialtone
    - Dial AAR/ARS, Dial 2nd dest. digits, Hear stutter dialtone
    - Dial authorization code
  - g. Single address with TAC or AAR/ARS and CDR account code
    - Dial **mm-call** button or FAC, Hear dialtone
    - Dial CDR FAC, Hear dialtone.

- Dial CDR account code, Hear dialtone
  - Dial TAC or AAR/ARS, Dial destination digits
- h. Dual address with TAC or AAR/ARS and CDR account code
- Dial **mm-multinbr** button or FAC, Hear dialtone
  - Dial CDR FAC, Hear dialtone
  - Dial CDR account code, Hear dialtone
  - Dial TAC or AAR/ARS, Dial 1st dest. digits
  - Dial TAC or AAR/ARS, Dial 2nd dest. digits

### Answering multimedia calls

The user actions required to answer voice or multimedia calls at an Enhanced multimedia complex are identical if the H.320 DVC system is configured for auto-answer. If the H.320 DVC system is not configured for auto-answer an additional step is required. See Answering multimedia calls below.

 **Note:**

Avaya recommends, but does not require, that Enhanced mode complexes place their desktop video system into an auto-answer mode of operation.

### Answering voice calls

Incoming voice calls will alert at the voice station of the Enhanced multimedia complex in the normal manner. Standard alerting and call appearance flashing will occur. They are answered in the normal manner by selecting the alerting call appearance and going off-hook on the voice station.

### Answering multimedia calls

Incoming multimedia calls will alert at the voice station of the Enhanced multimedia complex in the same manner as voice calls with one addition. If the alerting station has an administered mm-call button and the alerting call appearance is the selected call appearance (for instance, the red LED is lit, on the alerting call appearance), then the mm-call button status lamp will go on indicating that the call on the selected call appearance is a multimedia call.

The incoming multimedia call is answered in the normal manner by selecting the alerting call appearance and going off-hook on the voice station. If the H.320 DVC system for the answering party is configured for auto-answer, no other action is needed to complete the multimedia call. If the H.320 DVC system for the answering party is not configured for auto-answer, the H.320 DVC system will alert and must also be answered by the user.

 **Note:**

Avaya recommends, but does not require, that Enhanced mode complexes place their desktop video system into an auto-answer mode of operation.

If the originating party is providing a video signal, then a complete 2-way multimedia call will exist. If the originating party is not providing a video signal, the answering party will receive loopback video. The audio signal will exist at the handset of the voice station. The audio signal

can be moved to the H.320 DVC system via activation of a **mm-pcaudio** button on the voice station.

### Hourglass Tone

The answering party might hear different things when the incoming multimedia call is answered depending on the nature of the originator. If the origination is directly from an H.320 DVC system or if the originator is an Enhanced mode complex on a remote server, an immediate audio path will not exist between the two parties. This is because the H.320 protocol must be established after the call is answered. It takes several seconds for the H.320 protocol to establish an audio path. During this interval the answering party will hear special ringback. When the audio path exists the special ringback will be removed and replaced with a short "incoming call tone" indicating that audio now exists. The combination of special ringback followed by incoming call tone is referred to as "hourglass tone". Hourglass tone is an indication to the answering party that they should wait for the H.320 call to establish audio.

### Early Answer

The answering party can administer their station in such a way as to avoid hearing hourglass tone. If the Station screen has set the **Early Answer** field to  $\checkmark$ , then the system will answer the incoming multimedia call on behalf of the station and proceed to establish the H.320 protocol. After audio path has been established, the call will then alert at the voice station of the Enhanced mode complex destination. The station can then answer by going off-hook and will have immediate audio path. No hourglass tone will be heard by the answering party.

### Multiple call appearance operation

With an Enhanced mode complex all calls to or from the complex are controlled via the voice station. Each voice or multimedia call has its own call appearance which can be selected without regard for the nature of the call using the specific call appearance. This allows a multifunction station to control multiple voice or multimedia calls in exactly the same way they would control multiple voice calls.

As an example, a user can originate a simple voice call on the first call appearance. A multimedia call can then arrive on the second call appearance. The user activates **HOLD** on the first call appearance and selects the second call appearance to answer the multimedia call. The user can then activate **HOLD** on the second call appearance and reselect the first call appearance or select a third call appearance and originate another call.

### A multi-party video conference

An Enhanced multimedia complex can create a spontaneous video conference in the same way that a spontaneous voice conference is created. Given an active call, the user activates the **CONFERENCE** button. This puts the current call on **HOLD** and activates a new call appearance. The user makes a multimedia call according to the instructions for originating a multimedia call and then selects **CONFERENCE** to combine or merge the two call appearances. This results in a 3-way conference.

If all three parties are video equipped, then a 3-way video conference results. Conference members see the current speaker on video. The current speaker sees the last speaker on video. If one of the parties is not video equipped, then a 3-way audio conference exists and the two video equipped parties have 2-way video. The **CONFERENCE** action can be repeated until 6 parties have been conferenced together. The 6 parties can be any mix of voice or video, local or remote parties.

## Data Collaboration

Once you have established a multi-point video conference, multi-point T.120 data collaboration can be enabled for that call. This will allow all video parties on the current conference to collaborate. T.120 Data conferencing is made possible through the Extended Services Module (ESM) server, which is an adjunct to the Avaya DEFINITY Server. Up to six parties can participate in a single data conference, and up to 24 parties can use ESM facilities for data collaboration at any given time.

### Joining a multimedia conference after T.120 data sharing has been enabled

If a multimedia conference with T.120 data sharing is already active and it is desired to conference in a new video endpoint, the new video endpoint can be conferenced into the existing call. The new endpoint will be allowed into the data conference if there exists sufficient ESM server resources for the new endpoint. The new endpoint will get voice/video and data sharing if the new endpoint supports the data rate chosen by the system when T.120 data collaboration was activated. If the endpoint does not support the pre-existing data rate, the new endpoint will only receive voice and video.

### Activating HOLD while on a T.120 data collaboration conference

If an Enhanced multimedia complex is active on a multimedia call and the call has activated T.120 data collaboration, the user should be receiving voice/video and data. If the station places this existing call on hold, audio and video will be disconnected for the current call. The data collaboration portion of the call will remain intact and unaffected. While this T.120 data conference is on hold, the user will only be allowed to receive audio on all other call appearances. Thus a user is limited to one call appearance that has T.120 data collaboration active

## Creating a multi-party video conference

Create a multi-party voice/video conference

- 
1. Enhanced mode complex station A originates a multimedia call to, or receives a multimedia call from, party B. Station A and party B have 2-way voice and video.
  2. Station A, activates CONFERENCE
  3. Station A originates a multimedia call (i.e. uses the mm-call button/FAC/etc.) and dials the party to be added, Enhanced multimedia complex C.
  4. Party C, answers the call from station A.
  5. Station A selects CONFERENCE to complete the 3-way conference. Parties A,B and C will be in a 3-way voice/video conference.

#### Note:

If party C is another Enhanced mode complex on the same Communication Manager server as station A, station A does not need to indicate a multimedia call prior to dialing the new party in step 3. While A consults with C, the call will be audio only. When A completes the conference in step 5, party C's video will be activated.

A multi-party video conference uses voice-activated switching to determine which parties are seen. The current speaker is seen by all other parties. The current speaker sees the previous speaker.

Additional voice or video parties can be added by repeating these steps.

---

## Data Sharing to a Video Conference

---

1. Set up a multimedia conference.
2. Once a multimedia call is active, any member can initiate data collaboration by pressing the **mm-datacnf** button. Or, to use the feature access code to initiate a data conference, press the **Transfer** button.  
A second line-appearance becomes active and you hear dial tone. Dial the multimedia data conference feature access code. Confirmation tone is heard and the system automatically reselects the held call appearance of the multimedia conference. Avaya Communication Manager will select an MLP data rate acceptable to all H.320 DVC systems in the current call.  
  
If the system does not have sufficient ESM server resources available for all parties currently in the call, activation of T.120 data sharing will be denied. The mm-datacnf status lamp will flash denial or the mm-datacnf FAC will produce reorder.
3. Each H.320 DVC system in the conference call is joined to the data conference. On many DVC systems, the provided GUI might prompt the user with a dialog box, requesting the user to select a specific conference to join.  
With MMCH, there should only be one conference available to select.
4. The user must now use the PC's GUI to begin application sharing. The method for beginning application sharing or file transfer is different for each H.320 multimedia application.  
One of the H.320 DVC systems activates data sharing from the H.320 DVC vendor provided GUI. See your H.320 DVC system documentation for details.
5. The same H.320 DVC system as in step 4, opens an application, whiteboard, etc. to share and the image of the application is displayed on all H.320 DVC systems in the conference.  
For details on how multiple users can control the shared application, see the vendor provided documentation for your specific H.320 DVC system.
6. To end the data collaboration session and retain the voice/video conference, the station that selected the **mm-datacnf** button or FAC can press the **mm-datacnf** button or press Transfer and dial the mm-datacnf deactivation FAC.

 **Note:**

Currently, many endpoints do not respond correctly to ending the data collaboration session and retaining voice/video. Some H.320 DVC systems drop the entire call. Avaya recommends that once T.120 data sharing has been enabled for a conference, that it remain active for the duration of the conference

call. When all endpoints have dropped from the call, the T.120 resources will be released.

---

### Single server or switch data collaboration

When all parties involved in data collaboration conference are located on the same physical Avaya S8XXX Server, there is no restriction on the type of user. The parties can be any combination of Enhanced multimedia complexes, Basic multimedia complexes or stand-alone H.320 DVC systems.

### Multi-switch data collaboration

When all parties involved in data collaboration conference are not located on the same physical Avaya S8XXX Server, the parties located on the Avaya server hosting the data conference (i.e. the server which activated **mm-datacnf**) can be any combination of Enhanced multimedia complexes, Basic multimedia complexes or stand-alone H.320 DVC systems.



**Note:**

All parties on remote servers must not be Enhanced multimedia complexes: they must be Basic multimedia complexes or stand-alone H.320 DVC systems.

Prior to originating or receiving a multimedia mode call, the **mm-basic** feature button or feature access code can be used to dynamically change an Enhanced mode complex into a Basic mode complex and back again.

### Voice station audio vs. H.320 DVC system audio

When an Enhanced mode complex originates or receives a voice or multimedia call, the call is originated with the station handset or answered with the station handset. The audio path will be through the handset. If the user's H.320 DVC system has speakers and a microphone, the user might wish to use the H.320 DVC system for audio in much the same manner as a built-in or separate telephone speakerphone. The user can move the station's audio to the H.320 DVC system by selecting an **mm-pcaudio** feature button on the voice station. There is no feature access code for this function.

The **mm-pcaudio** feature button works very much like a speakerphone on/off button. If the station is off-hook and selects **mm-pcaudio**, audio is directed to the PC DVC system. The switch-hook can be placed on-hook. If the handset is taken off-hook, the audio moves back to the handset. If the **mm-pcaudio** button is selected while audio is already on the DVC system and the handset is on-hook, this acts as a speakerphone off action and disconnects the current call.

The **mm-pcaudio** feature button can be used for voice as well as multimedia calls. If the **mm-pcaudio** feature button is selected while on a voice only call, the DVC system is alerted and brought into the call. No video will be transmitted or displayed. Audio will be directed through the PC DVC system.

### Switching between Basic and Enhanced modes

There might be occasions when an Enhanced mode complex needs to switch to Basic mode operation temporarily. One example is when a user wishes to make a direct point to point multimedia call originated directly from the H.320 DVC. Basic mode operation allows this functionality at the expense of losing multimedia call handling capabilities (i.e. hold/xfer/conf). To switch from Enhanced mode to Basic mode, the station can either select a **mm-**

**basic** feature button or dial the mm-basic feature access code. Both of these actions are valid only if the Enhanced mode station has no multimedia calls active.

When in Basic mode, the status lamp for the mm-basic button, if present, will be on solid. The **mm-basic** feature button acts as a toggle. If the status lamp is on, when the button is selected, the lamp will go off and the station will return to Enhanced mode. The mm-enhanced feature access code will set the state of the station back to Enhanced. Switching to Enhanced mode is only valid if the associated H.320 DVC system is idle.

 **Note:**

Toggleing between Basic and Enhanced mode changes the station's administered Multimedia mode. When in Basic mode this field on the Station screen will show basic. When in Enhanced mode this field on the Station screen will show enhanced. The current station Multimedia mode will be saved to translation when a `save translation` command is executed.

### Forwarding of voice and multimedia calls

The Enhanced multimedia mode complex voice station can use the existing standard call forwarding mechanisms to activate forwarding for voice calls. If the forwarding destination is on the same server, then this will also forward multimedia calls as multimedia calls to the destination. If the forwarding destination is off-switch, multimedia calls will forward off-switch as voice-only calls. This is appropriate when the user will be at a location that is not able to receive multimedia calls.

To forward multimedia calls off-switch as multimedia calls, the user must activate multimedia call forwarding. This can be done with an **mm-cfwd** button or feature access code. The user can also activate standard voice call forwarding and select the **mm-call** button prior to entering the forwarding address.

### Coverage

Multimedia calls to an Enhanced mode complex are subject to the same coverage criteria as voice calls and follow the coverage path administered for the voice Station of the Enhanced multimedia mode complex.

If a plain voice station or a Basic mode complex is the covering party, the answering voice station will receive audio only. If all voice stations in the coverage path have the Station screen **Early Answer** field set to n and the originator of the multimedia call was not a local Enhanced mode complex, the answering station will hear hourglass tone.

If an Enhanced mode complex is the covering party, the answering voice station will receive voice and video. If all voice stations in the coverage path have the Station screen Early Answer field set to n and the originator of the multimedia call was not a local Enhanced mode complex, the answering station will hear hourglass tone.

ForwardingVoiceMultimediaCalls2.dita

### Multimedia calls and off-net call coverage

If the principal station's coverage path include a remote coverage point, the multimedia call will cover off-switch as voice only. If the call is unanswered off-switch and proceeds to the next coverage point on-switch, the multimedia nature of the call is preserved.

## Multimedia calls and coverage to voice mail

Voice mail systems such as AUDIX are typically the last point in a coverage path and are usually implemented as a hunt group. In order to guarantee that the originator of an H.320 multimedia call hears the voice mail greeting, the hunt group that defines the list of voice mail ports should have the **Early Answer** field on the Hunt Group screen set to y. This field will have no effect on voice calls to the voice mail system.

## Hunt Groups using Enhanced Mode Complexes

When creating hunt groups with Enhanced multimedia mode complexes, only the station extension should ever be entered as a hunt group member. Any hunt group or ACD skill can include the voice station of an Enhanced multimedia complex as a member. The data extension of an Enhanced mode complex should never be entered as any hunt group member. A hunt group or skill might have a mix of members that are stand-alone stations and Enhanced mode complex stations. In order to guarantee that all members of the hunt group or skill can receive voice or multimedia calls, all members should have the **H.320** field on the Station screen set to y. Simple voice stations will receive voice only. Enhanced mode stations will receive voice and video

The **MM Early Answer** field on the Hunt Group screen tells the system to answer an incoming multimedia call and establish audio before it reaches the first member of the hunt group. Thus, when the talk path is established, the caller is able to speak with an agent immediately.

## Other considerations

CMS measurements can indicate unusually slow ASA, because of the time required for the system to establish early-answer before offering the call to an agent.

### Call association (routing)

Typically incoming voice calls consist of 2 B-channel calls to the same address, to provide greater bandwidth and better video resolution. Communication Manager attempts to correctly pair up incoming calls and offer them as a unit to a single agent. MMCH uses call association to route both calls to the extension that answered the first call, regardless of how the call was routed internally.

Two 56K/64K data calls with the same calling party number to the same destination number are considered to be associated. The system makes every attempt to route both calls of a 2-channel call to the same answering party. If the first call terminates at a member of a hunt group, the second call does not have to hunt, but goes directly to the same member.

In order for 2B multimedia calls to be correctly given to a single agent, incoming calls to the hunt group must have ANI information. The ANI information can be in the form of ISDN calling party number or DCS calling party number. Multimedia calls made on the same server as the hunt group are easily associated. If multimedia calls into a hunt group have insufficient ANI information (i.e. all calls from server X to sever Y include the LDN for server X), then as the volume of calls increases the number of mis-associated calls will increase. If multimedia calls into a hunt group have no ANI information, Communication Manager will never associate pairs of calls and all calls will be treated independently and routed to separate agents. This is not a recommended configuration.

## Multimedia vectors

Very often, calls are routed to hunt groups or skills via a vector. The existing VDNs and vectors which exist for routing voice calls can be used to route multimedia calls.

In order to use a vector for multimedia calls, you must set the **Multimedia** field on the Call Vector screen to y. This field has no effect on voice calls routing through the vector. This field will cause multimedia calls routed through the vector to receive early answer treatment prior to processing the vector steps. This provides a talk path to the caller for announcements or immediate conversation with an agent.

 **Note:**

Vectors which have the **Multimedia** field set must eventually route to hunt groups, skills or numbers which are voice extensions. A vector with the **Multimedia** field set to y should never be set up to route to a hunt group or number which is a data extension

## Interactions

Interactions are listed here only if the operation is different from standard.

### Administered Connections

An Enhanced multimedia complex voice station can serve as the origination point or destination of an administered connection. If the Multimedia call feature access code is included in the administration of the administered connection, this will result in a video AC.

An Enhanced multimedia complex H.320 DVC system cannot serve as the origination point of an administered connection.

### X-porting

You cannot use X in the **Port** field when administering a data module or the data endpoint in a multimedia complex. However, you can use this to administer the telephone.

### Bridged Appearances

Enhanced multimedia complex voice station users can bridge onto a call if the user has a bridged appearance. If the bridged appearance is for a multimedia call, selecting the bridged appearance will result in a multimedia call.

### Call Detail Recording

Each channel of a 2-channel multimedia call generates a separate CDR record that is tagged as data.

### Call forwarding

Users cannot forward calls from a multimedia complex using multi-number dialing, either by mm-multnbr button or feature access code.

### Call Park

Any station can park a multimedia call, and unpark the call from another telephone. If a multimedia call is unparked by an Enhanced mode complex station, a multimedia call will result. Users cannot park or unpark calls using multimedia endpoints.

### Call Pickup

Any member of a pickup group can answer a multimedia call after the call has begun alerting at a station call appearance. If the station picking up the call is an Enhanced mode complex station and the call is multimedia, a multimedia call will result. This is true for standard or directed call pickup.

## **Consult**

After a multimedia call has been answered, consult can be used when transferring or conferencing the call.

## **COR/COS**

The Class of Restriction and Class of Service for a multimedia call originated from an Enhanced multimedia complex are those of the voice station in the complex.

## **Data Call Setup**

An Enhanced mode multimedia H.320 DVC system cannot originate calls from the DVC system. All calls, both voice or video are originated from the voice station.

## **Data Hotline**

An Enhanced multimedia complex H.320 DVC endpoint cannot be used to originate a call for hotline dialing. In order to setup a video hotline function with an Enhanced mode complex, the hotline number administered for the voice station should include the Multimedia call feature access code.

## **Data Trunk Groups**

Data trunk groups can be used to carry H.320 calls of a fixed (administered) bearer capability.

## **ISDN Trunk Groups**

Avaya highly recommends that you use ISDN trunks for multimedia calls. ISDN PRI trunks allow complete 1-number access for an Enhanced multimedia complex. ANI provided over PRI trunks allows correct routing of multiple bearer channels to the correct destination device. ISDN also provides the bearer capability on a call by call basis that can be used to distinguish voice calls from multimedia calls.

## **Night Service**

Incoming H.320 calls follow established night-service processing for data calls.

## **Remote Access**

Communication Manager does not prevent Enhanced multimedia complexes from attempting to use remote access. However, these endpoints will most likely not be able to dial the necessary codes.

## **Station Hunting**

Multimedia calls to Enhanced mode complex voice stations that have an extension administered in the hunt-to-station field hunt based on established hunting criteria. If the hunt-to-station is also an Enhanced mode complex station, a multimedia call will result when the call is answered.

## **Terminating Extension Groups**

A multimedia call to a TEG can be answered by any member of the TEG. If the member answering the call is an Enhanced mode complex station, a multimedia call will result.

## **Telephone Display**

Display information for calls to or from an Enhanced multimedia complex contains the display information associated with the voice station.

## Troubleshooting

If one channel of a 2 B-channel call goes down, your choices are to continue with reduced transmission quality, or to hang up the call and start over. It is not possible to re-establish the second channel while the call is still active.

If you cannot share data with others, it might be that both parties do not have the same endpoint software. This is true for some data collaboration, but most whiteboard and file transfer software implementations are compatible.

## Monitoring MMCH

This section briefly discusses some of the commands you can use to monitor multimedia complexes and conferences. The Maintenance manual for your Avaya server might discuss some of these commands and their output in more detail.

| Action  | Objects   | Qualifier   |
|---------|---|---|
| display | station data module   | xxxxx (extension)<br>xxxxx (extension)  |
| list    | mmi measurements<br>multimedia  | multimedia-interface voice-conditioner<br>esm<br>endpoints ['print' or 'schedule'] h.320-<br>stations ['print' or 'schedule']   |
| status  | attendant<br>conference<br>conference<br>conference<br>data module<br>station<br>trunk<br>esm | xxxx (console number)<br>all<br>xxx (conference ID)<br>xxx (conference ID) endpoint (endpoint ID)<br>xxxxx (extension)<br>xxxxx (extension)<br>(group number or group number/ member<br>number) |

## Status commands

The `status` commands for data module, station, trunk, and attendant provide the conference ID and endpoint ID for any of these involved in an active multimedia conference.

The following fields specific to multimedia appear on the station General Status, Attendant, Data Module, and Trunk Group screens.

- **MM Conference ID** — This field appears only if the station is active on a multimedia conference. It displays the ID for the conference. Enter this number with the status conference command to get more information about this conference.
- **MM Endpoint ID** — This field appears only if the station is active on a multimedia conference. It displays the endpoint ID for the station. Enter this number with the status conference endpoint command to learn more about this endpoint's involvement in the conference.

## List commands

The `list multimedia endpoints` command shows you all the multimedia data modules that exist in your system, and their associated telephones, if any. The `list multimedia H.320-stations` command shows you all the stations that are administered for H.320 conversion.

The list multimedia `ip-stations` command shows you the administered IP stations/modules and whether they are registered.

**Considerations**

Each channel of a 2-channel BRI call takes one port on an MMI circuit pack. This alone limits the number of multimedia calls your system can handle. In addition, each conference takes one port on a voice-conditioner circuit pack. Also note that there is a limit to the total number of conversion calls the system can handle simultaneously. If you experience traffic problems after installing multimedia, you might want to reduce the number of stations that use H.320 conversion.

**Screen References**

**AAR and ARS Digit Analysis Table**

**AAR and ARS Digit Analysis Table**

Avaya Communication Manager compares dialed numbers with the dialed strings in this table and determines the route pattern for the number.

Example command:

- `change aar analysis n`
- `change ars analysis n`

**ANI Reqd**

Available only if **Request Incoming ANI (non-AAR/ARS)** is disabled for Multifrequency Signaling.

| Valid Entry | Usage  |
|-------------|--|
| y           | ANI is required on incoming R2-MFC or Russian MF ANI calls.  |
| n           | ANI is <i>not</i> required on R2-MFC or Russian MF ANI calls.  |
| r           | Drop a call on a Russian Shuttle trunk or Russian Rotary trunk if the ANI request fails.<br>Available only if <b>Allow ANI Restriction on AAR/ARS</b> is enabled for the system. |

**Related topics:**

- [Allow ANI Restriction on AAR/ARS](#) on page 591
- [Request Incoming ANI \(non-AAR/ARS\)](#) on page 795

**Call Type (AAR only)**

This field indicates the call type associated with each dialed string. Call types indicate numbering requirements on different trunk networks.

| Valid Entry | Usage  |
|-------------|--|
| aar         | Regular AAR calls  |
| intl        | The Route Index contains public network ISDN trunks that require international type of number encodings  |
| pubu        | The Route Index contains public network ISDN trunks that require unknown type of number encodings  |
| lev0–lev2   | ISDN Private Numbering Plan (PNP) number formats   |
| unku        | Sets up an Implicit (Unknown) Numbering Plan, in which users dial each other by extension without an ARS or AAR Access Code. For example, “9” or “8”. These extensions are optionally preceded by a node number. |

## ISDN Protocol:

| Call Type Numbering | Numbering Plan Identifier | Type of Numbering   |
|---------------------|---------------------------|---------------------|
| aar                 | E.164 (1)                 | national(2)         |
| intl                | E.164 (1)                 | international(1)    |
| pubu                | E.164 (1)                 | unknown(0)          |
| lev0                | PNP(9)                    | local(4)            |
| lev1                | PNP(9)                    | Regional Level 1(2) |
| lev2                | PNP(9)                    | Regional Level 2(1) |

**Call Type (ARS only)**

| Valid Entry | Usage  | China Number 1, Call Type |
|-------------|--|---------------------------|
| alrt        | Alerts attendant consoles or other digital telephones when an emergency call is placed | normal                    |
| emer        | Emergency call   | normal                    |
| fnpa        | Ten-digit North American Numbering Plan (NANP) call (11 digits with Prefix Digit “1”)  | attendant                 |
| hpna        | Seven-digit NANP call  | normal                    |
| intl        | Public-network international number  | toll-auto                 |
| lop         | International operator   | attendant                 |
| locl        | Public-network local number  | normal                    |
| lpvt        | Local private  | normal                    |
| natl        | Non-NANP   | normal                    |
| npvt        | National private   | normal                    |
| nsvc        | National service   | normal                    |

| Valid Entry | Usage                                 | China Number 1, Call Type |
|-------------|---------------------------------------|---------------------------|
| op          | Operator                              | attendant                 |
| pubu        | Public-network number (E.164)-unknown | normal                    |
| svcl        | National(2)                           | toll-auto                 |
| svct        | National(2)                           | normal                    |
| svfl        | Service call, first party control     | toll                      |
| svft        | Service call, first party control     | local                     |

**Dialed String**

Dialed numbers are matched to the dialed string entry that most closely matches the dialed number. For example, if 297-1234 is dialed and the table has dialed string entries of 297-1 and 297-123, the match is on the 297-123 entry.

An exact match is made on a user-dialed number and dialed string entries with wildcard characters and an equal number of digits. For example, if 424 is dialed, and there is a 424 entry and an X24 entry, the match is on the 424 entry.

Accepts up to 18 digits that the call-processing server analyzes. Also accepts x and X wildcard characters.

**Location**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 250    | (Depending on your server configuration, see <i>Avaya Aura™ Communication Manager System Capacities Table</i> , 03-300511.) The location of the endpoint that is dialing the digits. Available only if <b>Multiple Locations</b> is enabled for the system. See the Location sections in <i>Avaya Aura™ Communication Manager Feature Description and Implementation</i> , 555-245-205, for the other ways, and for a list of features that use location. |
| all         | Indicates that this table is the default for all port network (cabinet) locations. Available only if <b>Multiple Locations</b> is disabled for the system.  |

**Related topics:**

[Multiple Locations](#) on page 948

**Max**

The maximum number of user-dialed digits the system collects to match to the dialed string.

**Min**

The minimum number of user-dialed digits the system collects to match to the dialed string.

**Node Number**

| Valid Entry       | Usage   |
|-------------------|---|
| 1 to 999<br>blank | The number of the destination node in a private network when using node number routing or Distributed Communication System (DCS). |

**Percent Full**

| Value    | Comments  |
|----------|---|
| 0 to 100 | The percentage of system memory resources that have been used by the table. |

**Route Pattern**

The route number that the server running Communication Manager uses for this dialed string.

| Valid Entry                                 | Usage   |
|---|---|
| p1 to p2000                                 | The route index number established on the Partition Routing Table   |
| 1 to 640<br>1 to 999 — for<br>S8300 servers | The route pattern used to route the call  |
| r1 to r32                                   | The remote home-numbering plan area table. Used if RHNPA translations are required for the corresponding dialed string. |
| node  | Designates node number routing  |
| deny  | Blocks the call   |

**AAR and ARS Digit Conversion Table****AAR and ARS Digit Conversion Table**

The AAR or ARS Digit Conversion Table is used to change a dialed number for more efficient routing. Digits can be inserted or deleted from the dialed number. For instance, administrators can tell the server running Communication Manager to delete a 1 and an area code on calls to one of their locations, and avoid long-distance charges by routing the call over the private network.

Example command:

- `change aar digit-conversion`
- `change ars digit-conversion`

**ANI Req'd**

Available only if **Request Incoming ANI (non-AAR/ARS)** is disabled for Multifrequency Signaling.

| Valid Entry | Usage  |
|-------------|--|
| y           | ANI is required on incoming R2-MFC or Russian MF ANI calls.  |
| n           | ANI is <i>not</i> required on R2-MFC or Russian MF ANI calls.  |
| r           | Drop a call on a Russian Shuttle trunk or Russian Rotary trunk if the ANI request fails.<br>Available only if <b>Allow ANI Restriction on AAR/ARS</b> is enabled for the system. |

**Related topics:**

[Allow ANI Restriction on AAR/ARS](#) on page 591

[Request Incoming ANI \(non-AAR/ARS\)](#) on page 795

**Conv**

Allows or prohibits additional digit conversion.

**Del**

Number of digits the system deletes from the beginning of the dialed string.

**Location**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 250    | (Depending on your server configuration, see <i>Avaya Aura™ Communication Manager System Capacities Table</i> , 03-300511.) The location of the endpoint that is dialing the digits. Available only if <b>Multiple Locations</b> is enabled for the system. See the Location sections in <i>Avaya Aura™ Communication Manager Feature Description and Implementation</i> , 555-245-205, for the other ways, and for a list of features that use location. |
| all         | Indicates that this table is the default for all port network (cabinet) locations. Available only if <b>Multiple Locations</b> is disabled for the system.  |

**Related topics:**

[Multiple Locations](#) on page 948

**Matching Pattern**

The number that the server running Communication Manager uses to match dialed numbers. Accepts up to 18 digits and the x and X wildcard characters.

**Max**

The maximum number of user-dialed digits the system collects to match to the dialed string.

**Min**

The minimum number of user-dialed digits the system collects to match to the dialed string.

**Net**

The call-processing server network uses the following methods to analyze the converted number.

| Valid Entry | Usage  |
|-------------|--|
| ext         | Analyzes the converted digit-string as an extension number |
| aar         | Analyzes the converted digit-string as an AAR address      |
| ars         | Analyzes the converted digit-string as an ARS address      |

**Percent Full**

| Value    | Comments  |
|----------|---|
| 0 to 100 | The percentage of system memory resources that have been used by the table. |

**Replacement String**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9, *   | The digits that replace the deleted portion of the dialed number. Accepts up to 18 digits. |
| #           | Indicates end-of-dialing used at the end of the digit string.                              |
| blank       | Deletes the digits without replacement.  |

**Abbreviated Dialing****Abbreviated Dialing Enhanced List**

Establishes system-wide or personal lists for speed dialing.

The Enhanced Abbreviated Dialing List can be accessed by users to place local, long-distance, and international calls; to activate or deactivate features; or to access remote computer equipment.

 **Note:**

Dialing must be enabled in the license file before the Enhanced List can be programmed.

Example command: `display abbreviated-dialing enhanced`

**Related topics:**

[Abbreviated Dialing Enhanced List](#) on page 942

**DIAL CODE**

| Valid Entry   | Usage   |
|---------------|---|
| Digits 0 to 9 | The number the system dials when users enter this dial code. While the system is waiting, a call progress tone receiver is tied up, and since there are a limited number of receivers in the system, outgoing calling capability might be impaired.<br>A Vector Directory Number extension can also be assigned. Accepts up to 24 characters. |
| * (star)      | Part of FAC   |
| # (pound)     | Part of FAC   |
| ~p            | Pause 1.5 seconds   |
| ~w            | Wait for dial tone  |
| ~m            | Change to outpulse DTMF digits at the end-to-end rate   |
| ~s            | Start suppressing display of the digits being outpulsed   |
| ~W            | Wait indefinitely for dial tone. Use this only if network response time is more than 30 seconds. Not available for some S8300 servers.  |

**Privileged**

Allows or denies users permission to dial any number in the list, regardless of their station class of restriction (COR).

**Size (multiple of 5)**

| Valid Entry         | Usage   |
|---------------------|---|
| 5, 10, 15, ..., 100 | The number of dial code list entries wanted in the list. Allows up to 100 entries per screen. |

Example command: `add abbreviated-dialing system`

**Group List**

Implements the Abbreviated Dialing Group List. The System Administrator controls the Group Lists. Up to 100 numbers can be entered for every group list. Users can access this list to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Example command: `change abbreviated-dialing group`

**DIAL CODE**

| Valid Entry   | Usage   |
|---------------|---|
| Digits 0 to 9 | The number the system dials when users enter this dial code. While the system is waiting, a call progress tone receiver is tied up, and since there |

| Valid Entry | Usage   |
|-------------|---|
|             | are a limited number of receivers in the system, outgoing calling capability might be impaired.<br>A Vector Directory Number extension can also be assigned. Accepts up to 24 characters. |
| * (star)    | Part of FAC   |
| # (pound)   | Part of FAC   |
| ~p          | Pause 1.5 seconds   |
| ~w          | Wait for dial tone  |
| ~m          | Change to output pulse DTMF digits at the end-to-end rate   |
| ~s          | Start suppressing display of the digits being outputted   |
| ~W          | Wait indefinitely for dial tone. Use this only if network response time is more than 30 seconds. Not available for some S8300 servers.  |

**Group List**

The number assigned to the group list.

**Privileged**

Allows or denies users permission to dial any number in the list, regardless of their station class of restriction (COR).

**Program Ext**

The extension that has permission to program the Group List.

**Size (multiple of 5)**

| Valid Entry         | Usage   |
|---------------------|---|
| 5, 10, 15, ..., 100 | The number of dial code list entries wanted in the list. Allows up to 100 entries per screen. |

Example command: `add abbreviated-dialing system`

**Personal List**

Establishes a personal dialing list for telephone or data module users. The personal list must first be assigned to the telephone by the System Administrator before the telephone user can add entries in the list. Users access the lists in order to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Example command: `change abbreviated-dialing personal`

**DIAL CODE**

| Valid Entry   | Usage   |
|---------------|---|
| Digits 0 to 9 | The number the system dials when users enter this dial code. While the system is waiting, a call progress tone receiver is tied up, and since there are a limited number of receivers in the system, outgoing calling capability might be impaired.<br>A Vector Directory Number extension can also be assigned. Accepts up to 24 characters. |
| * (star)      | Part of FAC   |
| # (pound)     | Part of FAC   |
| ~p            | Pause 1.5 seconds   |
| ~w            | Wait for dial tone  |
| ~m            | Change to outpulse DTMF digits at the end-to-end rate   |
| ~s            | Start suppressing display of the digits being outpulsed   |
| ~W            | Wait indefinitely for dial tone. Use this only if network response time is more than 30 seconds. Not available for some S8300 servers.  |

**List Number**

Indicates which of the three personal lists is defined for the telephone.

**Personal List**

The extension of the telephone using this list.

**Size (multiple of 5)**

| Valid Entry         | Usage   |
|---------------------|---|
| 5, 10, 15, ..., 100 | The number of dial code list entries wanted in the list. Allows up to 100 entries per screen. |

Example command: `add abbreviated-dialing system`

**System List**

Implements a system abbreviated-dialing list. Only one system list can be assigned and is administered by the System Administrator. Users access the list in order to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Example command: `add abbreviated-dialing system`

**DIAL CODE**

| Valid Entry   | Usage   |
|---------------|---|
| Digits 0 to 9 | The number the system dials when users enter this dial code. While the system is waiting, a call progress tone receiver is tied up, and since there are a limited number of receivers in the system, outgoing calling capability might be impaired.<br>A Vector Directory Number extension can also be assigned. Accepts up to 24 characters. |
| * (star)      | Part of FAC   |
| # (pound)     | Part of FAC   |
| ~p            | Pause 1.5 seconds   |
| ~w            | Wait for dial tone  |
| ~m            | Change to outpulse DTMF digits at the end-to-end rate   |
| ~s            | Start suppressing display of the digits being outpulsed   |
| ~W            | Wait indefinitely for dial tone. Use this only if network response time is more than 30 seconds. Not available for some S8300 servers.  |

**Label Language**

Provides administration of personalized labels on the 2420/4620 telephone sets. If this field is changed to another language, all administered labels in the original language are saved and the labels for the new language are read in and displayed.

| Valid Entry  | Usage  |
|--|--|
| English<br>Italian<br>French<br>Spanish<br>user-defined<br>Unicode | The appropriate language for the <b>2420/4620</b> labels.<br><br> <b>Note:</b><br>Unicode display is only available for Unicode-supported telephones. Currently, 4610SW, 4620SW, 4621SW, 4622SW, Sage, Spark, and 9600-series telephones (Avaya one-X Deskphone Edition SIP R2 or later) support Unicode display. Unicode is also an option for DP1020 (aka 2420J) and SP1020 (Toshiba SIP Phone) telephones when enabled for the system. |

**Related topics:**

[Display Character Set](#) on page 938

**LABELS FOR 2420/4620 STATIONS**

Provides the administrative capability to customize the labels for the system-wide Abbreviated Dial buttons on the 2420 and 4620 telephone sets. Accepts up to 15 alphanumeric characters.

**Privileged**

Allows or denies users permission to dial any number in the list, regardless of their station class of restriction (COR).

**Size (multiple of 5)**

| Valid Entry         | Usage   |
|---------------------|---|
| 5, 10, 15, ..., 100 | The number of dial code list entries wanted in the list. Allows up to 100 entries per screen. |

Example command: `add abbreviated-dialing system`

**7103A Button List**

Assigns abbreviated dialing numbers to the 7103A telephone buttons. The entries can then be accessed by 7103A telephone users to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Applies only to 7103A fixed feature telephones. Only one 7103A abbreviated dialing list can be implemented in the system and it applies to all 7103A fixed feature telephones in the system. This list is controlled by the System Administrator.

Example command: `display abbreviated-dialing 7103A-buttons`

**DIAL CODE**

The number to assign to each dial code button. Any additions or changes apply to all 7103A fixed feature telephones. While the system is waiting, a call progress tone receiver is tied up, and, since there are a limited number of receivers in the system, outgoing calling capability might be impaired.

A Vector Directory Number extension can also be assigned.

| Valid Entry   | Usage   |
|---------------|---|
| Digits 0 to 9 | The number the system dials when users enter this dial code. While the system is waiting, a call progress tone receiver is tied up, and since there are a limited number of receivers in the system, outgoing calling capability might be impaired.<br>A Vector Directory Number extension can also be assigned. Accepts up to 24 characters. |
| * (star)      | Part of FAC   |
| # (pound)     | Part of FAC   |
| ~p            | Pause 1.5 seconds   |
| ~w            | Wait for dial tone  |
| ~m            | Change to output pulse DTMF digits at the end-to-end rate   |
| ~s            | Start suppressing display of the digits being output pulsed   |
| ~W            | Wait indefinitely for dial tone. Use this only if network response time is more than 30 seconds. Not available for some S8300 servers.  |

## Access Endpoint

Administers Access Endpoints and Wideband Access endpoints. Wideband Access Endpoints can be administered only if **Wideband Switching** is enabled for the system.

An Access Endpoint is a non-signaling trunk that neither responds to signaling nor generates signaling. Access Endpoints eliminate the need to dedicate an entire trunk group for the access of a single trunk by providing the capability to assign an extension number to a single trunk.

An Access Endpoint can be specified as the Originator or Destination endpoint of an administered connection.

A Wideband Access Endpoint (WAE) is an endpoint application connected to line-side non-ISDN T1 or E1 facilities and, like Access Endpoints, have no signaling interface with the system.

The WAE is defined by a starting port (DS0) and a width specifying the number of adjacent nonsignaling DS0s (positioned within a DS1 facility) that make up the endpoint. This width can be between 2 and 31 adjacent DS0s.

### Note:

Access Endpoints and Wideband Access Endpoints consume the same resources that trunks use. Thus, the sum of Access Endpoints and trunks cannot exceed the maximum number of trunks available in your system configuration.

Example command: `add access-endpoint next`

### Related topics:

[Wideband Switching](#) on page 950

## Communication Type

| Valid Entry      | Usage   |
|------------------|---|
| voice-grade-data | An analog tie trunk access endpoint                       |
| 56k-data         | A DS1 access endpoint                                     |
| 64K-data         | A DS1 access endpoint — not allowed for robbed-bit trunks |
| wideband         | A wideband access endpoint                                |

## COR

| Valid Entry | Usage  |
|-------------|--|
| 0 to 995    | The class of restriction (COR) number assigned to the Access Endpoint. The COR must be administered so that only an administered connection (AC) endpoint can be connected to another AC endpoint. |

**COS**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 15     | The appropriate Class of Service (COS) number assigned to the Access Endpoint. The COS must be administered so that Call Forwarding All Calls for access endpoints is prohibited. |

**Extension**

The extension number assigned to the non-signaling trunk and used to access the trunk endpoint.

**ITC (Information Transfer Capability)**

Determines the type of transmission facilities used for ISDN calls originating from this endpoint. Available when the **Communication Type** is 56k-data, 64k-data, or Wideband.

- When adding an access endpoint with ITC administered as unrestricted, its associated port has to be a channel of a DS1 circuit pack with **Zero Code Suppression** administered as B8ZS.
- When adding an access endpoint with the ITC administered as restricted, its associated port can be a channel from a DS1 circuit pack with **Zero Code Suppression** administered as ZCS or B8ZS.
- For an existing access endpoint, ITC can be changed only from restricted to unrestricted if its associated port is a channel of a DS1 circuit pack with **Zero Code Suppression** administered as B8ZS.

| Valid Entry  | Usage   |
|--------------|---|
| unrestricted | Only unrestricted transmission facilities (b8zs) are used to complete the call. An unrestricted facility is a transmission facility that does not enforce 1's density digital transmission. In other words, digital information is sent exactly as is for Wideband Access Endpoints.  |
| restricted   | Either restricted (zcs-ami) or unrestricted transmission facilities are used to complete the call. A restricted facility is a transmission facility that enforces 1's density digital transmission. In other words, a sequence of eight digital zeros is converted to a sequence of seven zeros and a digital one using zcs coding on a DS1 circuit pack. |

**Name**

Name of the endpoint.

 **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**(Starting) Port**

| Valid Entry                              | Usage   |
|--|---|
| 01 to 64                                 | First and second characters are the cabinet number. |
| A to E                                   | Third character is the carrier.                     |
| 0 to 20                                  | Fourth and fifth characters are the slot number.    |
| 01 to 04 (Analog TIE trunks)<br>01 to 31 | Six and seventh characters are the circuit number.  |
| 1 to 250                                 | Gateway   |
| V1 to V9                                 | Module  |
| 01 to 31                                 | Circuit   |

For example, 01A0612 is in cabinet 01, carrier A, slot 06, and circuit number (port) 12.

 **Note:**

For Wideband Access Endpoints, analog tie trunks cannot be used and the DS1 Interface circuit pack, Version C or later, must be used.

The DS1 circuit number corresponds to the channel that will carry the data traffic. Channels 1 through 31 (DS1 Interface only) or channels 1 through 24 (DS1 Tie Trunk, DS1 Interface, or DS1 Interface (32) circuit packs can be used when the DS1 circuit board is administered with a robbed-bit or isdn-ext. For Common Channel or ISDN-PRI signaling, channel use is limited to channels 1 through 30 (DS1 Interface circuit pack only) or channels 1 through 23 (DS1 Interface (32) or DS1 Interface). A channel can be administered as an access endpoint regardless of the DS1 signaling type.

**Related topics:**

[Signaling Mode](#) on page 550

**TN**

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

**Width**

Required if the **Communication Type** is wideband.

| Valid Entry | Usage   |
|-------------|---|
| 2 to 31     | The number of adjacent DS0 ports beginning with the specified Starting Port, that make up the WAE |
| 6           | Defines a 384 Kbps WAE  |

**Related topics:**

[Communication Type](#) on page 429

## Administered Connection

Assigns an end-to-end Administered Connection (AC) between two access endpoints or data endpoints. The AC is established automatically by the system whenever the system restarts or the AC is due to be active.

Example command: `change administered-connection`

### Connection Number

The Administered Connection (AC) number.

### Destination

The address of the destination access or data endpoint. This endpoint is the terminating party of the AC and need not be local to the server on which the AC is assigned. The entry must be consistent with the local Communication Manager server's dial plan (that is, the first digits are assigned as an extension, feature access code, or trunk access code, or DDD Number). If a local extension is entered, it must be assigned to either an access or data endpoint. Abbreviated Dialing entries can be used in this field.

### Enable

| Valid Entry | Usage   |
|-------------|---|
| y           | An attempt is made to establish the AC when the AC is due to be active. |
| n           | The AC is not made, or the connection drops if currently active.        |

### Name

A short identification of the AC. Accepts up to 27 alphanumeric characters.

 **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

### Originator

The assigned access endpoint extension or data module extension.

Data Line circuit pack

Asynchronous EIA 232C compatible equipment

Digital Line circuit pack connections, including:

- MPDM (700D), MTDM (700B, 700C, 700E), 7400D data module
- 7400A, 7400B, 7400C HSL, 8400B data module
- 7401D telephone with 7400B or 8400B data module

- 7403D/7405D/7407D/7410D/7434D telephone with DTDM or 7400B or 8400B data module
- 7404D or 7406D telephone
- 510D personal terminal
- 515 BCT, 615 BCT, or 715 BCT terminal
- Connection between PC and the server running Communication Manager

ISDN-BRI Line circuit pack connections, including:

- 7500 data module
- 7505D/7506D/7507D telephone with ADM

The endpoint must be local to the server on which the AC is administered. Nonsignaling DS1 trunk or analog tie trunk.

## AUTHORIZED TIME OF DAY

### *Continuous*

| Valid Entry | Usage   |
|-------------|---|
| y           | The AC is scheduled to always be active. The connection is up all the time or re-established if the connection goes down. |
| n           | The AC attempts to activate during scheduled start days and times.  |

### Related topics:

[Start Days \(Sun through Sat\)](#) on page 433

[Start Time](#) on page 434

### *Duration*

The period of time that the scheduled AC remains active. The maximum duration is 167 hours and 59 minutes. In other words, 1 minute less than 1 week. Only required for a noncontinuous connection.

| Valid Entry     | Usage   |
|-----------------|---------|
| 000 through 167 | Hours   |
| 00 through 59   | Minutes |

### *Start Days (Sun through Sat)*

The days when an attempt is made to establish the AC. This is not necessarily the days it is active. A scheduled AC might be active over a number of days. In this situation, these fields should be used only to specify the days when the AC starts and not other days when the AC might be active. Only required for a noncontinuous connection.

| Valid Entry | Usage  |
|-------------|--|
| y           | The required days of the week that an attempt is made to establish the AC. |
| n           | Displays the start day fields.   |

**Start Time**

Available only if **Continuous** is not active.

| Valid Entry         | Usage   |
|---------------------|---|
| 00:00 through 23:59 | The time of the day when an attempt should begin to establish a scheduled AC. |

**Related topics:**

[Continuous](#) on page 433

**MISCELLANEOUS PARAMETERS**

**Alarm Threshold**

Available only if **Alarm Type** is specified.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 10     | The number of times an attempt to establish or reestablish an AC must fail consecutively before an AC alarm generates. (An alarm is generated after the fourth retry has failed; thus, with the retry interval of 2 minutes, an alarm is generated approximately 8 minutes after the first failure occurs.) An alarm generates on the first failure if this field is 1. |

**Related topics:**

[Alarm Type](#) on page 434

**Alarm Type**

The type of alarm generated if the AC cannot be initially established, or fails and cannot be reestablished, and the number of consecutive failures that equal the alarm threshold. All AC alarms and the errors that caused the alarms are recorded in the system’s alarm and error log. In addition, a status lamp associated with an attendant console or telephone feature button can be used to indicate the AC alarm.

| Valid Entry | Usage  |
|-------------|--|
| major       | Failures that cause critical degradation of service and require immediate attention.   |
| minor       | Failures that cause some degradation of service, but do not render a crucial portion of the system inoperable. This condition requires action, but its consequences are not immediate. Problems might be impairing service to a few trunks or stations or interfering with one feature across the entire system. |

| Valid Entry | Usage   |
|-------------|---|
| warning     | Failures that cause no significant degradation of service or failures in equipment external to the system. Warning alarms are not reported to the attendant console or INADS. |
| none        | The alarm notification is disabled for this AC.   |

### Auto Restoration

| Valid Entry | Usage  |
|-------------|--|
| y           | An attempt is to be made to reestablish an AC that failed. Auto restoration is available only for an AC that is established over an ISDN Software Defined Data Network (SDDN) trunk group. |
| n           | An attempt is <i>not</i> made to reestablish an AC that failed.  |

### Priority

| Valid Entry | Usage   |
|-------------|---|
| 1 to 8      | The order in which ACs are established. 1 is the highest and 8 the lowest priority. |

### Retry Interval

| Valid Entry | Usage  |
|-------------|--|
| 1 to 60     | The number of minutes between attempts to establish or reestablish the AC. |

## Agent Login ID

In an Expert Agent Selection (EAS) environment, adds or changes agent login IDs and skill assignments. If skills are added or changed on the media server, the agent must log out and then log in again before the changes take effect.

Example command: `add agent-loginID n`, where *n* is the agent login ID.

### Agent Login ID: page 1

#### AAS

| Valid Entry | Usage   |
|-------------|---|
| y           | This extension is used as a part for an Auto Available Split/Skill. Clears the password and requires that the agent be removed. |
| n           | This extension is used for switch adjunct equipment ports only, not human agents. This is the default.                          |

**ACW Agent Considered Idle**

| Valid Entry | Usage   |
|-------------|---|
| y           | Agents who are in After Call Work are included in the Most-Idle Agent queue. This means that ACW is counted as idle time. |
| n           | Exclude ACW agents from the Most-Idle Agent queue.  |
| system      | System-wide values apply.   |

**Related topics:**

[ACW Agents Considered Idle](#) on page 615

**AUDIX**

Sets up or removes this extension as a port for voice messaging. An extension that is used for an Auto Available Split/Skill cannot be used as a voice messaging port.

**Audix Name for Messaging**

- The name of the messaging system used for LWC Reception.
- The name of the messaging system that provides coverage for this Agent LoginID.

**Auto Answer**

When using EAS, the agent's auto answer setting applies to the station where the agent logs in. If the auto answer setting for that station is different, this setting overrides the station setting.

| Valid Entry | Usage   |
|-------------|---|
| all         | Immediately sends all ACD and non ACD calls to the agent. The station is also given a single ring while a non-ACD call is connected. The <b>ringer-off</b> button can be used to prevent the ring when enabled on the system. |
| acd         | Only ACD split /skill calls and direct agent calls go to auto answer. Non ACD calls terminated to the agent ring audibly.   |
| none        | All calls terminated to this agent receive an audible ringing treatment. This is the default.   |
| station     | Auto answer for the agent is controlled by the auto answer parameters on the station screen.  |

**Related topics:**

[Auto Answer](#) on page 61

[Allow Ringer-off with Auto-Answer](#) on page 619

**Aux Work Reason Code Type**

| Valid Entry | Usage   |
|-------------|---|
| system      | System-wide settings apply. This is the default.              |
| none        | An agent does not enter a Reason Code when entering AUX work. |

| Valid Entry | Usage  |
|-------------|--|
| requested   | An agent can enter a Reason Code when entering AUX mode but is not forced to do so. <b>Reason Codes</b> must be enabled on the system. |
| forced      | An agent must enter a Reason Code when entering AUX mode. <b>Reason Codes</b> must be enabled on the system.                           |

**Related topics:**

[Aux Work Reason Code Type](#) on page 621

[Reason Codes](#) on page 952

**COR**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 995    | The Class of Restriction (COR) for the agent. The default value is 1. |

**Coverage Path**

The number of the coverage path used by calls to the LoginID. The coverage path is used when the agent is logged out, does not answer, or is busy to personal calls when logged in.

| Valid Entry       | Usage                    |
|-------------------|--------------------------|
| 1 to 199, blank   | Path number              |
| t1 to t999, blank | Time-of-day table number |

**Direct Agents Calls First**

Available when percent-allocation is specified.

| Valid Entry | Usage   |
|-------------|---|
| y           | Direct agent calls override the percent-allocation call selection method and deliver before other ACD calls |
| n           | Direct agent calls are treated like other ACD calls   |

**Related topics:**

[Call Handling Preference](#) on page 440

**Forced Agent Logout Time**

Administers a time of day to automatically log out agents for the Forced Agent Logout by Clock Time feature.

| Valid Entry        | Usage                         |
|--------------------|-------------------------------|
| 01 to 23           | Valid entries for the hour.   |
| 00, 15, 30, and 45 | Valid entries for the minute. |
| blank              | Default (not administered)    |

Examples: 15:00, 18:15, 20:30, 23:45.



**Note:**

**Forced Agent Logout Time** field in multi location environment works only if the **Timezone Offset** field is set with a 15 minutes increment.

**Related topics:**

[Timezone Offset](#) on page 772

**Login ID**

The identifier for the Logical Agent.

**LoginID for ISDN Display**

| Valid Entry | Usage  |
|-------------|--|
| y           | The Agent LoginID CPN (Calling Party Number) and <b>Name</b> are included in ISDN messaging over network facilities. |
| n           | Default. The calling party name and number are determined by the conditions administered for the trunk group.        |

**Related topics:**

[Name](#) on page 439

**Logout Reason Code Type**

| Valid Entry | Usage   |
|-------------|---|
| system      | Default value. System-wide settings apply.  |
| none        | Agents are prohibited from entering reason codes when logging out.  |
| requested   | Agents can optionally enter reason codes when logging out. Reason codes must be enabled on the system.                              |
| forced      | Agents are required to enter a reason code when logging out and when entering AUX mode. Reason codes must be enabled on the system. |

**Related topics:**

[Logout Reason Code Type](#) on page 622

[Reason Codes](#) on page 952

**LWC Reception**

Indicates where Leave Word Calling (LWC) messages are stored.

| Valid Entry | Usage  |
|-------------|--|
| audix       | LWC messages are stored on the voice messaging system. |
| none        | LWC messages are not be stored.                        |

| Valid Entry | Usage   |
|-------------|---|
| spe         | LWC messages are stored in the system or on the switch processor element (spe). |

**Related topics:**

[AUDIX Name](#) on page 662

**Maximum time agent in ACW before logout (sec)**

The maximum time the agent can be in ACW on a per agent basis.

| Valid Entry    | Usage  |
|----------------|--|
| system         | System-wide values apply. Default value.   |
| none           | ACW timeout does not apply to this agent   |
| 30 to 9999 sec | The number of seconds in a specific timeout period. This setting takes precedence over the system setting for maximum time in ACW. |

**Related topics:**

[Maximum Time Agent in ACW before Logout \(sec.\)](#) on page 623

**Messaging Server Name for Messaging**

- The name of the Messaging Server used for LWC Reception
- The name of the Messaging Server that provides coverage for this Agent LoginID
- Blank (not administered). This is the default

**MIA Across Skills**

| Valid Entry | Usage  |
|-------------|--|
| system      | The system-wide values apply. Default value.   |
| y           | Remove an agent from the MIA queues for all the splits or skills for which an agent is available when the agent answers a call from any assigned splits or skills. |
| n           | Exclude ACW agents for the queue.  |

**Related topics:**

[MIA Across Splits or Skills](#) on page 616

**Name**

The name of the agent. Accepts up to 27 alphanumeric characters.

**Note:**

Supported by Unicode language display for the 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones. Unicode is also an option for the 2420J

telephone when the **Display Character Set** is katakana. For more information on the 2420J, see *2420 Digital Telephone User's Guide*.

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Related topics:**

[Display Character Set](#) on page 938

**Password**

The password the agent enters upon login.

- The minimum number of digits allowed is specified by the **Minimum Agent-LoginID Password Length** field.
- The maximum number of digits allowed is nine digits.

Passwords can be administered only for extensions that are not used for a voice messaging system or for Auto Available Split/Skill.

**Related topics:**

[Minimum Agent-LoginID Password Length](#) on page 610

**Password (enter again)**

The same password exactly as it was entered. Default is blank.

**Port Extension**

The assigned extension for the AAS or a voice messaging port. This extension cannot be a Vector Directory Number (VDN) or an Agent LoginID. Default is blank.

**Security Code**

The four-digit security code (password) for the Demand Print messages feature.

**TN**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 20     | The partition number for tenant partitioning. Default value is 1. |

**Agent Login ID: page 2**

**Call Handling Preference**

Determines which call an agent receives next when calls are in queue.

| Valid Entry        | Usage  |
|--------------------|--|
| skill-level        | The oldest, highest priority call waiting for the highest-level agent skill.   |
| greatest-need      | The oldest, highest priority call waiting for any agent skill.   |
| percent-allocation | The call from a skill that deviates the most from its administered allocation. Percent-allocation is available only with Avaya Business Advocate software. |

**Direct Agent Skill**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 99     | The number of the skill used to handle Direct Agent calls. |
| blank       | Not administered. This is the default value.               |

**Local Call Preference**

Enables or disables Local Call Preference. For calls queued in more than one skill for a multi-skilled EAS agent, the system gives preference to matching the trunk location number of the queued call to the location number of the previously-busy agent. Available only with Call Center Release 3.0 and later when **Multiple Locations** is enabled for the system.

**Related topics:**

[Multiple Locations](#) on page 948

[Call Center Release](#) on page 951

**PA (Percent Allocation)**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 100    | If the call handling preference is percent-allocation, the percentage for every agent skill. The total for all of the agent's skills must equal 100%. Percent Allocation is available as part of the Avaya Business Advocate software. |

**RL (Reserve Level)**

Assigns reserve levels or interruptible levels. Reserve levels are assigned to the agent for the skill with the Avaya Business Advocate Service Level Supervisor feature. Interruptible levels are assigned with the Interruptible AUX Work feature. Changes take effect the next time the agent logs in.

| Valid Entry | Usage  |
|-------------|--|
| 1 or 2      | Reserve level. The EWT threshold level for the agent is added to the assigned skill as a reserve agent. When the EWT for the skill reaches the corresponding threshold set on the Hunt Group screen, automatically the assigned skill gets added to the agent logged in skills. The agent delivers calls from this skill until the corresponding threshold drops below the assigned overload threshold for that level. Available only if the Business Advocate feature is enabled. |
| a           | Interruptible level of auto-in-interrupt.  |
| m           | Interruptible level of manual-in-interrupt.  |
| n           | Interruptible level of notify-interrupt.   |
| blank       | No reserve or interruptible level.   |

**Related topics:**

[Interruptible Aux Threshold](#) on page 650

### **Service Objective**

Enables or disables the Service Objective feature. The server selects calls for agents according to the ratio of Predicted Wait Time (PWT) or Current Wait Time (CWT) and the administered service objective for the skill. Service Objective is a feature that is part of the Avaya Business Advocate software.

Available only when greatest-need or skill-level is the call handling preference.

#### **Related topics:**

[Call Handling Preference](#) on page 440

### **SL (Skill Level)**

Skill level for every skill assigned to an agent. If EAS-PHD is not optioned, two priority levels are available. If EAS-PHD is optioned, 16 priority levels are available. In releases prior to R3V5, level 1 was the primary skill and level 2 was the secondary skill.

### **SN (Skill Number)**

Identifies the skill hunt groups that this agent handles. The same skill cannot be entered twice. Consider the following options:

- If EAS-PHD is not optioned, up to four skills are available.
- If EAS-PHD is optioned, up to 20 or 60 skills are available depending on the platform. Assigning a large number of skills to agents can potentially impact system performance.

## **Alias Station**

- Configures the system so that new telephone types that are not supported by system software can be administered
- Maps new telephone models to a supported telephone model. This mapping does not guarantee compatibility, but allows unsupported models to be administered and tracked by their own names.
- “Names” non-telephone devices

Without this feature, modems must be added to the system by administering the extension as the standard analog type 2500; modems then cannot be identified on a list of stations. Instead, a “modem” alias is created to type 2500 and entered as a type for every modem added to the system.

#### **Tip:**

When a system is upgraded to a new release that uses an alias set type, the system determines if the aliased type is supported in the new release (is now a native set type). Alias types that have become native can be identified if the last character of the aliased set type is a “#”.

Example command: `change alias station`

## Alias Set Type

A name for the non-supported telephone type that is used to alias to a similar supported telephone type. Accepts up to five characters. Blank characters are not supported.

## Supported Set Type

A supported telephone type used to map or alias to the alias set type.

### Note:

Data Communication Protocol (DCP) telephone types must be aliased to DCP telephone types, hybrid types to hybrid types, and analog to analog types.

## Alphanumeric Dialing Table

Associates alpha-names to dialed digit strings. This allows telephone users to place a data call by typing the alpha-name. Users only need to remember far-end alpha-names instead of the digit strings.

The screen consists of paired **Alpha-name/Mapped String** fields. Entries can be made in any order on the screen. However, before the screen is displayed for changing or reviewing, the entries in the table are sorted alphanumerically by the alpha-name. All entries are moved to the beginning of the table, leaving all blank entries at the end.

Example command: `change alphanumeric-dial-table`

### Alpha-name

All alpha-names in the table must be unique and cannot be referenced in their own **Mapped String**. The alpha-names can be used multiple times in any other **Mapped String**. Must start with an alphabetic character and cannot have blank spaces between characters. Accepts up to eight alphanumeric characters.

### Mapped String

From 1 to 24 characters that might contain alphanumeric, readability, delimiters, or special characters. The entry is used to generate the final dialing string and can include Facility Access Codes.

### Note:

A Mapped String cannot contain an Alpha-Name whose Mapped String also contains an Alpha-Name.

| Valid Entry    | Usage   |
|----------------|---|
| 0 to 9         | Numeric   |
| A to Z, a to z | Alpha. Uppercase entries are mapped to lowercase. |
| (              | Readability character                             |
| )              | Readability character                             |
| /              | Readability character                             |
| -              | Readability character                             |

| Valid Entry | Usage                                       |
|-------------|---|
| +           | Wait for dial tone                          |
| %           | Rest of digits are for end to end signaling |
| “ ”<br>,    | Pause for 1.5 seconds                       |
| space       | Readability character                       |
| #           | DTMF digit pound                            |
| *           | DTMF digit asterisk                         |
| ^           | Readability character                       |

## Announcements/Audio Sources

Assigns announcements to circuit packs and port locations.

Example command: `add announcement n`, where *n* is the extension number.

### Ann Name

The name of the announcement you are associating with the specified extension. Accepts up to 27 character filename. For VAL circuit packs only — no ., /, :, \*, ?, <, >, \, .wav, or blanks.

For VAL announcements, this field is required. The value in this field becomes the filename of the announcement. The .wav file extension, which is part of the filename stored on the circuit pack, does not appear. Do not enter .wav as part of the filename. Names on a single VAL circuit pack must be unique. The system checks for duplicate filenames on the same VAL circuit pack.



#### Note:

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

### Ann Type

The type of announcement assigned to this extension number.

| Valid Entry | Usage  |
|-------------|--|
| analog      | Play announcements from an external device for a specific period and hang up when finished. When the device hangs up, the caller hears a click. Connects to the server running Avaya Communication Manager through an analog port. Ringing starts playback.  |
| analog-m    | Playing continuous music or audio source from an external announcement device.   |
| analog-fd   | Use to play announcements from an external device for a specific period and hang up when finished. When the device hangs up, the caller hears a click. Connects to the server running Avaya Communication Manager through an analog port. Ringing starts playback. Sends forward disconnect signal to stop playback. |

| Valid Entry | Usage   |
|-------------|---|
| aux-trunk   | Auxiliary trunk. Used with an external announcement device with a 4-wire "aux" interface.   |
| aux-trk-m   | Auxiliary trunk. Used with continuously playing music or audio sources that do not indicate playback is active.   |
| ds1-fd      | Assigned to DS1 ports on circuit packs. Callers do not hear a click when the device hangs up. Provides a disconnect to stop playback when the announcement is done. |
| ds1-ops     | Callers do not hear a click when the device hangs up.   |
| ds1-sa      | Provides a disconnect to stop playback when the announcement is done. Callers do not hear a click when the device hangs up.   |
| integrated  | Stored internally on a special integrated announcement circuit pack. Used for general announcements and VDN of Origin Announcements.                                |
| integ-mus   | Integrated music source.  |
| integ-rep   | Integrated repeating.   |

## COR

| Valid Entry | Usage   |
|-------------|---|
| 0 to 995    | The class of restriction (COR) associated with this announcement. |

## Extension

The extension number associated with the announcement being added, displayed, changed, or removed.

### Note:

When entering a Multi-Location Dial Plan shortened extension in a field designed for announcement extensions, certain administration end validations that are normally performed on announcement extensions are not done, and resultant warnings or submittal denials do not occur. The shortened extensions also do not appear in any display or list that shows announcement extensions. Extra care should be taken to administer the correct type of announcement for the application if assigning shortened extensions.

## Group/Port

The announcement board location or the Audio Group number. For an integrated announcement type, this field displays as **Group/Board**. If the announcement type is not integrated, the field displays as Port.

The group port number is represented in one of the following ways:

- Gnn where nn represents a one or two-digit audio group number.
- The location of the VAL or the TN750 announcement circuit pack. Characters are in the aaxss format (where aa = the cabinet number, x = the carrier, and ss = the slot number).
- gggv9 for media gateway vVAL, where ggg is the gateway number of the media gateway. Up to 250 numbers are allowed.

 **Note:**

To administer DID Intercept announcements in a multi-location system where each location or city needs a different announcement, enter an audio group in this field instead of a VAL port.

**Protected**

Sets the protection mode for an integrated announcement or music extension.

| Valid Entry | Usage  |
|-------------|--|
| y           | Protects the integrated announcement from being deleted or changed by any user using a telephone session or an FTP using VAL Manager or SAT. For VAL, after an announcement file that was recorded or transferred using FTP resides on the circuit pack, the file is protected as read-only.   |
| n           | Allows telephone session users with console permission or FTP to change or delete an announcement. This value is used when administrators initially administer an announcement or subsequently need to change or delete it. The recording can be changed or deleted by users with console permissions to delete or change the recording. Changing or deleting using the telephone recording session requires the console permissions class of service (COS). |

**Queue**

| Valid Entry | Usage  |
|-------------|--|
| y           | Queues calls for the announcement if the announcement type is integrated, integ-rep or aux-trunk. The caller is always connected to the beginning of the announcement. ACD, vectoring delay announcements and call centers should always use this option. This is the default. |
| n           | No queue nor barge-in. The caller is always connected to the beginning of the announcement. The announcement does not play if a port is unavailable.   |
| b           | Sets up barge-in if the announcement type is integrated, integ-rep or aux-trunk. When the announcement type is integ-mus, this field defaults to b. Callers are connected to the announcement at any time while it is playing.   |

| Valid Entry | Usage  |
|-------------|--|
|             | <p> <b>Note:</b></p> <p>The same non-charge-in announcement can be played through more than one port (or all ports) of an integrated circuit pack. The initial request to play an announcement selects an available port on the board on which the announcement resides. If there are additional requests to play the announcement while it is playing on another port(s), another port is selected. If all ports are busy, new requests to play announcements go to the integrated announcement system queue. Otherwise, the request to play is denied, and processing continues without the caller hearing the announcement. When a port becomes available, all queued calls (up to the platform “calls connected” limit) are connected at the same time to hear the announcement play from the beginning.</p> <p>A charge-in announcement starts playing when first requested and continues playing through a port, repeating until there are no more requests. Call processing simultaneously connects calls to the playing charge-in announcement. Each call remains connected until the requesting feature operation removes the call (for example, wait step times out). Charge-in type announcements never select another port to play the same announcement once it is playing on a specific port.</p> |

### Queue Length

The number of calls that queues for this announcement. The maximum number of queues depends on the system configuration.

### Rate

The recording rate speed in 1000 bits/seconds for TN750 or ISSPA integrated announcements. A different recording speed can be used for each integrated announcement. With VAL type sources, the default is 64 and cannot be changed.

| Valid Entry | Usage  |
|-------------|--|
| 16          | <p>16 kbps</p> <ul style="list-style-type: none"> <li>• 8 minutes and 32 seconds of announcement time per circuit pack</li> <li>• 1 hour and 24 minutes for 10 circuit packs for the TN750</li> <li>• 240 minutes of storage time for the ISSPA</li> </ul> <p>This rate does not provide a high-quality recording. Avaya does not recommend this for customer announcements, but it is adequate for VDN of Origin announcements.</p> |
| 32          | <p>32 kbps</p> <ul style="list-style-type: none"> <li>• 4 minutes and 16 seconds of total announcement time for the TN750</li> <li>• 120 minutes of storage time for the ISSPA</li> </ul>  |

| Valid Entry | Usage  |
|-------------|--|
| 64          | 64 kbps <ul style="list-style-type: none"> <li>• 2 minutes and 8 seconds of announcement time per circuit pack</li> <li>• 42 minutes for 10 circuit packs for the TN750</li> <li>• 60 minutes of storage time for the ISSPA</li> </ul> This is the default for VAL |

**TN**

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

**ARS Toll Table**

Assigns ARS Toll Tables used by Subnet Trunking. Specifies whether calls to local telephone company central office codes listed on the table are toll or non-toll calls. Non-toll calls are specified based on the last two digits of the distant-end of the trunk group.

Example command: `change ars toll`

**Attendant Console**

Assigns an Attendant Console to the system.

Example command: `add attendant n`, where *n* is the console number.

**Attendant console: page 1**

***Attendant Console x***

Number assigned to the attendant console. The attendant console is the main answering position for an organization.

***Auto Answer***

| Valid Entry | Usage   |
|-------------|---|
| all         | An incoming call to an idle attendant is answered automatically without any required button presses by the attendant.             |
| acd         | Only ACD split/skill calls and direct agent calls can auto answer. Non-ACD calls terminated to an attendant console ring audibly. |
| none        | All calls terminated to this attendant console receive some sort of audible ringing treatment.                                    |

**Console Type**

This console's intended use. There can only be one night-only or one day/night console in the system unless Tenant Partitioning is administered. Night Service is activated from the principal console or from the one station set per-system that has a **nite-serv** button.

| Valid Entry | Usage  |
|-------------|--|
| principal   | Puts the attendant console into night service. |
| day-only    | Handles only day service calls.                |
| night-only  | Handles only night service calls.              |
| day/night   | Handles day or night service calls.            |

**COR**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 95     | The class of restriction (COR) for this attendant console. |

**COS**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 15     | The class of service (COS) for this attendant console. |

**Data Module**

Enables or disables a connection between the console and data terminal.

**Related topics:**

[Data Module](#) on page 516

**Disp Client Redir**

Controls how the station displays calls originating from a station with Client Room Class of Service. Available only if the Hospitality feature is enabled.

| Valid Entry | Usage   |
|-------------|---|
| y           | <p>Displays redirection information for a call originating from a Client Room and terminating to this station.</p> <p> <b>Note:</b><br/>For stations with an audix station type, AUDIX Voice Power ports, or ports for any other type of messaging that needs display information, this field must be enabled.</p> |
| n           | Does not display redirection information for all calls originating from a Client Room, including redirected calls that terminate to this station. Displays only the client name and extension, or room.   |

**Related topics:**

[Hospitality \(Basic\)](#) on page 946

[Hospitality \(G3V3 Enhancements\)](#) on page 946

**Display Language**

| Valid Entry  | Usage  |
|--|--|
| English<br>French<br>Italian<br>Spanish<br>user-defined<br>Unicode | Language in which console messages are displayed. Unicode display is available only for Unicode-supported telephones (models 4610SW, 4620SW, 4621SW, 4622SW), Sage, Spark, and 9600-series. Spice telephones support Unicode display. Unicode is also an option for the 2420J telephone when enabled for the system. |

**Related topics:**

[Display Character Set](#) on page 938

**Extension**

The extension for the individual attendant console. Individual attendant extensions allow attendants to use features that an attendant group cannot use. For example, extensions can be members of a DDC or UCD group. An individual attendant extension can have its own Class of Restriction and Class of Service.

If attendants have an individual extension, users can call the attendant by dialing the extension, or users can be assigned an abbreviated-dialing button for fast access to the attendant.

If an extension is not assigned, the attendant can only be addressed as a member of the attendant group. If the attendant has a data module, this field cannot be blank.

**Group**

| Valid Entry | Usage                       |
|-------------|-----------------------------|
| 1 to 128    | The attendant group number. |

**H.320 Conversion**

Enables or disables the conversion of H.320 compliant calls made to this telephone to voice-only. Because the system can handle only a limited number of conversion calls, the number of telephones with H.320 conversion should be limited.

**Name**

Name of the console. Any entry is accepted. Accepts up to 27 alphanumeric characters.

 **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Port**

Each attendant console requires a port on a digital line circuit pack. For reliability, the attendant consoles should not be assigned to ports on the same digital line circuit pack. For example, if three attendant consoles are to be provided, each console should be assigned to a port on

three different digital line circuit packs, if possible. However, if required, all attendant consoles can be assigned to ports on the same digital line circuit pack.

| Valid Entry                              | Usage  |
|--|--|
| 1 to 64                                  | First and second characters are the cabinet number   |
| A to E                                   | Third character is the carrier   |
| 0 to 20                                  | Fourth and fifth characters are the slot number  |
| 01 to 04 (Analog TIE trunks)<br>01 to 31 | Six and seventh characters are the circuit number  |
| 1 to 250                                 | Gateway  |
| V1 to V9                                 | Module   |
| 01 to 31                                 | Circuit  |
| ip                                       | SoftConsole IP attendant. The ip option is allowed only if IP attendant consoles are enabled for the system.               |
| x  | There is no hardware associated with the port assignment. An individual attendant extension must be assigned in this case. |

**Example:** 01A0612 designates cabinet 01, carrier A, slot 06, and circuit number (port) 12.

#### Related topics:

[Extension](#) on page 450

[IP Attendant Consoles](#) on page 946

#### Security Code

The security code required by the SoftConsole IP attendant.

#### TN

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

#### Type

| Valid Entry | Usage  |
|-------------|--|
| console     | The type of attendant console being administered |
| 302         | 302B/C/D or SoftConsole IP attendant             |

#### Direct Trunk Group Select Button Assignments (Trunk Access Codes)

The trunk access codes (TACs) for local and remote servers. The local TAC (one to four digits) refers to a trunk group or Loudspeaker Paging zone on this server. Remote TACs are only useful in a private network (including DCS) network. The remote TAC (one to three digits) refers to a trunk group on the remote server. If a remote TAC is given, then the local TAC must see

a trunk group that connects directly to the remote server running Communication Manager and is also limited to one to three digits.

The characters \* and # can be used as the first digit.

Avaya recommends a DCS trunk be specified as the local TAC between the local and remote servers. If the TAC specified as local between the local and remote servers is not a DCS trunk, the remote trunk cannot be monitored by the local server running Communication Manager.

### ***Hundreds Select Button Assignments***

The hundreds group to be associated with a **Hundreds Group Select** button located on an optional selector console.

A hundreds group number represents all but the last two digits of an extension number. Fields 1 through 8 are used when the selector console is a 24A-type console and fields 1 through 20 are used for a 26A-type console.

#### **Example**

The **Hundreds Select** button on the selector console for extension 3822 would be “38”.

### **Attendant console: page 2 Softconsole IP Attendant**

#### ***Always Use***

If enabled:

- A softphone can register no matter what emergency call handling settings the user entered into the softphone.
- If a softphone dials 911, the administered **Emergency Location Extension** is used. The user-entered settings on the softphone are ignored.

Does not apply to SCCAN wireless telephones, or to extensions administered as type h.323.

#### **Related topics:**

[Emergency Location Ext](#) on page 59

### ***Direct IP-IP Audio Connections***

Allows or denies direct audio connections between IP endpoints that saves on bandwidth resources and improves sound quality of voice over IP transmissions.

### ***Emergency Location Ext***

Specifies the Emergency Location Extension for the SoftConsole IP Attendant. Defaults to the telephone extension. This extension is the starting point for identifying the street address or nearby location when an emergency call is made. The entry in this field is manipulated by CAMA Numbering Format before being sent over CAMA trunks; or similarly by Numbering — Public/Unknown Format before being sent over ISDN trunks. Accepts extensions of up to eight digits.

### ***IP Audio Hairpinning***

If enabled, allows IP endpoints connected through the IP circuit pack in the server in IP format to bypass the Communication Manager TDM bus.

## Remote Softphone Emergency Calls

Tells Communication Manager how to handle emergency calls from the IP telephone. Available when **IP Softphone** is enabled for the system.

### **Caution:**

An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. Please be advised that an Avaya IP endpoint cannot dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. Do not use an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations. Please contact your Avaya representative if you have questions about emergency calls from IP telephones.

| Valid Entry | Usage  |
|-------------|--|
| as-on-local | <p>If the administrator populates the IP Address Mapping screen with emergency numbers, the value as-on-local functions as follows:</p> <ul style="list-style-type: none"> <li>• If the <b>Emergency Location Extension</b> field is the same as the <b>Emergency Location Extension</b> field in the IP Address Mapping screen, the value as-on-local sends the extension to the Public Safety Answering Point (PSAP).</li> <li>• If the <b>Emergency Location Extension</b> field is different from the <b>Emergency Location Extension</b> field in the IP Address Mapping screen, the value as-on-local sends the extension in the IP Address Mapping screen to the Public Safety Answering Point (PSAP).</li> </ul>   |
| block       | <p>Prevents the completion of emergency calls. Used for users who are mobile but always have a circuit-switched telephone nearby, and for those who are farther away from the media server or switch than an adjacent area code served by the same 911 Tandem office. When users attempt to dial an emergency call from an IP Telephone and the call is blocked, they can dial 911 from a nearby circuit-switched telephone instead.</p>   |
| cesid       | <p>Allows Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP. The end user enters the emergency information into the IP Softphone.</p> <p>Used for IP Softphones with road warrior service that are near enough to the Avaya S8XXX server that an emergency call routed over the trunk reaches the PSAP that covers the server or switch.</p> <p>If the Avaya S8XXX server uses ISDN trunks for emergency calls, the digit string is the telephone number, provided that the number is a local direct-dial number with the local area code, at the physical location of the IP Softphone. If the Avaya S8XXX server uses CAMA trunks for emergency calls, the end user enters a specific digit string for each IP Softphone location, based on advice from the local emergency response personnel.</p> |

| Valid Entry | Usage   |
|-------------|---|
| option      | Allows users to select the option (extension, block, or cesid) that the user selected during registration and the IP Softphone reported. Used for extensions that can be swapped back and forth between IP Softphones and a telephone with a fixed location.<br>Users choose between block and cesid on the softphone. A DCP or IP telephone in the office automatically selects <b>extension</b> . |

**Related topics:**

[IP Softphone](#) on page 71

**Attendant console: page 2 VIS feature options**

***VIS FEATURE OPTIONS***

These fields administer Visually Impaired Services options.

**Auto Start**

Allows or denies an attendant permission to press any key on the keypad to start a call without the need to first press the **Start** button.

**Echo Digits Dialed**

Enables and disables voiced confirmation of dialed digits.

**Attendant console: page 3**

Displays if the attendant console is to be connected to a data terminal using a 7400B or 8400 data module.

**Related topics:**

[Data Module](#) on page 449

***ATTENDANT DATA MODULE***

**Bcc**

Determines compatibility when non-ISDN facilities are connected to ISDN facilities (ISDN Interworking feature).

**COR**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 995    | The Class Of Restriction (COR) number for the data module. |

**COS**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 15     | The (COS) number used to designate allowed features. |

**Data Extension**

The extension number assigned to the data module. This value must agree with the system dial plan. Accepts a one- to five-digit number.

## Name

The name assigned to the data module extension number.

**Related topics:**

[Ext](#) on page 456

## TN

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

**ABBREVIATED DIALING**

## List1

| Valid Entry | Usage  |
|-------------|--|
| s           | System   |
| g           | Group — A group number is also required            |
| p           | Personal — A personal list number also is required |
| e           | Enhanced   |

**SPECIAL DIALING OPTION**

Identifies the destination of all calls when this data module originates calls. The following dialing options are available:

| Valid Entry | Usage  |
|-------------|--|
| hot-line    | Allows single-line telephone users to automatically place a call to an extension, telephone number, or Feature Access Code (FAC).      |
| default     | An associated Abbreviated Dialing number is dialed when the user goes off-hook and enters a carriage return following the DIAL prompt. |

**HOT LINE DESTINATION — Abbreviated Dialing Dial Code**

The AD number dialed when the user goes off-hook on a Data Hot Line call.

Hot Line Service allows single-line telephone users, by simply lifting the handset, to automatically place a call to a preassigned destination (extension, telephone number, or feature access code).

The Hot Line Service destination number is stored in an Abbreviated Dialing List.

A Direct Department Calling (DDC), a Uniform Call Distribution (UCD), a Terminating Extension Group (TEG) extension, or any individual extension within a group can be a Hot Line Service destination. Also, any extension within a DDC group, UDC group, or TEG can have Hot Line Service assigned.

Use Hot Line Service when very fast service is required and when you use a telephone only for accessing a certain facility. Loudspeaker Paging Access can be used with Hot Line Service to provide automatic access to paging equipment.

Available only for a default or hot-line special dialing option.

**Related topics:**

[SPECIAL DIALING OPTION](#) on page 455

**DEFAULT DIALING Abbreviated Dialing Dial Code**

The AD number dialed when the user goes off-hook and enters a carriage return following the “DIAL” prompt. The data call originator also can perform data terminal dialing by specifying a dial string that might or might not contain alphanumeric names. Available only for a default special dialing option.

**Related topics:**

[SPECIAL DIALING OPTION](#) on page 455

**ASSIGNED MEMBER**

Ext

The extension number of a previously-administered user who has an associated **Data Extension** button and who shares the use of the module.

Name

The name assigned to the data module extension number.

**Related topics:**

[Ext](#) on page 456

**Attendant console: page 3 feature button assignments**

**FEATURE BUTTON ASSIGNMENTS**

Administers the feature buttons assigned to the attendant console. The split and forced release buttons are administered in a fixed location. The **hold**, **night-serv**, and **pos-busy** buttons have default locations. The following table provides descriptions of feature buttons that are unique to the attendant console.

**Audible Tones On/Off**

| Valid Entry | Usage   |
|-------------|---|
| cw-ringoff  | Call waiting ringer off; turns on/off the audible tone for call waiting on attendant console (1 per console). |
| in-ringoff  | Incoming call ringer off; turns on/off the audible tone for incoming call ringer (1 per console).             |
| re-ringoff  | Timed reminder ringer off; turns on/off the audible tone for timer reminder ringer (1 per console).           |

## Attendant Control of Trunk Group Access

| Valid Entry | Usage  |
|-------------|--|
| act-tr-grp  | Activate trunk group access; allows the attendant to control a trunk group. All calls going to the trunks are routed to the attendant (one per console).   |
| deact-tr-g  | Deactivate trunk group access; allows the attendant to release control of a trunk group (one per console).   |
| class-rstr  | Display Class of Restriction. Used to display the COR associated with a call (one per console).  |
| em-acc-att  | Emergency Access to the Attendant. The associated status lamp is flashed when there are one or more calls on the emergency attendant queue (one per console).  |
| hold        | Hold. When the Hold button is pressed while the attendant is active on a loop, the party on the loop is put on hold and the call type button associated with the loop is lit (one per console).  |
| pos-busy    | <p>Position Busy. When this button is pushed, the attendant is put into position busy mode, the "Pos Avail" light is turned off, and the light associated with the <b>pos-busy</b> button is lit. Pushing the <b>pos-busy</b> button a second time takes the console out of "position busy" mode, turns on the "Pos Avail" light and turns off the light associated with the <b>pos-busy</b> button.</p> <p>If the <b>pos-busy</b> button is administered on a 2-LED button, the top LED flashes when the last attendant goes into "Position Busy" mode. Otherwise, if the button has only one LED, the single LED associated with the <b>pos-busy</b> button flashes (one per console).</p> |
| serial-cal  | Serial Call. Allows attendant-extended calls to return to the same attendant if the trunk remains off-hook (one per console).  |
| override    | Attendant Override. Enables the attendant to override diversion features such as, Call Forwarding, Call Coverage, and so on (one per console).   |
| intrusion   | Call Offer. Allows the attendant to extend a call when the called party is active on another call (one per console).   |
| dont-split  | Don't Split. Allows the attendant to not split away a call when dialing (one per console).   |
| vis         | <p>Visually Impaired Attendant Service (vis). Activates visually impaired service for the attendant. When this service is activated, the attendant can listen to console status or messages by pressing buttons that have been translated as follows:</p> <ul style="list-style-type: none"> <li>• "con-stat" repeats the console status.</li> <li>• "display" calls out display contents.</li> <li>• "dtgs-stat" calls out the DTGS status.</li> </ul>  |

| Valid Entry | Usage  |
|-------------|--|
|             | <ul style="list-style-type: none"> <li>• “last-mess” repeats the last message.</li> <li>• “last-op” calls out the last operation.</li> </ul> |

### Trunk Group Select

Up to 12 **DTGS** buttons can be administered. The status lamp associated with the feature button is used to monitor the busy/idle status of the trunk. Trunk groups administered on these buttons cannot be controlled using **Attendant Control of Trunk Group Select** buttons.

| Valid Entry | Usage  |
|-------------|--|
| local-tgs   | Local trunk group select; allows the attendant to access trunk groups on the local server running Communication Manager.       |
| remote-tgs  | Remote trunk group select; allows the attendant to access trunk groups on a remote server running Avaya Communication Manager. |

### Other

| Valid Entry | Usage   |
|-------------|---|
| alt-frl     | Alternate facility restriction level; allows the attendant to activate or deactivate the AFRL feature. When activated, this allows the originating device (lines or trunks) to use an alternate set of the facility restriction levels to originate a call (one per console).   |
| hundrd-sel  | <p>Hundreds group select; additional administered hundreds group select feature buttons. When a feature button is administered as “hundrd-sel”, a subfield appears that must then be administered with a 1 to 3 digit hundreds group plus prefix, if needed. Administered hundrd-sel feature buttons operate in the same manner as fixed <b>HGS</b> buttons.</p> <p>The total number of hundreds group select buttons (fixed and administered) allowed on a console is 20. Thus, if all 20 fixed <b>HGS</b> buttons have been administered, no additional <b>hundrd-sel</b> feature buttons can be administered.</p> <p>If 12 HGS buttons are assigned, Avaya recommends that the <b>night</b>, <b>pos-busy</b>, and <b>hold</b> buttons be reassigned to locations 20, 21, and 3, respectively. The <b>HGS</b> buttons should then be assigned to the right-most three columns, as required.</p> |
| group-disp  | Group Display. Allows the attendant to see a display of extensions currently being tracked on the DXS module.   |
| group-sel   | Group Select. Allows the attendant to select a specific group of hundreds by dialing the first 2 or 3 digits of the hundreds group.   |
| occ-rooms   | Occupied rooms; allows the attendant to see which rooms are occupied.   |
| maid-stat   | Maid status; allows the attendant to see which rooms are in one of six specified states.  |

| Valid Entry | Usage  |
|-------------|--|
| vu-display  | VuStats ( <b>vu-display</b> ). Allows users with display telephones and attendants to turn on the VuStats display. The limit to the number of VuStats feature buttons depends on how many feature buttons are available on the attendant console. The system is designed to allow you to set up a separate VuStats display format for each feature button. Therefore, agents can change the type of measurements on their display by selecting a different VuStats feature button. |

## Attendant console: page 4 display module button assignments

### Display Module Button Assignments

Display-type buttons obtain display functions on the associated alphanumeric display. Also, several feature buttons can be administered so that their associated status lamps can be used to provide visual indications of the associated feature or function. In some cases, the button itself is not operational. These buttons are noted as [status lamp]. If a **Call Cover Msg Rt** (cov-msg-rt) button is assigned, a Leave Word Calling Delete Msg (delete-msg) button and a **Next** (next) button must also be assigned.

## Audio Group

Adds, changes, or displays a specified audio group. An audio group is a collection of recorded audio sources that have been placed in a group to facilitate their selection.

Example command: `add audio-group n`, where *n* is the group number.

### Audio Source Location

The board location for this audio group:

- cabinet (1 to 64), carrier (A to E), slot (0 to 20)
- gateway (1 to 250), module (V1 to V9)

### Group Name

An alpha-numeric name of the audio group for identification.

#### Note:

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

## AUDIX-MSA Node Names

Example command: `change node-names audix`

### AUDIX Names

The name of the voice messaging node consisting of a one- to seven-character string. Used as a label for the associated IP address. The node names must be unique on each server running Communication Manager.

### IP Address

The IP address associated with the node name.

### MSA Names

Identifies the name of the MSA node. Accepts a one- to seven-character string. The MSA names must be unique on each server running Communication Manager.

## Authorization Code — COR Mapping

Assigns authorization codes and the class of restriction (COR) that is associated with a given authorization code.



### Security alert:

To maximize security:

- Administer authorization codes to the maximum length allowed by the system
- Create random (nonconsecutive) authorization codes
- Change authorization codes at least quarterly
- Deactivate authorization codes immediately if a user leaves the company or changes assignments
- Assign each authorization code the minimum level of calling permissions required

Example command: `change authorization-code n`, where *n* is the authorization code.

### AC

The authorization code number. The AC number can be any combination of numbers between 4 and 13 digits. The number of digits must agree with the assigned system-wide value. To enhance system security, choose Authorization Codes of 13 random digits.

### Related topics:

[Authorization Code Length](#) on page 586

### COR

| Valid Entry | Usage  |
|-------------|--|
| 0 to 995    | When a user dials the associated authorization code, this is the COR that the telephone or other facility assumes for that call. |

### Number of Codes Administered

The number of authorization codes already administered. There is a maximum number of authorization codes depending on system configuration.

## Authorization Code — PIN Checking for Private Calls

Restricts users from making internal or external private calls by forcing them to enter a Personal Identification Number (PIN) code after dialing the PIN feature access code. If the PIN is valid,

the user can dial the destination digits to make a call. PINs are administered on the same screen as authorization codes.

Example command: `change authorization-coden`, where *n* is the authorization code.

## Best Service Routing

Compares specified skills, identifies the skill that provides the best service to a call, and delivers the call to that resource. If no agents are currently available in that skill, the call is queued. To respond to changing conditions and operate more efficiently, BSR monitors the status of the specified resources and adjusts call processing and routing as appropriate.

Example command: `change best-service-routing n`, where *n* is the routing number.

## Interflow VDN

The routing number including the dial access code used to access the Interflow Vector Directory Number (VDN) at the remote location. Accepts up to 16 characters.

| Valid Entry | Usage                           |
|-------------|---------------------------------|
| 0 to 9      | Includes the * and # characters |
| ~p          | Pause                           |
| ~w/~W       | Wait                            |
| ~m          | Mark                            |
| ~s          | Suppress                        |

## Location Name

A name that identifies each location where this feature is administered. Accepts up to 15 alphanumeric characters.

## Lock

| Valid Entry | Usage   |
|-------------|---|
| y           | Provides extra security by not sending any BSR information to the Call Management System. |
| n           | Sends BSR information to the CMS.   |

## Maximum Suppression Time

Prevents callers from connecting to a VDN within a certain time period after receiving a busy signal.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 60     | The maximum poll suppression time in seconds. |

| Valid Entry | Usage  |
|-------------|--|
|             | For example, if the poll suppression time is set to 30 seconds, the remote location polling is suppressed for up to 30 seconds if the Expected Wait Time (EWT) is far from being the best. |

**Net Redir**

Enables or disables Network Call Redirection.

**Num**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 255    | The location number that corresponds to the <b>consider location x</b> step. |

**Number**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 255    | The identifying number of the current BSR plan. |

**Status Poll VDN**

The routing number including the dial access code used to access the Status Poll VDN at the remote location. Accepts up to 16 characters.

| Valid Entry | Usage                           |
|-------------|---------------------------------|
| 0 to 9      | Includes the * and # characters |
| ~p          | Pause                           |
| ~w/~W       | Wait                            |
| ~m          | Mark                            |
| ~s          | Suppress                        |

**Switch Node**

| Valid Entry         | Usage   |
|---------------------|---|
| 1 to 32767<br>blank | The Network Node ID for each switch if the Universal Call ID is being used. This is optional. |

**Bulletin Board**

The bulletin board is used to post and receive information. The first 10 lines are for high-priority messages from Avaya personnel. An `init` or `inads login` is used to enter high-priority information to trigger the high-priority message at login time. Additional lines can be used by anyone with access. The system automatically enters the date the message was posted or last changed to the right of each message line.

Up to 40 characters of text per line are allowed, as well as one blank line. If more than one blank line is entered, the system consolidates them and displays only one. The system also deletes any blank line if it is line one of any page. Text cannot be indented on the bulletin board.

Example command: `change bulletin-board`

### Date

The date the bulletin board information was entered or last changed.

### Text lines

Used for high priority messages on the bulletin board. Anyone with an `init` or `inads` login can enter high-priority information to trigger the high-priority message at login time. Additional lines can be used by anyone with access.

## Button Type Customization Restriction

Restricts customized button labels of up to 50 specified button types for users who are not considered VIP users. Manages system allocation of customized button labels to ensure that VIP users have the available customized button label resources.

Example command: `change button restriction`

### Restrict Customization Of Button Types

| Valid Entry | Usage  |
|-------------|--|
| y           | Restricts the use of customized feature button labels. This is the default.              |
| n           | Users can customize labels for all buttons on their telephones without any restrictions. |

### Restrict Customization Of Labels For the Following Button Types

The button type restricted from being customized.



#### Note:

The **abr-spchar** and the **abr-dial** button types require a special associated character.

Available only when **Restrict Customization of Button Types** is enabled.

#### Related topics:

[Restrict Customization Of Button Types](#) on page 463

## Call Type Digit Analysis Table

Specifies how to modify telephone numbers for internal contacts dialed from the telephone call log or from a corporate directory. Users can automatically place outgoing calls based on the telephone number information in the telephone call log without having to modify the telephone number. Requires at least one entry to activate.

## Managing inventory

Example command: `change calltype analysis`

### Delete

Communication Manager deletes this number of digits in the original digit string from the left-hand side of the original digit string to complete analysis and routing.

### Dialed String length (Min, Max)

Communication Manager compares digit strings of this length to the original digit string, looking for a match to complete analysis and routing.

### Dialed String Match

Communication Manager compares this digit string to the original digit string, looking for a match to complete analysis and routing. The characters x and X can be used as wildcards.

### Insert

Communication Manager inserts these digits into the left-hand side of the original digit string to complete analysis and routing.

### Location

| Valid Entry                 | Usage  |
|-----------------------------|--|
| <i>Numeric value</i><br>all | Phones dialing from this location use the entries in the Call Type Digit Analysis Table. If there are matching entries in the telephone's location, those entries are used. If there are no matching entries in the phone's location, the Communication Manager tries the entries in location all. |

### Type

The administered call type for this dialed string. Communication Manager tests the modified digit string against the administered call type.

| Valid Entry | Usage   |
|-------------|---|
| aar         | Automatic Alternate Routing — digit analysis algorithm commonly used for private network calls. |
| ars         | Automatic Route Selection — digit analysis algorithm commonly used for public network calls.    |
| ext         | Extension entries in the dialplan analysis tables of type ext.                                  |
| udp         | Extension entries in the <b>uniform-dialplan tables</b> .                                       |

## Call Vector

Programs a series of commands that specify how to handle calls directed to a Vector Directory Number (VDN).

Example command: `change vector n`, where *n* is the vector number.

**01 through XX**

The following vector commands that specify how to handle calls directed to a VDN are located on lines 01 through XX. The maximum allowed depends on the configuration.

| Valid Entry     | Usage  |
|-----------------|--|
| adjunct routing | Causes a message to be sent to an adjunct requesting routing instructions based on the CTI link number.  |
| announcement    | Provides the caller with a recorded announcement.  |
| busy            | Gives the caller a busy signal and causes termination of vector processing.  |
| check           | Checks the status of a split (skill) for possible termination of the call to that split (skill).   |
| collect         | Allows the user to enter up to 16 digits from a touch-tone telephone, or allows the vector to retrieve Caller Information Forwarding (CINFO) digits from the network.  |
| consider        | Defines the resource (split, skill, or location) that is checked as part of a Best Service Routing (BSR) consider series and obtains the data BSR uses to compare resources.   |
| converse-on     | Delivers a call to a converse split (skill) and activates a voice response script that is housed within a Voice Response Unit (VRU).   |
| disconnect      | Ends treatment of a call and removes the call from the server running Communication Manager. Also allows the optional assignment of an announcement that will play immediately before the disconnect.                        |
| goto            | Allows conditional or unconditional movement (branching) to a preceding or subsequent step in the vector.  |
| messaging       | Allows the caller to leave a message for the specified extension or the active or latest VDN extension.  |
| queue-to        | Unconditionally queues a call to a split or skill and assigns a queueing priority level to the call in case all agents are busy.   |
| reply-best      | Used only in status poll vectors in multi-site Best Service Routing applications, where it "returns" best data for its location to the primary vector on the origin server.  |
| return          | Returns vector processing to the step following the <b>goto</b> command after a subroutine call has processed.   |
| route-to        | Routes calls either to a destination that is specified by digits collected from the caller or an adjunct (route-to digits), or routes calls to the destination specified by the administered digit string (route-to number). |
| set             | Performs arithmetic and string operations and assigns values to a vector variable or to the digits buffer during vector processing.  |
| stop            | Halts the processing of any subsequent vector steps.   |

| Valid Entry | Usage  |
|-------------|--|
| wait-time   | Delays the processing of the next vector step if a specified delay time is included in the command's syntax. Also provides feedback (in the form of silence, ringback, or music) to the caller while the call advances in queue. |

### **ANI/II-Digits**

Indicates whether or not the use of ANI and II-Digits vector routing commands is allowed. ANI/II-Digits Routing is a **G3V4 Enhanced** feature.

**Related topics:**

[G3V4 Enhanced](#) on page 467

### **ASAI Routing**

Indicates whether or not the **CallVisor Adjunct/Switch Applications Interface (ASAI) Routing** option is enabled.

**Related topics:**

[Attendant Vectoring](#) on page 944

### **Attendant Vectoring**

Indicates whether or not Attendant Vectoring is optioned on this VDN. Attendant Vectoring does not support Call Center features.

**Related topics:**

[Attendant Vectoring](#) on page 944

### **Basic**

Indicates whether Vectoring (Basic) is enabled for system.

**Related topics:**

[Vectoring \(Basic\)](#) on page 952

### **BSR**

Indicates if the Best Service Routing option is enabled on the system. BSR commands and command elements can be used in vectors only if this option is enabled.

**Related topics:**

[Vectoring \(Best Service Routing\)](#) on page 952

### **CINFO**

Indicates if Caller Information Forwarding (CINFO) Routing is enabled on the system. CINFO allows a call to be routed based on digits supplied by the network in an ISDN-PRI message.

**Related topics:**

[Vectoring \(CINFO\)](#) on page 952

**EAS**

Indicates if Expert Agent Selection (EAS) is enabled on the system.

 **Note:**

When EAS is enabled, the terminology changes from “Split” to “Skill” for help messages, error messages, and vector commands. For example, check backup split becomes check backup skill.

**Related topics:**

[Expert Agent Selection \(EAS\)](#) on page 951

**G3V4 Adv Route**

Indicates if G3V4 Advanced Vector Routing commands are allowed.

**Related topics:**

[Vectoring \(G3V4 Advanced Routing\)](#) on page 952

**G3V4 Enhanced**

Indicates if G3V4 Enhanced Vector Routing commands and features are allowed.

**Related topics:**

[Vectoring \(G3V4 Enhanced\)](#) on page 953

**Holidays**

Indicates if Holiday Vectoring features are allowed.

**Related topics:**

[Vectoring \(Holidays\)](#) on page 953

**LAI**

Indicates if Look-Ahead Interflow is enabled.

**Related topics:**

[Lookahead Interflow \(LAI\)](#) on page 951

**Lock**

Controls access to the vector from the Call Management System.

 **Security alert:**

Always lock vectors that contain secure information (for example, access codes).

| Valid Entry | Usage   |
|-------------|---|
| y           | This vector is <i>not</i> accessible from the CMS. Locked vectors can only appear and be administered through the SAT or a terminal emulator. If Meet-me Conference is enabled, <b>Lock</b> must also be enabled. |
| n           | Gives CMS users the ability to administer this vector.  |

### Meet-me Conf

Indicates if the Meet-me Conference feature is enabled. If enabled, designates the VDN as a Meet-me Conference VDN. Attendant Vectoring and Meet-me Conference cannot be enabled at the same time.

**Related topics:**

[Enhanced Conferencing](#) on page 945

### Multimedia

| Valid Entry | Usage   |
|-------------|---|
| y           | Multimedia calls are set to be answered and billed at the start of vector processing. Multimedia Call Handling must be enabled. |
| n           | The vector is not expected to receive multimedia calls and Multimedia Call Handling is disabled. This is the default.           |

**Related topics:**

[Multimedia Call Handling \(Basic\)](#) on page 948

[Multimedia Call Handling \(Enhanced\)](#) on page 948

### Name

Optionally provides a reference for the vector name. Used to activate Network Call Redirection. Accepts up to 27 alphanumeric characters.

Available only if ISDN Network Call Redirection is enabled.

 **Note:**

Supported by Unicode language display for the 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones. Unicode is also an option for the 2420J telephone when the **Display Character Set** is katakana. For more information on the 2420J, see *2420 Digital Telephone User's Guide*.

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Related topics:**

[Display Character Set](#) on page 938

[ISDN/SIP Network Call Redirection](#) on page 947

### Number

The vector number.

### Prompting

Indicates if Vectoring (Prompting) is enabled for the system.

**Related topics:**

[Vectoring \(Prompting\)](#) on page 953

## CAMA Numbering Format

Administers the Centralized Automatic Message Accounting (CAMA) trunks and provides Caller's Emergency Service Identification (CESID) information to the local community's Enhanced 911 system through the local tandem office.

Provides the CESID format by extension number or number blocks. This allows for multiple CESID formats to be sent over multiple CAMA trunk groups allowing for mixed station numbering plans and some limited conversion from non-DID to DID numbers typically required by the Private Switch/Automatic Location Interface (PS/ALI) database.

Example command: `change cama-numbering`

### CESID

The number used to identify the calling terminal within an emergency service system. This field can represent a prefix to an extension or the entire CESID. Accepts up to 16 digits. The maximum number of allowed digits depends on the equipment.

### Ext Code

The leading digits or all of the digits in the extension for the specified CESID. If the extension length is greater than the number of digits in the extension code, the extension code is interpreted as a block of digits.

**Example:** If the extension length is 4 and the extension code is 11, the CESID serves extensions 1100 through 1199.

### Ext Len

The number of digits in the extension. Accepts up to 13 digits.

### System CESID Default

The number sent over the CAMA trunk if the Extension Code for the CESID is not specified. Accepts up to 16 digits.

#### Related topics:

[Ext Code](#) on page 469

### Total Length

The total number of sent digits. Accepts up to 16 digits.

## CDR system parameters

Administers the Call Detail Recording (CDR) feature used to record information on incoming, outgoing, and tandem calls for each trunk group administered for CDR, including auxiliary trunks. The system records information on each trunk-group call and each station-to-station call.

Example command: `change system-parameters cdr`

**CDR system parameters: page 1**  
***Calls to Hunt Group — Record***

| Valid Entry | Usage  |
|-------------|--|
| member-ext  | Records the extension of the telephone or data terminal where the call terminated. |
| group-ext   | Records the extension that was dialed.   |

***CDR Account Code Length***

| Valid Entry | Usage  |
|-------------|--|
| 1 to 15     | The number of digits to record when a user enters an account code. For some record formats, a long account code overwrites spaces on the record that are usually assigned to other fields. |

***CDR Date Format***

| Valid Entry            | Usage   |
|------------------------|---|
| month/day<br>day/month | The format for the date stamp that begins each new day of call records. |

***Condition Code ‘T’ for Redirected Calls***

Enables or disables identification of CDR records of calls that have been redirected automatically off the server running Communication Manager.

| Valid Entry | Usage   |
|-------------|---|
| y           | The Condition Code of both CDR records for the call is ‘T.’ |
| n           | Special identification is applied.                          |

***Digits to Record for Outgoing Calls***

| Valid Entry | Usage   |
|-------------|---|
| dialed      | Record the digits a user dials.   |
| outpulsed   | Record the digits that Communication Manager sends out over the trunk, including any additions or deletions that take place during routing. |

***Disconnect Information in Place of FRL***

| Valid Entry | Usage   |
|-------------|---|
| y           | Replace the Facility Restriction Level (FRL) with information about why a call disconnects. |
| n           | Record the call FRL.  |

**Enable CDR Storage on Disk**

Enables or disables the Survivable CDR feature for the main server, Survivable Remote Server (Local Survivable Processor), and Survivable Core Server (Enterprise Survivable Server). Default is disabled.

**Force Entry of Acct Code for Calls Marked on Toll Analysis Form**

Specifies whether or not an account code is required when making a toll call. Account codes might not be required on all charged calls, and might be required on some non-charged calls.

| Valid Entry | Usage   |
|-------------|---|
| y           | Denies all toll calls unless the user dials an account code. Available only if Forced Entry of Account Codes is enabled for the system. |
| n           | Allows calls without an account code. This does not override other calling restrictions.  |

**Related topics:**

[Forced Entry of Account Codes](#) on page 946

**Inc Attd Call Record**

Enables or disables separate recording of attendant portions of outgoing calls that are transferred or conferenced.

Available only if Incoming Trunk Call Splitting is enabled.

**Related topics:**

[Inc Trk Call Splitting](#) on page 471

**Inc Trk Call Splitting**

Enables or disables the creation of separate records for each portion of incoming calls that are transferred or conferenced.

Available only if **Record Outgoing Calls Only** is disabled.

**Related topics:**

[Record Outgoing Calls Only](#) on page 474

**Interworking Feat-flag**

| Valid Entry | Usage   |
|-------------|---|
| y           | The feature flag indicates interworked outgoing ISDN calls.             |
| n           | The feature flag indicates no answer supervision for interworked calls. |

**Intra-Switch CDR**

Enables or disables the recording of calls within Communication Manager. Requires administration of intra-switch CDR extensions.

**Related topics:**

[Intra-Switch CDR](#) on page 674

**Modified Circuit ID Display**

Affects the “printer”, “teleser”, and “59-character” output formats.

| Valid Entry | Usage  |
|-------------|--|
| y           | <p>Displays the circuit ID in its actual format (100's, 10's, units). For example, circuit ID 123 displays as 123.</p> <p> <b>Note:</b><br/>Requires verification that an output device can accept this format.</p> |
| n           | <p>Displays the circuit ID in its default format (10's, units, 100's). For example, circuit ID 123 appears as 231.</p>   |

**Node Number (Local PBX ID)**

Displays the DCS switch node number in a network of switches.

**Outg Attd Call Record**

Enables or disables separate recording of attendant portions of outgoing calls that are transferred or conferenced.

Available only if Outgoing Trunk Call Splitting is enabled.

**Related topics:**

[Inc Trk Call Splitting](#) on page 471

[Outg Trk Call Splitting](#) on page 472

**Outg Trk Call Splitting**

Enables or disables the creation of separate records for each portion of outgoing calls that are transferred or conferenced

**Primary Output Endpoint**

Determines where the server running Communication Manager sends the CDR records. Required if a Primary Output Format is specified.

| Valid Entry             | Usage  |
|-------------------------|--|
| eia                     | The EIA port is used to connect the CDR device.  |
| <i>Extension number</i> | The extension of the data module that links the primary output device to the server running Communication Manager. |
| CDR1, CDR2              | The CDR device is connected over a TCP/IP link, and this link is defined as either CDR1 or CDR2 for IP Services.   |

**Related topics:**

[IP Services](#) on page 716

**Primary Output Format**

Indicates the format of the call records sent to the primary output device.

| Valid Entry   | Usage  |
|---|--|
| customized  | For special call accounting needs that standard record formats do not accommodate. Requires call accounting software that is also customized to receive these records. Call accounting vendors should be consulted before using this option. |
| printer   | Call detail records are sent to a printer rather than to a record collection or call accounting system.  |
| 59-char expanded<br>lsu<br>lsu-expand<br>int-direct<br>int-isdn<br>int-process<br>teleseer<br>unformatted | For standard record formats. The selection must be compatible with your call accounting software. Verify this through your vendor or the accounting system documentation.  |

**Privacy — Digits to Hide**

Indicates how much of the dialed number to hide on the CDR record for stations administered for CDR privacy.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 7      | The number of digits to hide, counting from the end right to left. |

**Example**

For a value of 4, when the user dials 555-1234, only “555” appears in the CDR record.

**Related topics:**

[CDR Privacy](#) on page 69

**Record Agent ID on Incoming**

Determines whether or not to include the EAS agent login ID instead of the physical extension in the CDR record.

Available only if Expert Agent Selection (EAS) is enabled for the system. Cannot be enabled if **Record Called Vector Directory Number Instead of Group or Member** is enabled.

**Related topics:**

[Record Called Vector Directory Number Instead of Group or Member](#) on page 474

**Record Agent ID on Outgoing**

Determines whether or not to include the EAS agent's LoginID instead of the physical extension in the CDR record.

Available only if Expert Agent Selection (EAS) is enabled for the system.

**Related topics:**

[Expert Agent Selection \(EAS\)](#) on page 951

**Record Call-Assoc TSC**

Enables or disables the creation of records for call-associated temporary signaling connections. A large number of data connections could increase the number of records, so call collection device capacity must be taken into consideration.

**Record Called Vector Directory Number Instead of Group or Member**

Determines whether or not to include the Vector Directory Number (VDN) in the CDR record. If enabled, the called VDN overrides the group or member information that normally appears in the CDR record. If a call is directed through more than one VDN, the first VDN used for the call is stored. This applies only to calls routed to a hunt group by a vector, not to calls routed directly to an extension by a vector.

Cannot be enabled if **Record Agent ID on Incoming** is enabled.

**Related topics:**

[Record Agent ID on Incoming](#) on page 473

**Record Non-Call-Assoc TSC**

Enables or disables the creation of records for non-call-associated temporary signaling connections. A large number of data connections could increase the number of records, so record collection device capacity must be taken into consideration.

**Record Outgoing Calls Only**

| Valid Entry | Usage   |
|-------------|---|
| y           | Record only outgoing calls.<br><br> <b>Note:</b><br>This can save space if you are only concerned with charges for outbound calls. |
| n           | Record both outgoing and incoming calls.  |

**Remove # From Called Number**

| Valid Entry | Usage  |
|-------------|--|
| y           | Removes the “#” or “E” symbol from the <b>Dialed Number</b> field of the call detail record. The output device must be able to accept this format.               |
| n           | Retains the trailing “#” or “E” symbol in the <b>Dialed Number</b> field whenever an inter-digit time-out occurs or users dial # to indicate the end of dialing. |

**Secondary Output Endpoint**

Available only if **Secondary Output Format** is administered.

| Valid Entry             | Usage  |
|-------------------------|--|
| eia                     | The secondary output device is connected to the eia port.  |
| <i>Extension number</i> | The extension of the data module that links the secondary output device to the server running Communication Manager. |
| CDR1, CDR2              | The CDR device is connected over a TCP/IP link, and this link is defined as either CDR1 or CDR2 for IP Services.     |

**Related topics:**

[Secondary Output Format](#) on page 475

[Service Type](#) on page 717

**Secondary Output Format**** Caution:**

Only qualified Avaya service personnel should administer a secondary output device. This option might cause loss of data when the buffer contains large amounts of data.

| Valid Entry   | Usage   |
|---|---|
| customized<br>int-direct<br>int-process<br>lsu<br>unformatted | The format of the call records sent to the secondary output device. Only these formats can be used for a secondary output device. The format must be compatible with call accounting software. Verify this through the vendor or the accounting system documentation. |

**Suppress CDR for Ineffective Call Attempts**

Ineffective call attempts are calls that are blocked because the user did not have sufficient calling privileges or because all outgoing trunks were busy. These calls appear on the CDR record with a condition code “E”.

| Valid Entry | Usage   |
|-------------|---|
| y           | Ignores ineffective call attempts. Used when there is limited storage space for CDR records and when records often overrun the buffer.  |
| n           | Reports ineffective call attempts. Used when users are often unable to place outgoing calls, or if a large number of incoming calls are not completed. Also used to keep records of attempts to contact a client, and when ISDN trunks are used. This option requires more space for records. |

**Use Enhanced Formats**

Enables or disables the use of the Enhanced version of the specified primary output formats. Enhanced formats provide additional information about time in queue and ISDN call charges, where available. This affects the expanded, teleseer, lsu, printer, and unformatted output formats. Enhanced formats and ISDN formats cannot be used at the same time.

**Use ISDN Layouts**

Enables or disables using the ISDN version of the specified primary output format. ISDN Layouts provide more accurate information about the inter-exchange carrier and ISDN network

services used for a call. This affects lsu and printer output formats, as well as any format with ISDN layouts, such as teleseer. ISDN formats and Enhanced formats cannot be used at the same time.

**Use Legacy CDR Formats**

Enables or disables the use of pre-Communication Manager 4.0 legacy Call Detail Recording (CDR) formats for CDR records. The default is enabled. Listed below are the CDR formats that are impacted by this field. All other CDR formats remain unchanged.

| CDR Format           | Communication Manager 3.1 and earlier length | Communication Manager 4.0 and later length |
|----------------------|--|--|
| ISDN Teleseer        | 80   | 82   |
| Enhanced Teleseer    | 81   | 83   |
| ISDN Printer         | 84   | 86   |
| Enhanced Printer     | 85   | 87   |
| ISDN LSU             | 59   | 61   |
| Enhanced LSU         | 59   | 61   |
| Expanded             | 135  | 139  |
| Enhanced Expanded    | 151  | 155  |
| Unformatted          | 105  | 109  |
| Enhanced Unformatted | 119  | 123  |
| Int-ISDN             | 136  | 140  |

**CDR System Parameters: page 2**

Used if there is an arrangement with the vendor to customize the call accounting system to receive these records.

Available only if **Primary Record Format** is customized.

**Related topics:**

[Primary Output Format](#) on page 473

**Data Item**

Itemizes the data items that appear on the customized record.

At least one field for a record must be included. The last two data items in the record must be line-feed and return, in that order.

| Data Item    | Length | Data Item     | Length |
|--------------|--------|---------------|--------|
| acct-code    | 15     | xc-code       | 4      |
| attd-console | 2      | line-feed     | 1      |
| auth-code    | 7      | location-from | 3      |

| Data Item      | Length | Data Item     | Length |
|----------------|--------|---------------|--------|
| bandwidth      | 2      | location-to   | 3      |
| bcc            | 1      | n-trk-code    | 4      |
| calling-num    | 15     | ma-uui        | 1      |
| clg-pty-cat    | 2      | node-num      | 2      |
| clg-num/in-tac | 10     | null          | 3      |
| code-dial      | 4      | out-crt-id    | 3      |
| code-used      | 4      | ppm           | 5      |
| cond-code      | 1      | res-flag      | 1      |
| country-from   | 3      | return        | 1      |
| country-to     | 3      | sec-dur       | 5      |
| dialed-num     | 23     | space         | 1      |
| duration       | 4      | time          | 4      |
| feat-flag      | 1      | timezone-from | 3      |
| fri            | 1      | timezone-to   | 6      |
| in-crt-id      | 3      | tsc_ct        | 4      |
| ins            | 3      | tsc_flag      | 1      |
| sdn-cc         | 11     | vdn           | 5      |

### ***Length***

The length of each data item. The maximum record length depends on the call accounting system. Check with the vendor. The date field should be six digits to ensure proper output. Certain fields default to the required length.

### ***Record Length***

Displays the accumulated total length of the customized record, updated each time the length of a data item changes.

## **Change Station Extension**

Changes extensions on the switch from one extension to another all at once. Specifically:

- All administration that was associated with the current extension is associated with the new extension.
- Any administration references on the changing extension, such as references used in a vector, coverage, and so on, are now referenced to the new extension.
- All references to the previous extension are removed from the system.

If an extension is changed that is also administered on an adjunct, such as voice mail or an ASAI link, the extension on the adjunct must also be changed to ensure proper functionality.

For fields that are changing, current information prior to the change displays under **From Extension**.

A forwarded extension administered as a button is not automatically changed.

### Exceptions

Station extensions cannot be changed if that station is administered as the emergency location extension for another station. For example, if station A is administered as the emergency location extension for station B, then:

- First assign station B to a different emergency location extension.
- First change station B. The system displays station A's extension as the emergency location extension.

Example command: `change extension-station n`, where *n* is the extension assigned to a station.

### Emergency Location Extension

The new extension for the emergency location extension. Up to seven numbers can be used to make up a valid extension number for the dial plan.

### IP Parameter Emergency Location

The emergency location extension already administered for the current extension.

#### Related topics:

[IP network region](#) on page 689

### Message Lamp

The new extension for the message lamp extension. Up to seven numbers can make up a valid extension number for the dial plan.

### Port

The port of the existing extension.

### Station

The new extension. Up to seven numbers can make up a valid extension number for the dial plan.

### Station Name

The name of the existing extension.

#### **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

## Circuit Packs

Adds, changes, or removes circuit packs that are inserted into port, expansion control, and switch node carriers. For more information, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

## Class of Restriction

Establishes classes of restriction (COR). Classes of restriction restrict users from originating or terminating certain types of calls. A system might use only one COR or as many as necessary to control calling privileges.

Example command: `change cor n`, where *n* is the COR number.

### Class of restriction: page 1

#### Access to MCT

Grants or denies access to the Malicious Call Trace feature.

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows this user to activate a request to trace a malicious call.  |
| n           | Prohibits this user from requesting a malicious call trace, but does not prevent this extension from appearing in the MCT History report should this extension be the subject of a malicious call trace. |

#### Add/Remove Agent Skills

Allows or denies users permission to add or remove skills.

#### APLT

Allows or denies permission to access APLT trunk group Enhanced Private Switched Communications System (EPSCS) or Common Control Switched Arrangement (CCSA) off-net facilities.

#### Automatic Charge Display

Shows the cost of an active outgoing call using Periodic Pulse Metering (PPM) or ISDN Advice of Charge (AOC) on Digital Communications Protocol (DCP) or Avaya BRI stations. Not available in the U.S.

| Valid Entry | Usage   |
|-------------|---|
| y           | Call charges display during and at the end of the call.                                       |
| n           | Call charges display only when users press the <b>disp-chrg</b> button before the call drops. |

### Called Party Restriction

| Valid Entry | Usage  |
|-------------|--|
| Inward      | Blocks the calling party from receiving incoming exchange network calls, attendant originated calls, and attendant completed calls.  |
| Manual      | Blocks the called party from receiving all calls except for those originated or extended by the attendant.   |
| Public      | Blocks the called party from receiving public network calls. Attendant calls are allowed to go through to the called party as well as attendant-assisted calls if administered for this COR. |
| Termination | Blocks the called party from receiving any calls at any time.  |
| none        | No called party restrictions.  |

**Related topics:**

[Restriction Override](#) on page 484

### Calling Party Restriction

Determines the level of calling restriction associated with this COR.



**Important:**

Limit calling permissions as much as possible.

| Valid Entry | Usage  |
|-------------|--|
| Origination | Blocks the calling party from originating a call from the facility at any time. The party can only receive calls. A telephone with this COR can initiate Remote Access calls, if the COR of the barrier code allows it.  |
| Outward     | Blocks the calling party from calling outside the private network. Users can dial other users on the same server running Communication Manager or within a private network. To enhance security, Avaya recommends that you use outward restrictions when practical.                                    |
| All-toll    | Blocks the calling party from making ARS and trunk access calls to certain toll areas as defined by the Dialed String on the ARS Toll Analysis table. The call completes if the facility COR is also associated with an Unrestricted Call List and whose Dialed String also matches the dialed number. |
| Tac-toll    | Blocks the calling party from making trunk access calls to certain toll areas as defined by the Dialed String on the ARS Toll Analysis table. The call completes if the facility COR is also associated with an Unrestricted Call List and whose Dialed String also matches the dialed number.         |
| none        | No calling party restrictions.   |

**Related topics:**

[Dialed String](#) on page 420

**Can Be a Service Observer**

Allows or denies a user with this COR permission to be a service observer.

Available only if Basic Service Observing is enabled for the system.

 **Caution:**

Service Observing might be subject to federal, state, or local laws, rules, or regulations; or require the consent of one or both of the parties to the conversation. Customers should familiarize themselves with and comply with all applicable laws, rules, and regulations before using these features.

**Related topics:**

[Service Observing \(Basic\)](#) on page 952

**Can Be Picked Up By Directed Call Pickup**

Allows or denies calls for this station or EAS agent to be picked up using the Directed Call Pickup Up feature.

Available only if Directed Call Pickup is enabled for the system.

**Related topics:**

[Directed Call Pickup](#) on page 631

**Can Be Service Observed**

Allows or denies service observing for not only physical extensions, but also for logical agent IDs and VDNs.

**Can Change Coverage**

Allows or denies station users permission to:

- Select one of two previously-administered coverage paths
- Activate, change, or deactivate call forward all calls or call forward busy/don't answer from any on-site or off-site location

**Can Use Directed Call Pickup**

Allows or denies the station, attendant, or EAS agent permission to pick up calls using the Directed Call Pickup feature.

Available only if Directed Call Pickup is enabled for the system.

**Related topics:**

[Directed Call Pickup](#) on page 631

**COR Description**

The description of the COR. Accepts up to 35 characters.



**Tip:**

A clear description makes it easier to remember which COR to assign when adding users.

**Example**

Two examples of COR descriptions include “Customer Service” and “Legal Department”.

**COR Number**

The COR number.

**Direct Agent Calling**

Allows or denies users permission to use the Direct Agent Calling feature. Direct Agent Calling allows users to dial an ACD agent extension directly, rather than anyone in the agent pool. If the system is in Night Service, the call routes to the Night Service extension. If the extension with this COR belongs to an agent, the agent can receive calls directly.

**Facility Access Trunk Test**

Allows or denies users permission to perform Facility Access Trunk Tests. When this feature is active, the **trk-ac-alm** feature button status lamp lights when a successful test attempt occurs.

**Forced Entry of Account Codes**

If enabled, allows the Forced Entry of Account Codes (FEAC) feature on this COR. Any telephone assigned the associated COR must dial an account code before making an outgoing call. If a call is being routed by ARS, account code checking is not done on the COR.

Available only when the FEAC feature is enabled for the system.



**Important:**

If a COR using the FEAC feature is assigned to a VDN, the route-to commands executed by the associated vector will not be successful.

**Related topics:**

[Forced Entry of Account Codes](#) on page 946

[CDR FEAC](#) on page 973

**FRL**



**Security alert:**

Assign the lowest possible FRL to enhance system security.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 7      | Assigns a Facilities Restriction Level (FRL) to the COR to enhance system security. AAR or ARS features use this entry to determine call access to an outgoing trunk group. Outgoing call routing is determined by a comparison of the FRLs in the AAR/ARS Routing Pattern and the FRL associated with the COR of the call originator. The call originator is |

| Valid Entry | Usage   |
|-------------|---|
|             | typically a telephone user. An originating FRL of 0 has the least calling privileges. |

### **Fully Restricted Service**

Not available for Enhanced Private Switched Communications System (EPSCS) or Common Control Switched Arrangement (CCSA) off-net facilities.

| Valid Entry | Usage   |
|-------------|---|
| y           | Stations do <i>not</i> have access to the public network for either incoming or outgoing calls. |
| n           | Stations have access to the public network for either incoming or outgoing calls.               |

### **Group II Category For MFC**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 10     | Controls categories for Russian signaling trunks. Also controls categories for R2-MFC signaling trunks if administered system-wide. The server running Communication Manager sends this value as the Calling or Called Party Category for telephones or trunks that use this COR. This administered Calling Party Category digit is included as part of the ANI information sent to the local telephone company central office on request using R2-MFC signaling. |

#### **Related topics:**

[Use COR for Calling Party Category](#) on page 796

### **Group Controlled Restriction**

| Valid Entry | Usage   |
|-------------|---|
| active      | The current COR is under controlled restriction.            |
| inactive    | The current COR is <i>not</i> under controlled restriction. |

### **Hear System Music on Hold**

If enabled, the Music on Hold feature can be activated by a telephone.

### **Hear VDN of Origin Announcement**

Allows or denies agents permission to receive VDN of Origin Announcement (VOA) messages that provide agents with a short message about the caller's city of origin or requested service based on the VDN used to process the call.

### **MF ANI Prefix**

The prefix applied to an extension number when ANI is sent to the local telephone company central office. Accepts up to seven digits. This COR-specific value overrides any ANI prefix administered system-wide for multifrequency signaling. The prefix does not apply when ANI is

tandemed through the Communication Manager server on tandem calls. Also applies to the ANI for the server when the originating side is a trunk and there was no ANI.

**Related topics:**

[ANI Prefix](#) on page 790

**Partitioned Group Number**

Available only if AAR/ARS Partitioning is enabled for the system and partition groups are administered.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 8      | The AAR/ARS partitioned group number associated with this COR. |

**Related topics:**

[ARS/AAR Partitioning](#) on page 943

**PASTE (Display PBX Data on telephone)**

| Valid Entry | Usage                       |
|-------------|-----------------------------|
| y           | Downloads all lists         |
| n           | Disallows the PASTE feature |

**Priority Queuing**

If enabled, a telephone user’s calls are placed ahead of non-priority calls in a hunt group queue.

**Related topics:**

[ACD](#) on page 950

**Restricted Call List**

Allows or denies this COR access to the Restricted Call List. If allowed, agents cannot make calls to numbers on the Restricted Call List from a facility assigned this COR.

**Related topics:**

[RCL](#) on page 974

**Restriction Override**

Allows users assigned this COR to override inward restriction during conference, transfer or call forwarding operation to a telephone that is inward restricted.

| Valid Entry | Usage   |
|-------------|---|
| attendant   | Attendants may override inward restrictions. A telephone with a COR that is inward restricted cannot receive public network, attendant-originated, or attendant-extended calls. |
| all         | All users can override inward restrictions  |
| none        | No users can override inward restrictions   |

**Send ANI for MFE**

Applicable only:

- For Spain
- For 2/6 signaling, but not 2/5 signaling
- If Expert Agent Selection (EAS) is enabled for the system

| Valid Entry | Usage   |
|-------------|---|
| y           | Enables Automatic Number Identification (ANI) in order to send the calling party's number to the public or IBERCOM network so that charges are broken down by line. |
| n           | Charges are not itemized by line. The company receives a single bill for the total number of calls made; also called <i>block charging</i> .                        |

**Related topics:**

[Expert Agent Selection \(EAS\) Enabled](#) on page 610

**Time of Day Chart**

Available only if Time of Day Routing is enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 8      | The AAR/ARS time-of-day-chart number associated with this COR. |

**Related topics:**

[Time of Day Routing](#) on page 950

**Unrestricted Call List**

| Valid Entry      | Usage  |
|------------------|--|
| 1 to 10<br>blank | Overrides specified toll call restrictions for a COR otherwise restricted from making ARS or trunk access calls. |

**Related topics:**

[Dialed String](#) on page 420

**Class of Restriction: page 2****ASAI Uses Station Lock**

| Valid Entry | Usage   |
|-------------|---|
| y           | Enables the ASAI originated calls to follow the restriction or permission assigned to the locked station, via the Station Lock COR feature. |
| n           | Enables the ASAI originated calls to follow the permission or restrictions of the COR assigned to the endpoint. The default value is n.     |

**Block Enhanced Conference/Transfer Display**

| Valid Entry | Usage  |
|-------------|--|
| y           | Blocks all the enhanced conference and transfer display messages on digital telephones except "Transfer Completed" . |
| n           | Allows all the enhanced conference and transfer display messages.  |

**Block Transfer Displays**

| Valid Entry | Usage  |
|-------------|--|
| y           | Prevents users of DCP, Hybrid, ISDN-BRI, or wireless display telephones from receiving a confirmation message when they transfer a call. |
| n           | Allows users to receive a confirmation message when they transfer a call.  |

**Brazil Collect Call Blocking**

If enabled, all Brazilian trunk calls that terminate to a station send back a double answer to the local telephone company central office (CO). This double answer tells the CO that this particular station cannot accept collect calls. The CO then tears down the call if it is a collect call.

**Erase 24xx User Data Upon: Dissociate or unmerge this phone**

Administers what local terminal data items are erased when the 24xx is dissociated or unmerged.

| Valid Entry    | Usage  |
|----------------|--|
| none           | Default value. No local terminal data is erased.   |
| log            | Terminal's local call Log data is erased.  |
| customizations | Call Log, Button labels, Speed Dial List, Local Terminal Options are erased.                     |
| all            | All local terminal data is erased (Call Log, Button Labels, Speed Dial List, Options, Language). |

**Erase 24xx User Data Upon: EMU login or logoff at this phone**

Administers what local terminal data items are erased upon Enterprise Mobility User (EMU) login or logoff.

| Valid Entry    | Usage  |
|----------------|--|
| none           | This is the default. No local terminal data is erased.   |
| log            | Terminal's local call Log data is erased.  |
| customizations | Call Log, Button labels, Speed Dial List, Local Terminal Options are erased.                     |
| all            | All local terminal data is erased (Call Log, Button Labels, Speed Dial List, Options, Language). |

**Line Load Control**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 4      | Specifies the line load control level for this COR, where 1 has no restrictions and 4 is the most restrictive. |

**Mask CPN/Name for Internal Calls**

| Valid Entry | Usage  |
|-------------|--|
| y           | Hides the display of calling and called party numbers and administered name on internal calls. |
| n           | Shows the display of calling and called party numbers and administered name on internal calls. |

**Maximum Precedence Level**

Assigns a maximum precedence level for extensions with this COR for use with the Multiple Level Precedence and Preemption feature.

| Valid Entry | Usage                               |
|-------------|-------------------------------------|
| fo          | Flash Override                      |
| fl          | Flash                               |
| im          | Immediate                           |
| pr          | Priority                            |
| ro          | Routine. This is the default value. |

**MF Incoming Call Trace**

If enabled, allows assignment of a Call Trace for a station. Communication Manager then generates an MFC backward signal during call setup instead of the “free” signal. This triggers the local telephone company central office to collect trace information before releasing the calling party.

**MLPP Service Domain**

| Valid Entry   | Usage   |
|---------------|---|
| 1 to 16777215 | The service domain for users and trunks to which this COR is assigned |

**Outgoing Trunk Alerting Timer (minutes)**

Applies an alerting tone to an outgoing trunk call after an administrable amount of time.

| Valid Entry | Usage   |
|-------------|---|
| 2 to 999    | The number of minutes to wait before an alerting tone is applied to the call. |

| Valid Entry | Usage   |
|-------------|---|
| blank       | The Alerting Tone for Outgoing Trunk Calls feature is disabled and the alerting tone is not applied to the call. This is the default. |

**Related topics:**

[Trunk Alerting Tone Interval \(seconds\)](#) on page 595

***Outgoing Trunk Disconnect Timer (minutes)***

Disconnects an outgoing trunk automatically after an administrable amount of time.

| Valid Entry | Usage  |
|-------------|--|
| 2 to 999    | The number of minutes to wait before automatically disconnecting the call. A warning tone is given to all parties on the trunk call 1 minute before the administered value and a second warning tone is heard 30 seconds later. The call is automatically disconnected 30 seconds after the second warning tone. |
| blank       | Outgoing trunk calls disconnect only when dropped by one or all parties. This is the default.  |

***Preemptable***

If enabled, makes extensions with this COR preemptable for Multiple Level Precedence and Preemption calls.

***Remote Logout of Agent***

If enabled, users can use a feature access code to logout an idle ACD or EAS agent without being at the agent's telephone.

***Service Observing by Recording Device***

If enabled, allows the service observer associated with this COR to use an audio recording device such as the Witness product.

***Station-Button Display of UUI IE Data***

If enabled, a station user can push a **uui-info station** button and see up to 32 bytes of ASAI-related User-User-Information Information Element (UUI-IE) data. Pressing the **uui-info** button displaces the incoming call/collected digits display. Pressing **callr-info** re-displays the collected digits.

Available only with Call Center release 3.0 or later.

**Related topics:**

[Call Center Release](#) on page 951

**Station Lock COR**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 995    | Extensions that are assigned this COR can use Station Lock with an administered Feature Access Code (FAC). This field defaults to the current COR. |

**Related topics:**

[Station Lock Activation/Deactivation](#) on page 567

**Class of Restriction: page 3**

The Send All Calls and Call Forwarding (SAC/CF) Override feature overrides active rerouting. This feature overrides these active rerouting settings:

- Send All Calls (SAC)
- Call Forwarding (CF) all
- Enhanced Call Forwarding (ECF) unconditional

**Auto Answer**

Enables or disables automatic answer on team button calls.

**Outgoing Trunk Disconnect Timer (minutes)**

Disconnects an outgoing trunk automatically after an administrable amount of time.

| Valid Entry | Usage  |
|-------------|--|
| 2 to 999    | The number of minutes to wait before automatically disconnecting the call. A warning tone is given to all parties on the trunk call 1 minute before the administered value and a second warning tone is heard 30 seconds later. The call is automatically disconnected 30 seconds after the second warning tone. |
| blank       | Outgoing trunk calls disconnect only when dropped by one or all parties. This is the default.  |

**Priority Ring**

Enables or disables priority ringing for speed dialing on team button calls.

**SAC/CF Override by Priority Call and Dialing**

Allows or denies a user of a station permission to enable the SAC/CF override feature:

- Depending on call initiation
- By pushing the **Priority** button
- Using the dial pad to dial

### **SAC/CF Override Protection for Priority Call and Dialing**

Allows or denies the user of a station permission to enable the SAC/CF override *protection* feature:

- Depending on call initiation
- By pushing the **Priority** button
- Using the dial pad to dial

### **SAC/CF Override Protection for Team Btn**

Enables or disables the protection of stations in this COR from SAC/CF Override rerouting.

### **SAC/CF Override by Team Btn**

Allows or denies a user permission to override active rerouting on a monitored station. When allowed, a user of a station with a **Team** button administered who is monitoring another station, can directly reach the monitored station by pushing the **Team** button. This overrides any currently-active rerouting — such as Send All Calls and Call Forwarding — on the monitored station.

### **Team Btn Display Name**

Enables or disables the display of station name on team button calls.

### **Team Btn Silent if Active**

Enables or disables audible ringing on team button calls.

### **Team Pick Up by Going Off Hook**

Enables or disables pick-up by going off hook on team button calls.

### **Class of restriction: page 4**

#### **CALLING PERMISSION**

Allows or denies an originating facility assigned to this COR being used to call facilities assigned to this COR.

#### **SERVICE OBSERVING PERMISSION**

Allows or denies permission to observe a specific COR.

## **Class of service**

Administers access permissions for call processing features that require dial code or feature button access.



#### **Note:**

Class of Service (COS) does not apply to trunk groups except for the Remote Access feature.

A COS assignment defines which features and functions a telephone user can access. Up to 16 different COS numbers can be administered (0 to 15). When Tenant Partitioning is enabled for the system, you can administer up to 100 COS groups, each with 16 Classes of Service.

The screen lists the default values for each COS or feature combination. For a particular combination, y allows access to the feature and n denies access.

 **Caution:**

Because many hunt groups are set up with COS 1, be careful when you assign restrictions to COS 1.

Example command: `change cos-group n`, where *n* is the COS group number.

**Related topics:**

[Tenant Partitioning](#) on page 949

**Class of service: page 1**

***Automatic Callback***

Enables or disables Automatic Callback. Automatic Callback allows internal users who place a call to a busy or an unanswered internal telephone to be automatically called back when the called telephone becomes available.

***Automatic Exclusion***

Available when Automatic Exclusion is enabled for the system and the applicable station has an assigned **Exclusion** button.

| Valid Entry | Usage   |
|-------------|---|
| y           | Allows Automatic Exclusion when a user goes off hook on a station. Automatically prevents other multi-appearance users from bridging onto a call. |
| n           | Denies Automatic Exclusion. Manual exclusion is available when the user presses the <b>Exclusion</b> button before dialing or during a call.      |

**Related topics:**

[Automatic Exclusion by COS](#) on page 625

***Call Forwarding All Calls***

Allows or denies the forwarding of all calls to any extension.

***Call Forwarding Busy/DA***

If enabled, users can forward calls to any extension when the dialed extension is busy or does not answer.

***Client Room***

Allows or denies users to access Check-In, Check-Out, Room Change/Swap, and Maid status functions. In addition, Client Room is required at consoles or telephones that are to receive message-waiting notification. Available only with Hospitality Services and a Property Management System interface.

***Console Permissions***

Allows or denies multi-appearance telephone users to control the same features that the attendant controls.

**Contact Closure Activation**

Allows or denies a user to open and close a contact closure relay. Contact closures control electrical devices remotely. Users dial a Feature Access Code (FAC) on a telephone to activate electrical devices such as electrical door locks.

**COS Group**

To administer a COS group, Tenant Partitioning must be enabled for the system.

| Valid Entry | Usage                 |
|-------------|-----------------------|
| 1 to 100    | The COS Group number. |

**Related topics:**

[Tenant Partitioning](#) on page 949

**COS Name**

The identifying name for this COS group. To administer a COS group, Tenant Partitioning must be enabled for the system.

**Related topics:**

[Tenant Partitioning](#) on page 949

**Data Privacy**

Allows or denies a user permission to enter a Feature Access Code (FAC) that protects a data call from being interrupted by any of the system override or ringing features.

**Extended Forwarding All**

Allows or denies a user permission to administer call forwarding from a remote location for all calls. Available only if Extended Coverage and Forwarding Administration is enabled for the system.

**Related topics:**

[Extended Cvg/Fwd Admin](#) on page 946

**Extended Forwarding B/DA**

Allows or denies a user permission to administer call forwarding from a remote location when the dialed extension is busy or does not answer. Available only if Extended Coverage and Forwarding Administration is enabled for the system.

**Related topics:**

[Extended Cvg/Fwd Admin](#) on page 946

**Off-Hook Alert**

Enables or disables the requirement that the system send an emergency call to the attendant if the telephone remains off-hook for a prescribed time. Available only if Basic Hospitality or Emergency Access to Attendant is enabled for the system.

**Related topics:**

[Emergency Access to Attendant](#) on page 945

[Hospitality \(Basic\)](#) on page 946

### **Personal Station Access (PSA)**

Allows or denies users permission to associate a telephone to their extension with their programmed services using a Feature Access Code (FAC). Do not enable for virtual telephones. Required for a user's home station in order for that user to use the Enterprise Mobility User (EMU) feature at other stations. Available only if Personal Station Access (PSA) is enabled for the system.

#### **Related topics:**

[Personal Station Access \(PSA\)](#) on page 948

### **Priority Calling**

Allows or denies a user permission to dial a Feature Access Code (FAC) to originate a priority call. Priority calls ring differently and override send all calls.

### **QSIG Call Offer Originations**

Allows or denies a user permission to invoke QSIG Call Offer services.

### **Restrict Call Fwd-Off Net**

| Valid Entry | Usage   |
|-------------|---|
| y           | Restricts a user from forwarding calls to the public network.<br><br> <b>Security alert:</b><br>For security reasons, this should be enabled for all classes of service except the ones used for special circumstances. |
| n           | Allows a user to forward calls to the public network.   |

### **Trk-to-Trk Restriction Override**

Allows or denies a user permission to override any system or COR-to-COR calling party restrictions that would otherwise prohibit the trunk-to-trunk transfer operation for users with this COS.

#### **Security alert:**

Use this COS capability with caution. The ability to perform trunk-to-trunk transfers greatly increases the risk of toll fraud.

### **Class of service: page 2**

### **Ad hoc Video Conferencing**

Enables or disables Ad-hoc Video Conferencing, so that up to six users can participate in a video conference call.

### **Call Forwarding Enhanced**

Allows or denies users permission to designate different preferred destinations for forwarding calls that originate from internal and external callers.

### **Masking CPN/Name Override**

Allows or denies users permission to override the MCSNIC capability. MCSNIC masks the display of calling party information and replaces it with a hard-coded system-wide text string, **Info Restricted**.

### **Priority Ip Video**

Allows or denies priority video calling. Video calls have an increased likelihood of receiving bandwidth and can also be allocated a larger maximum bandwidth per call.

### **VIP Caller**

Enables or disables automatic priority calling when assigned to the originator of a call. A call from a VIP phone is always a priority call without the use of a feature button or FAC.

## **Code Calling IDs**

On systems with chime paging, assigns a unique series of chimes to extensions using a chime code. The chime code assigned to an extension plays over the speakers whenever that extension is paged. Assigns chime codes to up to 125 extensions.

Example command: `change paging code-calling-ids`

### **Ext**

Assigns extensions to chime codes. Only one extension can be assigned to each chime code. The extension cannot be assigned to a code that is a Vector Directory Number (VDN).

## **Configuration Set**

Defines a number of call treatment options for Extension to Cellular calls for cellular telephones. The Extension to Cellular feature allows the use of up to 99 Configuration Sets, already defined in the system using default values.

Example command: `change off-pbx-telephone configuration-set n`, where *n* is the Configuration Set number.

### **Related topics:**

[Configuration Set](#) on page 885

[Mobility Trunk Group](#) on page 897

[XMOBILE Type](#) on page 915

### **Barge-In Tone**

Enables or disables a barge-in tone used to add security to Extension to Cellular calls. If a user is on an active Extension to Cellular call and another person joins the call from an Extension to Cellular enabled office telephone, all parties on the call hear the barge-in tone.

### **Call Appearance Selection for Origination**

Specifies how the system selects a Call Appearance for call origination. To use this feature, bridged calls must be enabled for the system.

| Valid Entry     | Usage   |
|-----------------|---|
| first-available | The system searches for the first available regular or bridged Call Appearance.   |
| primary-first   | <ul style="list-style-type: none"> <li>• Only regular Call Appearances are used for call origination. If a regular call appearance is not available, the call is not allowed.</li> <li>• The system first searches for a regular Call Appearance for call origination. If a regular Call Appearance is not available, a second search is made that includes both regular and bridged Call Appearances.</li> </ul> <p>This is the default.</p> |

**Related topics:**

[Bridged Calls](#) on page 917

**Calling Number Style**

Determines the format of the caller ID for calls from a local Avaya Communication Manager extension to an Extension to Cellular telephone.

| Valid Entry | Usage  |
|-------------|--|
| network     | Provides a display of only 10-digit numbers. For internal calls, the ISDN numbering tables are used to create the calling number and DCS calls use the ISDN calling number if provided. The externally provided calling number is used when available for externally originated calls. |
| pbx         | Provides a display of less than 10-digits. Extensions sent as the calling number for all internally- and DCS network-originated calls.   |

**Calling Number Verification**

Enables or disables restrictions on what types of calls are made to a cell phone with Extension to Cellular.

| Valid Entry | Usage  |
|-------------|--|
| y           | <p>Prevents all but the following calls from reaching the cell phone:</p> <ul style="list-style-type: none"> <li>• Network-provided</li> <li>• User-provided</li> <li>• Passed</li> </ul> <p>This setting has no effect on normal usage of the Extension to Cellular feature. This is the default.</p> |
| n           | No restrictions on calls reaching the cell phone.  |

**CDR for Calls to EC500 Destination**

Determines whether a Call Detail Record (CDR) is generated for any call to the cell telephone. Available only if CDR reports is enabled for the trunk group.

| Valid Entry | Usage   |
|-------------|---|
| y           | Treats calls to the XMOBILE station as trunk calls and generates a CDR.                   |
| n           | Treats calls to the XMOBILE station as internal calls and does <i>not</i> generate a CDR. |

**Related topics:**

[CDR Reports](#) on page 722

**CDR for Origination**

Determines the CDR report format when CDR records are generated for a call that originates from an Extension to Cellular cell phone. To generate this CDR, you must enable the Incoming Trunk CDR. The CDR report does not include dialed Feature Name Extensions (FNEs).

| Valid Entry  | Usage   |
|--------------|---|
| phone-number | The calling party on the CDR report is the 10-digit cell phone number. This is the default.                                     |
| extension    | The calling party on the CDR report is the internal office phone extension associated with the Extension to Cellular cell phone |
| none         | The system does not generate an originating CDR report.   |

**Cellular Voice Mail Detection**

Prevents cellular voice mail from answering an Extension to Cellular call. The call server detects when the cell phone is not the entity that answers the call and brings the call back to the server. Communication Manager treats the call as a normal call to the office telephone and the call goes to corporate voice mail. You can also set a timer for cellular voice mail detection that sets a time before Cellular Voice Mail Detection investigates a call.

| Valid Entry | Usage  |
|-------------|--|
| none        | No restrictions on cellular voice mail. This is the default.   |
| timed       | Amount of time from 1 to 9 seconds. The default is 4 seconds. Extension to Cellular call leg answered within the specified time is detected as being answered by the cellular voice mail and the call will continue to ring at the office telephone. If unanswered, it will go to corporate voice mail. This setting can be used for any type of network (GSM, CDMA, ISDN, etc). |
| message     | The message option works with carriers who use a non ISDN voice mail systems. It is not recommended to use this option with ISDN based voice mail systems.   |

## Configuration Set Description

A description of the purpose of the configuration set. Accepts up to 20 alphanumeric characters.

### Example

“Extension to Cellular handsets”

## Confirmed Answer

Enables or disables Confirmed Answer on Extension to Cellular calls for this station. If enabled, requires the user to input a digit to confirm receipt of a call sent to a cellular telephone by the Extension to Cellular feature. Upon answering the incoming call on the cellular telephone, the user hears a dial tone. The user must then press any one of the digits on the telephone keypad. Until the system receives a digit, the system does not treat the call as answered. The length of time to wait for the digit can be administered from 5 to 20 seconds, with a default of 10 seconds. The system plays a recall dial-tone to indicate that input is expected. During the response interval, the original call continues to alert at the desk set and any stations bridged to the call. If the user does not enter a digit before the time-out interval expires, the call is pulled back from the cell telephone.

## Fast Connect on Origination

Determines whether additional processing occurs on the server running Avaya Communication Manager prior to connecting a call. Reserved for future capabilities provided by the cell telephone provider but currently not used.

## Post Connect Dialing Options

Determines whether additional capabilities, beyond standard ISDN dialing, are available for those incoming ISDN trunk calls that are mapped into XMOBILE stations. These options come into effect after the call has entered the active state (Communication Manager has sent a CONNECT message back to the network).

| Valid Entry | Usage  |
|-------------|--|
| dtmf        | Expect digits from either in-band or out-of-band, but not simultaneously. The server allocates a DTMF receiver whenever it needs to collect digits. This option normally would be used for Extension to Cellular XMOBILE station calls.  |
| out-of-band | Expect all digits delivered by out-of-band signaling only. The server running Avaya Communication Manager collects digits that it needs from the out-of-band channel (no touch-tone receiver). In addition, any digits received when the server is not collecting digits are converted to DTMF and broadcast to all parties on the call. This option is in force for DECT XMOBILE station calls.                                       |
| both        | Expect all subsequent digits delivered by simultaneous in-band and out-of-band signaling. Out-of-band signaling consists of digits embedded in ISDN INFO messages while the in-band signaling consists of DTMF in the voice path. The server running Communication Manager collects all digits that it needs from the out-of-band channel. No touch tone receive is allocated in order to prevent collecting double digits. End-to-end |

| Valid Entry | Usage   |
|-------------|---|
|             | signaling occurs transparently to the server via in-band transmission of DTMF. This option is in force for PHS XMOBILE station calls. |

## Console parameters

Administers attendant console group parameters. This includes basic parameters for Centralized Attendant Service (CAS) and Inter-PBX Attendant Service (IAS). A list of the administered attendant consoles also displays.

Example command: `change console-parameters`

### Console parameters: page 1

#### **AAR/ARS Access Code**

An optional AAR/ARS access code used to route to the main switch. Accepts an up to four-digit access code. Available only for a QSIG branch CAS configuration.

#### **Related topics:**

[CAS](#) on page 499

#### **Alternate FRL Station**

The extension of the alternate facility restriction level (FRL) activation station.

#### **Attendant Group Name**

A name for the attendant group. Accepts up to 27 alphanumeric characters.

#### **Attendant Lockout**

Activates or deactivates Privacy — Attendant Lockout. Privacy — Attendant Lockout prohibits an attendant from reentering a conference call that has been placed on hold unless recalled by a telephone user on the call. This feature provides privacy for parties on a multiple-party call held on the console. The held parties can hold a private conversation without interruption by the attendant.

#### **Attendant Vectoring VDN**

Assigns the VDN extension for Attendant Vectoring to a console. Available only if Attendant Vectoring is enabled for the system and Tenant Partitioning is disabled.

#### **Related topics:**

[Attendant Vectoring](#) on page 944

[Tenant Partitioning](#) on page 949

#### **Backup Alerting**

Allows or denies system users permission to pick up alerting calls if the attendant queue has reached its warning state.

**Calls In Queue Warning**

The number of incoming calls that can be in the attendant queue before the console's second Call Waiting lamp lights. The queue maximum depends on system capacities.

**CAS**

The Centralized Attendant Service (CAS) allows users at separate locations to concentrate attendant positions at one location. Incoming trunk calls to unattended branch locations are routed to the main attendant.

| Valid Entry | Usage  |
|-------------|--|
| main        | The main Communication Manager server where the attendant group is located. Uses non-ISDN signaling. CAS Main must be enabled for the system.  |
| branch      | A branch Communication Manager server. There are no local attendants, so attendant-seeking calls route to the main Communication Manager server. Uses non-ISDN signaling. CAS Branch must be enabled for the system. |
| none        | Disables CAS.  |
| QSIG-main   | Same as main, but with QSIG signaling among the Communication Manager servers. Centralized Attendant must be enabled for the system.   |
| QSIG-branch | Same as branch, but with QSIG signaling among the Communication Manager servers. Centralized Attendant must be enabled for the system.   |

**Related topics:**

[RLT Trunk Group No.](#) on page 501

[Centralized Attendant](#) on page 954

**CAS Back-Up Ext**

| Valid Entry   | Usage   |
|---|---|
| Extension number<br>Individual attendant console<br>Hunt group<br>TEG | Extension in the dial plan that handles attendant-seeking calls if the RLT trunk group to the CAS Main server is out of service or if CAS Back-Up is activated. Neither a prefixed extension nor a VDN extension is allowed. Available only for the CAS Branch feature. |

**Related topics:**

[CAS Branch](#) on page 944

[CAS Main](#) on page 944

[Centralized Attendant](#) on page 954

**COR**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 995    | The class of restriction (COR) number for all attendant consoles. The COR for the individual Attendant Console overrides this value. |

**COS**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 15     | The class of service (COS) number that reflects the desired features for all your attendant consoles. The COS for the individual Attendant Console overrides this value. |

***DID-LDN Only to LDN Night Ext***

| Valid Entry | Usage  |
|-------------|--|
| y           | Only listed directory number (LDN) calls go to the listed directory night service extension. |
| n           | All attendant seeking calls route to the LDN night service extension.                        |

***Ext Alert Port (TAAS)***

The seven-digit port number assigned to the external alerting device. This supports the Night Service — Trunk Answer From Any Station feature.

An x indicates that there is no hardware associated with this port assignment. If an x is used, there should also be an value for **Ext Alert (TAAS) Extension**.

**Related topics:**

[Ext Alert \(TAAS\) Extension](#) on page 500

***Ext Alert (TAAS) Extension***

This extension is used by the Terminal Translation Feature (TTI) to assign a port to the Ext Alert Port from a station on the Ext Alert port during system installation or provisioning. Once a port is assigned either through TTI or by entering the Ext Alert Port, the extension is automatically removed and treated as unassigned. Available only when the Ext Alert Port (TAAS) has associated hardware.

**Related topics:**

[Ext Alert Port \(TAAS\)](#) on page 500

***IAS Att. Access Code***

The extension number of the attendant group at the main server running Communication Manager. Required when IAS Branch is enabled. Not available if the Centralized Attendant feature is enabled.

**Related topics:**

[IAS \(Branch\)](#) on page 501

[Centralized Attendant](#) on page 954

### **IAS (Branch)**

Enables or disables the Inter-PBX Attendant Service (IAS) Branch feature. Not available if Centralized Attendant is enabled.

#### **Related topics:**

[Centralized Attendant](#) on page 954

### **IAS Tie Trunk Group No.**

Not available if the Centralized Attendant feature is enabled.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 2000   | The number of the tie trunk group to the main for the IAS (Branch). Required when IAS Branch is enabled. |

#### **Related topics:**

[Centralized Attendant](#) on page 954

### **Night Service Act. Ext.**

The extension of the current night service activation station, if any. The station is administered by assigning it a **night-serv** button.

### **QSIG CAS Number**

Contains the complete number of the attendant group at the main server running Avaya Communication Manager, or a Vector Directory Number (VDN) local to the branch server. Accepts up to 20 digits. Cannot be left blank. Available only for an QSIG-branch CAS configuration.

#### **Related topics:**

[CAS](#) on page 499

### **RLT Trunk Group No.**

The trunk group number corresponding to the Release Link Trunk (RLT) trunk group to the main location when supporting CAS Branch service. Available only for a branch CAS configuration.

#### **Related topics:**

[CAS](#) on page 499

### **Console parameters: page 2**

#### **ABBREVIATED DIALING**

List1, List2, List3

Assigns up to three abbreviated dialing lists to each attendant. A personal list cannot be assigned to an attendant.

| Valid Entry | Usage  |
|-------------|--|
| enhanced    | Allows the attendant to access the enhanced system abbreviated dialing list.                             |
| group       | Allows the attendant to access the specified group abbreviated dialing list. A group number is required. |
| system      | Allows the attendant to access the system abbreviated dialing list.                                      |

SAC Notification

Enables or disables Enhanced Attendant Notification for Send All Calls.

**COMMON SHARED EXTENSIONS**

Busy Indicator for Call Parked on Analog Station Without Hardware?

Enables or disables the Busy Indicator lamp that lights for incoming calls parked on Administration Without Hardware (AWOH) stations.

Count

| Valid Entry        | Usage   |
|--------------------|---|
| 1 to 1182<br>blank | The number of consecutive extensions, beginning with the Starting Extension used as common, shared extensions |

**Example**

If you enter a starting extension of 4300 and a count of 3, the system provides three consecutive extension numbers (4300, 4301, and 4302) for parking calls.

**Related topics:**

[Starting Extension](#) on page 502

Starting Extension

The first extension number in a group of consecutive extensions that can be used by the attendant to park calls.

**Related topics:**

[Count](#) on page 502

**INCOMING CALL REMINDERS**

Alerting (sec)

The number of seconds after which a held or unanswered call is disconnected from an attendant loop and routed to another attendant or night service.

No Answer Timeout (sec)

| Valid Entry         | Usage   |
|---------------------|---|
| 10 to 1024<br>blank | The number of seconds a call to the attendant can remain unanswered without invoking a more insistent sounding tone. Allow 5 seconds for each |

| Valid Entry | Usage  |
|-------------|--|
|             | ring at all points in a coverage path to ensure the entire path is completed before the call returns to the console. |

### Secondary Alert on Held Reminder Calls?

| Valid Entry | Usage   |
|-------------|---|
| y           | Begin attendant alerting for Held Reminder Calls with secondary alerting.   |
| n           | Have held reminder calls alert the attendant the same as normal calls. Normal calls start with primary alerting and then switch to secondary alerting when an administered timeout expires. |

### Related topics:

[No Answer Timeout \(sec\)](#) on page 502

### TIMING

#### Overview timer to Group Queue (sec)

| Valid Entry | Usage   |
|-------------|---|
| 10 to 1024  | The number of seconds a returning call queues to the individual attendant before overflowing to the group. The value applies if the attendant who previously handled the call is busy or unavailable. |
| blank       | The call immediately goes to the group.   |

#### Return Call Timeout (sec)

| Valid Entry         | Usage   |
|---------------------|---|
| 10 to 1024<br>blank | The time in seconds before a split away call (call extended and ringing a station or otherwise split away from the console) returns to the console. Allow 5 seconds for each ring at all points in a coverage path to ensure the entire path is completed before the call returns to the console. |

#### Time In Queue Warning (sec)

| Valid Entry       | Usage  |
|-------------------|--|
| 9 to 999<br>blank | The number of seconds a call can remain in the attendant queue before activating an alert. |

#### Time Reminder on Hold (sec)

| Valid Entry | Usage  |
|-------------|--|
| 10 to 1024  | The number of seconds a call can remain on Hold. |

**Console parameters: page 3**

**Call-Type Ordering Within Priority Levels?**

Groups calls to the attendant in the following order:

1. Queue priority level
2. Call type
3. Order received

| Call type   | Description  |
|-------------|--|
| Type 1 call | Outgoing public-network calls receiving answer supervision when the Answer Supervision Timer of the trunk group expires, even if the trunk is actually still ringing. Also, incoming calls when answered by the attendant.   |
| Type 2 call | Incoming external public-network calls before they receive answer supervision or before the Answer Supervision Timer of the trunk group expires.   |
| Type 3 call | All other calls (internal calls, conference calls, and tie-trunk calls of any type). Note that external public-network calls have priority over all other calls including conference calls. Answered public-network calls have priority over those calls not yet answered. |

| Valid Entry | Usage  |
|-------------|--|
| y           | Orders calls by call type within each queue priority category. A <b>type-disp</b> button is assigned to the Attendant Console. The attendant can review the call type for the active call. |
| n           | Calls are queued in chronological order by queue priority level.   |

**QUEUE PRIORITIES**

Assigns a priority level from 1 through 13 to each call category when the call cannot be immediately terminated to an attendant. The calling party hears ringback until an attendant answers the call.

The same priority level can be assigned to more than one call.

**Assistance Call**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 13     | Assigns a priority level for assistance calls. A call from a telephone user who dials the attendant-group access code, or from a telephone that has the Manual Originating Line Service feature activated. Priority 1 is the highest priority. |

## DID to Attendant

| Valid Entry | Usage   |
|-------------|---|
| 1 to 13     | Assigns a priority level for DID to Attendant calls that are incoming DID trunk calls to an attendant group. This does not include trunk calls that return to the attendant group after a timeout or deferred attendant recall. Priority 1 is the highest priority. |

## Emergency Access

| Valid Entry | Usage   |
|-------------|---|
| 1 to 13     | Assigns a priority level for emergency access calls that are calls from a telephone user who dials the emergency access code. The default is 1. Priority 1 is the highest priority. |

## Individual Attendant Access

| Valid Entry | Usage   |
|-------------|---|
| 1 to 13     | Assigns a priority level for Individual Attendant Access calls that are calls from a telephone user, incoming trunk call, or a system feature to the Individual Attendant Access (IAA) extension of a specific attendant. If the attendant is busy, the call queues until the attendant is available. Priority 1 is the highest priority. |

## Interposition

| Valid Entry | Usage   |
|-------------|---|
| 1 to 13     | Assigns a priority level for Interposition calls that are calls from one attendant to the Individual Attendant Access (IAA) extension of another attendant. Priority 1 is the highest priority. |

## Miscellaneous Call

| Valid Entry | Usage  |
|-------------|--|
| 1 to 13     | Assigns a priority level for any other calls not listed. Priority 1 is the highest priority. |

## Redirected Call

| Valid Entry | Usage  |
|-------------|--|
| 1 to 13     | Assigns a priority level for any calls assigned to one attendant, but redirected to the attendant group because the attendant is now busy. Priority 1 is the highest priority. |

## Managing inventory

### Redirected DID Call

| Valid Entry | Usage  |
|-------------|--|
| 1 to 13     | Assigns a priority level for any DID or ACD calls that time out due to ring/no-answer, busy condition (if applicable), or Number Unobtainable. Calls are rerouted to the attendant group.<br>Priority 1 is the highest priority. |

### Return Call

| Valid Entry | Usage  |
|-------------|--|
| 1 to 13     | Assigns a priority level for any calls returned to the attendant after timing out. If the attendant is now busy, the call redirects to the attendant group.<br>Priority 1 is the highest priority. |

### Serial Call

| Valid Entry | Usage   |
|-------------|---|
| 1 to 13     | Assigns a priority level for any calls from the Attendant Serial Call feature when an outside trunk call (designated as a serial call by an attendant) is extended to and completed at a telephone, and then the telephone user goes on-hook. If the attendant who extended the call is busy, the call redirects to the attendant group.<br>Priority 1 is the highest priority. |

### Tie Call

| Valid Entry | Usage   |
|-------------|---|
| 1 to 13     | Assigns a priority level for incoming TIE trunk calls (dial-repeating or direct types) to an attendant group. This does not include trunk calls that return to the attendant group after a timeout or deferred attendant recall.<br>Priority 1 is the highest priority. |

### VIP Wakeup Reminder Call

| Valid Entry | Usage   |
|-------------|---|
| 1 to 13     | Assigns a priority level for VIP Wakeup Reminder Calls from the Hospitality feature that send a wake-up reminder to the attendant to call a hotel or motel room.<br>Priority 1 is the highest priority. |

## Console parameters: page 4

### **QUEUE PRIORITIES**

#### Flash

| Valid Entry | Usage  |
|-------------|--|
| 1 to 17     | The queue priority for Flash precedence level calls. |

## Flash Override

| Valid Entry | Usage   |
|-------------|---|
| 1 to 17     | The queue priority for Flash Override precedence level calls. |

## Immediate

| Valid Entry | Usage  |
|-------------|--|
| 1 to 17     | The queue priority for Immediate precedence level calls. |

## Priority

| Valid Entry | Usage   |
|-------------|---|
| 1 to 17     | The queue priority for Priority precedence level calls. |

## Console parameters: page 5

 **Note:**

If MLPP is not enabled, the MLPP Queues page does not appear, and a page with the following message displays:

Use the 'list attendant' command to see all administered attendants.

## Coverage Answer Group

Establishes Call Coverage Answer Groups.

An answer group contains up to eight members who act as a coverage point for another user. For example, if several secretaries are responsible for answering a department's redirected calls, all the secretaries could be assigned to an answer group. The answer group is assigned a group number, and that group number appears in the department's coverage path. All telephones in an answer group ring (alert) simultaneously. Any member of the group can answer the call.

Each coverage answer group is identified by a number from 1 through the maximum number allowed by your system configuration. The members of the group are identified by their extension number. Any telephone, including those administered without hardware (but not attendants) can be assigned to a coverage answer group.

 **Note:**

The members administered without hardware are not be alerted.

Example command: `change coverage answer-group n`, where *n* is the assigned group number.

### Ext

The extension number for each member of this coverage answer group. This number cannot be a Vector Directory Number (VDN) extension.

### Group Name

The group name used to identify this group. Accepts up to 27 characters. Use the extension numbers of group members as the group name to help when determining which stations are involved in call coverage and trunk coverage paths.

#### Example

“typing pool”, “room 12”, “secy”

### Group Number

The number associated with the Cover Answer Group.

### Name

The name assigned when the member’s telephone was administered.

## Coverage Path

Implements Call Coverage Paths by providing the means to specify the call coverage criteria, the points in the coverage path used to redirect calls, and the number of times a principal’s telephone rings before the call redirects to coverage.

Example command: `change coverage path n`, where *n* is the assigned coverage path number.

### Coverage Path Number

The coverage path being administered.

### Holiday Coverage

Holiday coverage must be set separately for both inside and outside calls.

| Valid Entry | Usage  |
|-------------|--|
| y           | Sends the call to an announcement.                     |
| n           | Sends the call to the next point in the coverage path. |

### Holiday Table

The number of the holiday table used for holiday coverage.

### Hunt After Coverage

| Valid Entry | Usage   |
|-------------|---|
| y           | Coverage treatment continues by searching for an available station in a hunt chain that begins with the hunt-to-station assigned to the station of the last coverage point. |
| n           | Coverage treatment is terminated; the call is left at the last available location (principal or coverage point).  |

**Linkage**

One or two additional coverage paths in the coverage path chain.

**Next Path Number**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 9999   | The number of the next coverage path in a coverage path chain. If the coverage criteria of the current coverage path is not satisfied, the system steps down this chain until it finds a coverage path with redirection criteria that matches the call status. If the chain is exhausted before the system finds a match, the call does not redirect to coverage. |
| blank       | This path is the only path for the principal.   |

**COVERAGE CRITERIA**  
**COVERAGE CRITERIA**

Assigns coverage criteria that when met, redirects the call to coverage.

| Valid entries       | Usage  |
|---------------------|--|
| Active              | Calls redirect if at least one call appearance is busy.  |
| Busy                | Calls redirect if all call appearances that accept incoming calls are busy.  |
| Don't Answer        | Calls redirect when the specified number of rings has been exceeded.   |
| All                 | Calls redirect immediately to coverage. Overrides any other criteria administered for this field.  |
| DND/SAC/Go to Cover | Allows a calling user, when calling to another internal extension, to redirect a call immediately to coverage by pressing a <b>Go to Cover</b> button. Allows a principal temporarily to direct all incoming calls to coverage, regardless of the other assigned coverage criteria by pressing the <b>Send All Calls</b> (or <b>Do Not Disturb</b> ) button. <b>Send All Calls</b> also allows covering users to temporarily remove their telephones from the coverage path. Must be assigned before a user can activate Do Not Disturb (Hospitality Services), Send All Calls (SAC), or Go to Cover features. |
| Logged off/PSA/TTI  | This field appears only when the <b>Criteria for Logged Off/PSA/TTI Stations</b> field is set to y. Calls redirect to coverage after the number of rings exceeds the number specified in the <b>Number of Rings</b> field. By default, the value of the <b>Criteria for Logged Off/PSA/TTI Stations</b> field is y. The associated <b>Number of Rings</b> field appears only when the <b>Logged off/PSA/TTI</b> field is set to y.   |

**Number of Rings**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 99     | The number of times a telephone rings before the system redirects the call to the first point in the coverage path. By default, the value is 2. |

**COVERAGE POINTS**

**Point1, Point2, Point3, Point4, Point5, Point6**

The alternate destinations that comprise a coverage path. Coverage points must be assigned sequentially without steps beginning with Point 1. Each path can have up to six coverage points.

Subsequent coverage points should not be listed if calls are redirected to:

- Message Center, a special Uniform Call Distribution hunt group
- Voice messaging
- The attendant

These calls normally queue and never redirect to another coverage point. Calls to any hunt group queue if possible. Calls redirect from a hunt group only if all hunt group members are busy and either the queue is full or there is no queue.

If the Coverage of Calls Redirected Off-Net feature is not enabled, a remote coverage point functions as the last point in the coverage path because the system no longer has control of the call once it has redirected off-net. However, if the Coverage of Calls Redirected Off-Net feature is enabled, a call redirected off-net can be monitored by the system and brought back for further call coverage processing.

| Valid Entry   | Usage   |
|---|---|
| extension   | Redirects the call to an internal extension or announcement.<br><br> <b>Note:</b><br>When entering a Multi-Location Dial Plan shortened extension in a field designed for announcement extensions, certain administration end validations that are normally performed on announcement extensions are not done, and resultant warnings or submittal denials do not occur. The shortened extensions also do not appear in any display or list that shows announcement extensions. Extra care should be taken to administer the correct type of announcement for the application if assigning shortened extensions. |
| attd  | Redirects the call to the attendant or attendant group. If the system has Centralized Attendant Service (CAS), the call goes to the CAS attendant.  |
| h1 to h999  | Redirects the call to the corresponding hunt-group. For example, h32 routes to hunt group 32.   |
| c1 to c750<br>c1 to c1000<br>(S8300D/duplex<br>Media Servers) | Redirects the call to the corresponding coverage answer group. For example, c20 routes to call coverage answer group 20.  |
| r1 to r999<br>r1 to r1000<br>S8300D/duplex<br>(Media Servers) | Redirects the call to the corresponding remote coverage point number. For example, r27 routes to remote coverage point 27.  |

| Valid Entry   | Usage  |
|---------------|--|
| v + extension | Redirects the call to the corresponding VDN extension. For example, v12345 routes to the VDN associated with extension 12345.<br><br> <b>Note:</b><br>A Vector Directory Number can be used only as the last administered point in a coverage plan. |

**Rng**

| Valid Entry      | Usage   |
|------------------|---|
| 1 to 99<br>blank | The number of rings at this coverage point before the system redirects the call to the next point in the coverage path. |

**Terminate to Coverage Pts. with Bridged Appearances**

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows a call to alert as both a bridged call and a redirected call.           |
| n           | The call skips the coverage point if it has already alerted as a bridged call. |

**Crisis Alert System Parameters**

Defines the system parameters associated with sending crisis alert messages.

Example command: `change system-parameters crisis-alert`

**ALERT STATION****Every User Responds**

Controls who needs to respond to a crisis alert.

| Valid Entries | Usage   |
|---------------|---|
| y             | All users who have a crisis alert button are notified and must clear the alert for every emergency alert. Crisis alert buttons should be assigned only to attendant consoles and stations that must be notified of an emergency call.   |
| n             | All users are notified, but only one user needs to acknowledge an alert. This user might be the attendant or any other digital telephone with a crisis alert button. When the alert is acknowledged by one user, the alert is cleared at all stations except the one that acknowledged the alert. |

**ALERT PAGER****Alert Pager**

Allows or denies use of the Crisis Alert to a Digital Pager.

**Crisis Alert Code**

The first three digits in the crisis alert pager message. This should be the numbers used to call the local emergency service or any digits used for an emergency situation (for example, 911).

Required when Crisis Alert to a Digital Pager is enabled.

**Related topics:**

[Alert Pager](#) on page 511

**DTMF Duration - Tone (msec)**

Available only when Crisis Alert to a Digital Pager is enabled.

| Valid Entry                      | Usage   |
|----------------------------------|---|
| 20 to 2550 (in increments of 10) | The length of time the Dual-Tone Multi-Frequency (DTMF) tone is heard for each digit. |

**Related topics:**

[Alert Pager](#) on page 511

**Main Number**

Identifies the location where the crisis alert call originated. It can be the main number to the location or a numerical identification. Any dashes are for display purposes only and not included in the message sent to the pager. This entry is the last group of digits displayed in the pager message. Accepts up to 15 digits. Available only when Crisis Alert to a Digital Pager is enabled.

**Related topics:**

[Alert Pager](#) on page 511

**Originating Extension**

Required when Crisis Alert to a Digital Pager is enabled.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 7      | Requires a valid unassigned extension according to the dial plan |

**Related topics:**

[Alert Pager](#) on page 511

**Pager Number**

The number for the pager that is alerted when an emergency number is dialed. Accepts up to 15 digits. Any dashes are for display purposes only and not included in the message sent to the pager. At least one pager number must be entered if Crisis Alert to a Digital Pager is enabled.

**Pause (msec)**

Available when Crisis Alert to a Digital Pager is enabled.

| Valid Entry                      | Usage   |
|----------------------------------|---|
| 20 to 2550 (in increments of 10) | The length of time between DTMF tones for each digit. |

**Related topics:**

[Alert Pager](#) on page 511

**Pin Number**

If the page service requires one, the PIN associated with the pager. The PIN can be up to 15 digits. Also accepts the p (pause), # and \* characters.

A pause of up to 2 seconds is used for the timing of the message. For instance, a pause might be necessary in order to allow time for the pager service to set up the correct pager message box.

Available only if Crisis Alert to a Digital Pager is enabled.

**Related topics:**

[Alert Pager](#) on page 511

**Retries**

Available when Crisis Alert to A Digital Pager is enabled.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 10     | The number of times the system tries to send out the alert message in case of an unsuccessful attempt. This increases the chances that the pager receives a crisis alert message. |

**Related topics:**

[Alert Pager](#) on page 511

**Retry Interval (sec)**

Available when the Crisis Alert to a Digital Pager is enabled and **Retries** is set to a value from 1 to 10.

| Valid Entry | Usage  |
|-------------|--|
| 30 to 60    | The time in seconds between retries. If an attempt to call the pager fails, the retry call attempts after the retry interval period. |

**Related topics:**

[Alert Pager](#) on page 511

[Retries](#) on page 513

## CTI Link

Available if either ASAI Link Core Capabilities or Computer Telephony Adjunct Links are enabled on the system.

Example command: `add cti-link n`, where *n* is the CTI link number.

### Related topics:

[ASAI Link Core Capabilities](#) on page 943

[Computer Telephony Adjunct Links](#) on page 944

### CTI link: page 1

#### **COR**

Class of Restriction (COR) number with the desired restriction.

#### **CTI Link**

The Computer Telephony Integration (CTI) link number.

#### **Extension**

The extension for this link.

#### **Name**

The name associated with this CTI link.

#### **Port**

For an ASAI or ADJLK CTI link, the seven characters that specify a port.

| Valid Entry | Usage  |
|-------------|--|
| 01 to 64    | First and second numbers are the cabinet number  |
| A to E      | Third character is the carrier   |
| 01 to 20    | Fourth and fifth characters are the slot number  |
| 01 to 32    | Sixth and seventh characters are the circuit number                                    |
| x           | Indicates that there is no hardware associated with the port assignment. Use for AWOH. |

#### **Type**

| Valid Entry                        | Usage              |
|------------------------------------|--------------------|
| ADJLK<br>ADJ-IP<br>ASAI<br>ASAI-IP | The CTI link type. |

**BRI OPTIONS****CRV Length**

Available for ASAI or ADJLK CTI links.

| Valid Entry | Usage                                |
|-------------|--------------------------------------|
| 1 to 2      | The length of CRV for each interface |

**Fixed TEI**

Indicates whether or not the endpoint has a fixed Terminal Endpoint Identifier (TEI). TEIs are administered for fixed TEI terminals. Available for ASAI or ADJLK CTI links.

**MIM Support**

Indicates if Management Information Message (MIM) support is enabled for an ASAI or ADJLK link.

**XID**

For an ASAI or ADJLK CTI link, identifies Layer 2 XID testing capability.

**CTI link: page 2****Block CMS Move Agent Events**

Enables or disables the blocking of certain event report messages involved with the move of agents while staffed. If the Call Management System sends an agent-move-while-staffed message (MVAGSFD8), ASAI does not send the associated agent Logout Event Report (C\_Logout), Login Event Report (C\_login) and Agent Work Mode Change event report messages.

**Event Minimization**

Enables or disables event minimization for this link that limits the number of event reports sent to an adjunct. This option can be used when event reports normally would be sent on multiple associations, but the adjunct does not need to see more than one. Typically, these event reports are identical except for the association they are sent over (for example, call control, domain control, or active notification). Some applications discard duplicate events, so in this case, there is no point in sending them across the ASAI CTI link. When enabled, this option allows only a single such event to be sent. The selection of the association on which the event is sent is based on association precedence as follows: active notification (if enabled), call control (if enabled), or domain control (if enabled).

**Send Disconnect Event for Bridged Appearance**

Indicates whether or not an event report is sent when a bridged appearance disconnects.

**Special Character for Restricted Number**

Enables or disables an ASAI CTI link that indicates the calling number restricted presentation within an event report. When enabled, a calling number received in a SETUP message has the presentation indicator set (octet 3a in the calling number), then "\*" is appended to the calling party number in the ASAI message.

**Two-Digit Aux Work Reason Codes**

Enables or disables sending two-digit Reason Codes over the ASAI link. All messages that include Aux Work Reason Codes allow codes from 1 to 99.

**Related topics:**

[Two-Digit Aux Work Reason Codes](#) on page 622

## Data Module

Example command: `change data-module n`, where *n* is the module number.

### Data module: page 1

#### **BCC**

Indicates the value that corresponds to the speed setting of the data module. Used with Data Line, Netcon, Processor Interface, Point-to-Point Protocol, Processor/Trunk (pdm selection), and System Port Data Modules. This field can be compared with the BCC value in an associated routing pattern when attempted calls utilizing the data module fail to complete. The BCC values must be the same.

Available only when ISDN-PRI or ISDN-BRI trunks are enabled.

| Valid Entry | Usage              |
|-------------|--------------------|
| 1           | Relates to 56-kbps |
| 2, 3, 4     | Relates to 64 kbps |

**Related topics:**

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

#### **Connected to**

Used with Data Line and Processor/Trunk (pdm selection) Data Modules.

| Valid Entry | Usage   |
|-------------|---|
| dte         | The Asynchronous Data Unit (ADU) is connected to Data Terminal Equipment. |
| isn         | The ADU is connected to the Information Systems Network.                  |

#### **COS**

Not available for ethernet.

| Valid Entry | Usage                       |
|-------------|-----------------------------|
| 0 to 15     | The COS for the data module |

#### **COR**

Does not appear for ethernet.

| Valid Entry | Usage                    |
|-------------|--------------------------|
| 0 to 995    | The allowed restriction. |

**Data Extension**

The extension number assigned to the data module. This value must agree with the system dial plan. Accepts a one- to five-digit number.

**ITC**

The Information Transfer Capability (ITC) is used with 7500, Announcement, data-line, Netcon, Processor/ Trunk (pdm selection), Processor Interface, and System Port Data Modules. Indicates the type of transmission facilities used for ISDN calls originating from this endpoint. Not available for voice-only or BRI stations.

| Valid Entry  | Usage   |
|--------------|---|
| restricted   | Either restricted or unrestricted transmission facilities are used to complete the call. A restricted facility is a transmission facility that enforces 1's density digital transmission. In other words, a sequence of 8 digital zeros are converted to a sequence of 7 zeros and a digital 1. |
| unrestricted | Only unrestricted transmission facilities are used to complete the call. An unrestricted facility is a transmission facility that does not enforce 1's density digital transmission. In other words, digital information is sent exactly as is.   |

**Name**

The name of the user associated with the data module. The name is optional and can be blank. Accepts up to 27 alphanumeric characters.

 **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Port**

A port location to which the data module is connected. Used with 7500, Data Line, Ethernet, Processor/Trunk, PPP, System Port, and World Class BRI Data Modules.

| Characters | Meaning        | Value                         |
|------------|----------------|-------------------------------|
| 1 to 2     | Cabinet number | 1 to 64 (S87XX Series IP-PNC) |
| 3          | Carrier        | A to E                        |
| 4 to 5     | Slot number    | 0 to 20                       |

| Characters | Meaning        | Value   |
|------------|----------------|---|
| 6 to 7     | Circuit Number | <ul style="list-style-type: none"> <li>• 01 to 31—S87XX Series IP-PNC (tdm, pdm) configurations</li> <li>• 01 to 16—ppp for S87XX Series IP-PNC</li> <li>• 01 to 08—system-port for S87XX Series IP-PNC</li> <li>17/33 (Ethernet on S87XX Series IP-PNC)</li> </ul> |

 **Note:**

An x in the **Port** field indicates that there is no hardware associated with the port assignment (also known as Administration Without Hardware (AWOH). These stations are referred to as “phantom stations”. If this data module is designated as a secondary data module, x cannot be entered. The port of a primary data module cannot be changed to x if a secondary data module is administered.

**Remote Loop-Around Test**

Used with Processor/Trunk Data Modules. Available with a pdm or tdm type trunk.

| Valid Entry | Usage   |
|-------------|---|
| y           | The data module supports a loop-back test at the EIA interface. In general, Avaya equipment supports this test but it is not required by Level 2 Digital Communications Protocol. |
| n           | Abort a request for this test   |

**Related topics:**

[Type](#) on page 519

**Secondary data module**

Used with Processor/Trunk Data Modules. Available with a pdm type trunk. The primary data module must be administered before the secondary data module can be added. A data module that is administered without port hardware cannot be a secondary data module.

| Valid Entry | Usage   |
|-------------|---|
| y           | This PDM is the secondary data module used for Dual I-channel AUDIX networking. |
| n           | This is the primary PDM, or this data module is not used for AUDIX networking.  |

**Related topics:**

[Port](#) on page 517

[Type](#) on page 519

**TN**

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

**Type**

The type of data module.

| Valid Entry  | Usage  |
|--------------|--|
| 7500         | Assigns a 7500 Data Module. The 7500 data module supports automatic TEI, B-channel, maintenance and management messaging, and SPID initialization capabilities. BRI endpoints, both voice or data, are assigned to either the ISDN-BRI - 4-wire S/T-NT Interface circuit pack or the ISDN-BRI - 2-wire U circuit pack. Each can support up to 12 ports. Since BRI provides multipoint capability, more than one ISDN endpoint (voice or data) can be administered on one port. For BRI, multipoint administration allows for telephones having SPID initialization capabilities, and can only be allowed if no endpoint administered on the same port is a fixed tie endpoint and no station on the same port has B-channel data capability. Currently, multipoint is restricted to two endpoints per port.  |
| announcement | Assigns an announcement data module. The announcement data module is built-in to the integrated announcement circuit pack. This data module allows the system to save and restore the recorded announcements file between the announcement circuit pack and the system memory.   |
| data-line    | <p>Assigns a Data Line Data Module. Allows for administered ports on the Data Line circuit pack (DLC) that allows EIA 232C devices to connect to the system. The DLC, with a companion Asynchronous Data Unit (ADU), provides a less expensive data interface to the system than other asynchronous DCP data modules.</p> <p>The DLC supports asynchronous transmissions at speeds of Low and 300, 1200, 2400, 4800, 9600, and 19200 bps over 2-pair (full-duplex) lines. These lines can have different lengths, depending on the transmission speed and wire gauge.</p> <p>The DLC has eight ports. The connection from the port to the EIA device is direct, meaning that no multiplexing is involved. A single port of the DLC is equivalent in functionality to a data module and a digital line port. The DLC appears as a data module to the Digital Terminal Equipment (DTE) and as a digital line port to the server running Communication Manager.</p> <p>The DLC connects the following EIA 232C equipment to the system:</p> <ul style="list-style-type: none"> <li>• Printers</li> <li>• Non-Intelligent Data Terminals</li> <li>• Intelligent Terminals, Personal Computers (PCs)</li> </ul> |

| Valid Entry | Usage   |
|-------------|---|
|             | <ul style="list-style-type: none"> <li>• Host Computers</li> <li>• Information Systems Network (ISN), RS-232C Local Area Networks (LANs), or other data switches</li> </ul>   |
| ethernet    | Assigns an Ethernet data module. Allows for administration of a 10BaseT port on the Control-LAN (C Lan) circuit pack. This port provides a TCP/IP connection to network hub or LAN.   |
| ni-bri      | Assigns an NI-BRI Data Module.  |
| pdm         | <p>Assigns a DCE interface for Processor/Trunk Data Modules. Allows for administration of a Modular Processor Data Modules (MPDMs) and Modular Trunk Data Modules (MTDMs).</p> <p>The MPDM, 7400B, or 8400B Data Module provides a Data Communications Equipment (DCE) interface for connection to equipment such as data terminals, CDR output devices, on-premises administration terminal, Message Server, Property Management System (PMS), AUDIX, and host computers. It also provides a Digital Communications Protocol (DCP) interface to the digital switch. (DCE is the equipment on the network side of a communications link that provides all the functions required to make the binary serial data from the source or transmitter compatible with the communications channel.)</p> <p>The MTDM provides an Electronic Industries Association (EIA) Data Terminal Equipment (DTE) interface for connection to off-premises private line trunk facilities or a switched telecommunications network and a DCP interface for connection to the digital switch. (DTE is the equipment comprising the endpoints in a connection over a data circuit. For example, in a connection between a data terminal and a host computer, the terminal, the host, and their associated modems or data modules make up the DTE.) The MTDM or 7400A Data Module also can serve as part of a conversion resource for Combined Modem Pooling.</p> |
| ppp         | Assigns a Point-to-Point Protocol data module. Allows for administration of a synchronous TCP/IP port on the Control Lan (C-Lan) circuit pack. These ports are tailored to provide TCP/IP connections for use over telephone lines.   |
| system-port | Assigns a System Port Data Module.  |
| tdm         | Assigns a DTE interface for Processor/Trunk Data Modules. See the pdm entry above.  |
| wcbri       | Assigns a World Class BRI Data Module.  |

**ABBREVIATED DIALING**

List1

The abbreviated dialing list for the data module. Used with 7500, Data Line, Netcon, Processor/Trunk, Processor Interface, and World Class BRI Data Modules. Supports Data Hot Line. This field can be left blank.

| Valid Entry | Usage                                      |
|-------------|--|
| e           | Enhanced                                   |
| g           | Group — requires a group list number       |
| p           | Personal — requires a personal list number |
| s           | System                                     |

### **ASSIGNED MEMBER**

#### Ext and Name

The extension number and name of the previously administered user with associated Data Extension buttons, who shares the module. Used with Data Line, Announcement, Netcon, Processor/Trunk, Processor Interface, and System Port Data Modules.

### **SPECIAL DIALING OPTION**

Identifies the type of dialing for calls when this data module originates calls. Used with 7500, Data Line, Netcon, Processor/Trunk, Processor Interface, and World Class BRI Data Modules.

| Valid Entry | Usage   |
|-------------|---|
| hot-line    | When the user goes off-hook on the data module, the hot line destination number gets dialed.  |
| default     | When the user goes off-hook on the data module and presses <b>Enter</b> at the DIAL prompt, the default dialing destination number gets dialed. |
| blank       | Normal keyboard dialing   |

### **Data module: page 2: Type data-line**

#### **CAPABILITIES**

##### Busy Out

Enables or disables the placement of the DLC port in a busied-out state once the DTE control lead to the DLC is dropped. This option should be enabled for DTEs that are members of a hunt group and to allow “busy out” when DTE turns power off so that calls do not terminate on that DTE.

##### Configuration

Allows or denies the viewing and changing of options from the DTE. Available only when **KYBD Dialing** is enabled. This option normally is enabled for “originate/ receive” DTE such as non-intelligent terminals and disabled for intelligent devices such as computers.

#### **Related topics:**

[KYBD Dialing](#) on page 521

##### KYBD Dialing

#### **Note:**

ADU-type hunt groups connecting the system to terminal servers on a host computer should have these hunt group extensions assigned as “no” keyboard dialing.

| Valid Entry | Usage  |
|-------------|--|
| y           | Enables keyboard dialing, allowing data endpoints to originate calls using the EIA 232C interface and obtain ASCII feedback text. The user gets the dial prompt. This option normally is enabled for a “originate/receive” DTE that has a need to set up data calls.                           |
| n           | Disables keyboard dialing. Originations cannot be done at the DTE and text feedback does not occur at the DTE during call setup or take down. Data call answering is still allowed but without text feedback. If the <b>Low</b> speed setting is enabled, keyboard dialing should be disabled. |

**OPTIONS**

Answer Text

Available only with **KYBD Dialing**.

Applies to the following messages:

- INCOMING CALL
- ANSWERED
- DISCONNECTED
- DISCONNECTED OTHER END

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows text messages to be delivered to the DTE when a call is being answered. Applies to DLC-generated text as well as text received from the system.                         |
| n           | The system still generates the text, but the DLC prevents it from being sent to the device. Usually is disabled when the answering DTE is a computer or an intelligent device. |

**Related topics:**

[KYBD Dialing](#) on page 521

Connected Indication

Available only with **KYBD Dialing**.

| Valid Entry | Usage   |
|-------------|---|
| y           | Generates a “CONNECTED” message to the DTE when the connection has been established.  |
| n           | The connected indication is provided by the DLC activating its EIA 232C control lead. |

**Related topics:**

[KYBD Dialing](#) on page 521

## Dial Echoing

Available only with **KYBD Dialing**.

| Valid Entry | Usage  |
|-------------|--|
| y           | Echos characters back to the DTE.  |
| n           | Disables Dial Echoing. Dial Echoing should be disabled when keyboard dialing is done by an intelligent device. |

**Related topics:**

[KYBD Dialing](#) on page 521

## Disconnect Sequence

Selects the sequence for a disconnect. Available only with **KYBD Dialing**.

| Valid Entry | Usage                                   |
|-------------|---|
| long-break  | A long-break is greater than 2 seconds. |
| two-breaks  | Two-breaks is within 1 second.          |

**Related topics:**

[KYBD Dialing](#) on page 521

## Parity

| Valid Entry                  | Usage   |
|------------------------------|---|
| even<br>odd<br>mark<br>space | The type of parity. The DLC generates the parities when call setup text is sent to the DTE. The DLC does not check the parity when receiving dialing characters. Parity has nothing to do with the far end; it is used by the DLC to terminal communications during call setup. Available only with <b>KYBD Dialing</b> . |

**Related topics:**

[KYBD Dialing](#) on page 521

## Permit Mismatch

Enables or disables the Permit Mismatch feature. Permit Mismatch:

- Allows the EIA interface to operate at a rate different than that agreed to in the data module handshake. The data module handshake is always the highest compatible rate as determined by the reported speed option of each data module.
- Instructs the DLC to operate at the highest selected speed, which is a higher rate than the far-end data module. The DLC reports the highest-optioned speed, all the lower speeds, or the previously-selected auto-adjust speed during the handshake process.
- Eliminates the need to change the DTE/DLC speed every time a call is placed to and from an endpoint operating at a different speed.

 **Caution:**

Caution must be used when using this option to send information from a DTE/ DCE that is transmitting data at higher rates than that of the far end. Sustained usage of this type transmission results in loss of data. Whenever this option is enabled, the DTE must match the highest speed selected for the associated DLC port.

This option is intended to be used by a DTE device operating locally at a higher baud rate than that of its far-end connection but transmitting relatively low amounts of data (for example, a user typing at a terminal).

 **Note:**

The Low speed setting is not reported as an available speed when **Permit Mismatch** is enabled.

**Related topics:**

[SPEEDS](#) on page 524

**SPEEDS**

Enables or disables the following operating speeds:

| Valid Entry                           | Usage   |
|---------------------------------------|---|
| Low                                   | Instructs the DLC to operate at a low speed from 0 to 1800 bits per second (bps). Disable if <b>KYBD Dialing</b> is enabled.  |
| 300, 1200, 2400, 4800, 9600, or 19200 | The DLC can be any one of these speeds. The speed is matched for the duration of the call, from call setup to call takedown. For multiple speeds, three or more should be selected. When multiple speeds are selected and autoadjust is disabled, the DTE's speed must be the highest selected speed. This is required because all feedback text is delivered to the DTE at the highest selected speed. |
| Autoadjust                            | <ul style="list-style-type: none"> <li>• Tells the DLC port to automatically adjust to the operating speed and to the parity of the DTE it is connected to</li> <li>• Can be used with any of the speeds listed</li> <li>• Applies only to calls originated by the user through Keyboard Dialing</li> <li>• Available only when <b>KYBD Dialing</b> is enabled</li> </ul>                               |

**Related topics:**

[KYBD Dialing](#) on page 521

**Data module: page 2 - Type 7500, WC-BRI, NI-BRI  
BRI LINK/MAINTENANCE PARAMETERS**

**Endpt Init**

Indicates whether or not the terminal's endpoint has initialization capability. Endpoint initialization is a procedure, required for multipoint operation, by which User Service Order Profile (USOP) is associated with an endpoint on the ISDN-BRI. This association is made through the Service Profile Identifier (SPID), administered into the system and entered into the ISDN-BRI terminal. For a ISDN-BRI terminal to become operational in a multipoint

configuration, both the administered SPID and the SPID programmed into the ISDN-BRI terminal must be the same. This means that the SPID of the new or re-used terminals must be programmed to match the administered SPID value. Used with 7500, World Class BRI, and NI-BRI Data Modules.

#### Fixed TEI

Indicates whether or not the endpoint has Fixed Terminal Equipment Identifier (TEI) capability. TEI identifies a unique access point within a service. For Fixed TEI stations, the TEI must be administered. For terminals with automatic TEI capability, the associated TEI is assigned by the system. Used with 7500, World Class BRI, and NI-BRI Data Modules.

#### MIM Mtce/Mgt

Enables or disables Management Information Message (MIM) support. MIM provides terminal support for MIM Maintenance and Management capabilities, other than endpoint initialization. Used with 7500 Data Modules.

#### MIM Support

Enables or disables the capability of MIM endpoint initialization (SPID support), and other Maintenance/Management. Used with 7500 Data Modules.

#### SPID

The Service Profile Identifier (SPID) is a variable parameter of up to 10 digits. The SPID must be different for all terminals on the ISDN-BRI and from the Service SPID. The SPID should always be assigned. If the SPID is not assigned for the first ISDN-BRI on a port, any other ISDN-BRI assignment to that port is blocked. Used with 7500, World Class BRI, and NI-BRI Data Modules. Available only if **Endpt Init** is enabled.

#### Related topics:

[Endpt Init](#) on page 524

#### TEI

Available only if **Fixed TEI** is enabled.

| Valid entry | Usage   |
|-------------|---|
| 0 to 63     | The Terminal Endpoint Identifier (TEI) is a layer 2 addressing parameter used by Communication Manager to exchange information with BRI endpoints over the point-to-point signaling link. Used with 7500, World Class BRI, and NI-BRI Data Modules. |

#### Related topics:

[Fixed TEI](#) on page 525

#### XID

Enables or disables layer 2 Exchange identification (XID) testing capability. Used with 7500, World Class BRI, and NI-BRI Data Modules. In almost all cases, Avaya recommends that XID is disabled.

## Date and Time

Sets the system date and time, selects the daylight savings plan number, if any, and shows whether the current time is standard time or daylight savings. Settings on this screen affect the internal clock and timestamp of the server running Communication Manager. Update the date and time for a leap year or a system restart after a power failure. The correct date and time assure that CDR records are correct. CDR does not work until the date and time have been entered.

Example command: `set time`

### Day of the Month

| Valid entry | Usage   |
|-------------|---|
| 1 to 31     | The current day of the month. The system clock uses this as the current date. |

### Day of the Week

| Valid Entry             | Usage   |
|-------------------------|---|
| Sunday through Saturday | The current day of the week. The system clock uses this as the current day. |

### Daylight Savings Rule

| Valid Entry | Usage   |
|-------------|---|
| 0 to 15     | The daylight savings rule in use for the system. The system clock uses this as the current daylight savings rule. |

#### Related topics:

[Daylight Savings Rules](#) on page 527

### Hour

| Valid Entry | Usage   |
|-------------|---|
| 0 to 23     | The current hour to be used by the system clock. The system uses a 24-hour clock. For example, 14:00 is the same as 2:00 p.m. |

### Minute

| Valid Entry | Usage   |
|-------------|---|
| 0 to 59     | The current minute. The system clock uses this as the current minute. |

**Month**

| Valid Entry         | Usage   |
|---------------------|---|
| January to December | The current month. The system clock uses this as the current month. |

**Second**

Displays the seconds and cannot be modified. Resets to zero when saved.

**Type**

| Valid Entry      | Usage   |
|------------------|---|
| daylight-savings | Indicates daylight savings time is in effect. |
| standard         | Indicates standard time is in effect.         |

**Year**

The current year in 20XX format. The system clock uses this as the current year.

**Daylight Savings Rules**

Administers up to 15 customized daylight savings rules. Specifies the exact date and time each daylight savings rule goes into effect and when it stops. Rule 0 makes no adjustment to the system clock for daylight savings and cannot be modified.

In this example, Rule 1 applies to all time zones in the U.S. and begins on the first Sunday on or after March 8 at 2:00 a.m. with a 01:00 increment. Daylight Savings Time stops on the first Sunday on or after November 1 at 2:00 a.m., also with a 01:00 increment used as a decrement when switching back to Standard time. Telephone displays reflect these settings.

```
1: Start: first _ Sunday_ on or after _March 8_ at 2:00_ 01:00__
   Stop: first _ Sunday_ on or after November 1_ at 2:00_
```

Example command: `change daylight-savings-rules`

**Change Day (Start)**

| Valid Entry        | Usage   |
|--------------------|---|
| Sunday to Saturday | The day of the week the clock moves ahead to begin daylight savings                                 |
| Day                | The clock changes on the exact date entered for <b>Month (Start)</b> and <b>Date (Start)</b> values |

**Related topics:**

[Month \(Start\)](#) on page 528

### Change Day (Stop)

| Valid Entry        | Usage   |
|--------------------|---|
| Sunday to Saturday | The day of the week the clock moves back to standard time   |
| Day                | The clock changes on the exact date entered for the <b>Month (Stop)</b> and <b>Date (Stop)</b> values |

#### Related topics:

[Month \(Stop\)](#) on page 528

### Date (Start)

| Valid Entry | Usage  |
|-------------|--|
| 0 to 31     | The day of the month the clock moves ahead to begin daylight savings |

### Date (Stop)

| Valid Entry | Usage  |
|-------------|--|
| 0 to 31     | The day of the month the clock moves back to standard time |

### Increment (Start)

| Valid Entry | Usage   |
|-------------|---|
| 0 to 23     | The number of hours the clock moves ahead for daylight savings and moves back to return to standard time                |
| 0 to 59     | The number of minutes you want the clock to move ahead for daylight savings and to move back to return to standard time |

### Month (Start)

| Valid Entry         | Usage   |
|---------------------|---|
| January to December | The month the clock moves ahead to begin daylight savings |

### Month (Stop)

| Valid Entry         | Usage   |
|---------------------|---|
| January to December | The month the clock moves back to standard time |

### Rule

The daylight savings rule number.

**Time (Start)**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 23     | The hour the clock moves ahead to begin daylight savings. The system uses a 24-hour clock. For example, 14:00 is the same as 2:00 p.m. |
| 0 to 59     | The minute the clock moves ahead to begin daylight savings   |

**Time (Stop)**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 23     | The hour the clock moves back to standard time. The system uses a 24-hour clock. For example, 14:00 is the same as 2:00 p.m. |
| 0 to 59     | The minute the clock moves back to standard time   |

**DCS to QSIG TSC Gateway**

Determines when and how to convert messages from an administered AUDIX NCA-TSC to a QSIG NCA-TSC. Maps the AUDIX NCA-TSC to the appropriate machine ID index to find the QSIG subscriber entry in the QSIG MWI-Prefix screen. Assigns the voice mail number used when a DCS served-user node interrogates a QSIG message center.

Available only if **Interworking with DCS** is enabled for the system.

Example command: `change isdn dcs-qsig-tsc-gateway`

**Related topics:**

[Interworking with DCS](#) on page 955

**AAR/ARS Access Code**

The AAR/ARS Access Code. Accepts up to four digits, including characters \* and #.

**Mach ID**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 20     | A unique machine ID. Do not repeat a machine ID if it is already associated with a processor channel on an Ethernet link. |

**Sig Grp**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 650    | The assigned signaling group number for each machine ID. |

**TSC Index**

The TSC Index for each machine ID.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 64     | The assigned signaling group number for the qsig-mwi application type. |

**Voice Mail Number**

The complete Voice Mail Dial Up number. Accepts up to 17 digits.

**Dial Plan Analysis Table**

The Dial Plan Analysis Table is the system’s guide to translating the digits dialed by users. It determines the beginning digits and total length for each type of call that Communication Manager needs to interpret. The Dial Plan Analysis Table and the Dial Plan Parameters screen work together to define the system’s dial plan.

Example command: `change dialplan analysis`

**Call Type**

| Valid Entry | Usage   |
|-------------|---|
| aar         | Automatic Alternate Routing — Routes calls within a company's own private network. Requires that <b>ARS/ AAR Dialing without FAC</b> is enabled.  |
| ars         | Automatic Route Selection — Routes calls that go outside a company over public networks. ARS also routes calls to remote company locations when there is not a private network. Requires that <b>ARS/ AAR Dialing without FAC</b> is enabled.   |
| attd        | Attendant — Defines how users call an attendant. If a telephone's COR restricts the user from originating calls, this user cannot access the attendant using this code. The attendant access code can also be administered by entering an fac or dac.   |
| dac         | Dial access code — Allows the use of trunk access codes (TAC) and feature access codes (FAC) in the same range.   |
| enb-ext     | Enbloc extension — Defines a block of extensions that must be dialed using a prefix when the caller dials from a keypad. These extensions can be dialed without a prefix if the caller dials enbloc, for example, from a station call log.  |
| ext         | Primary extension — Defines extension ranges that can be used on the system. Extension can have a first digit of 0 through 9 and can be one to seven digits in length. Extension cannot have the same first digit as a 1-digit ARS or AAR feature access code (FAC).  |
| fac         | Feature access code only — Users dial an FAC instead of programming a button.   |
| pext        | Prefixed extension — Identifies the call type as an extension. After digit collection, the prefix digit is removed from the string of dialed digits. The remaining digits make up the extension number and are then processed. A prefixed extension allows the use of extensions numbers with any dialed string. The extension length must be specified on the table. |

| Valid Entry | Usage   |
|-------------|---|
| udp         | Uniform Dial Plan — Shares a common dial plan among a group of servers. |

**Related topics:**

[UDP Extension Search Order](#) on page 534

[Dial Access](#) on page 724

[ARS/AAR Dialing without FAC](#) on page 943

**Dialed String**

The digits that Communication Manager analyzes to determine how to process the call. Two Dial Plan entries can use the same Dialed String only if the Dialed String consists of one digit. Longer Dialed Strings must all be unique. A new entry cannot be administered if it causes an existing extension, feature access code, or trunk access code to become inaccessible.

| Call Type | Valid Entry      | Usage   |
|-----------|------------------|---|
| aar       | 0 to 9           | Numbers can be one to four digits.  |
| ars       | 0 to 9           | Numbers can be one to four digits.  |
| attd      | 0 to 9           | Numbers can be one to two digits.   |
| dac       | 0 to 9<br>*<br># | Characters can be one to four digits.<br>The characters "*" and "#" can only be used as a first digit.  |
| ext       | 0 to 9           | Numbers can be one to seven digits.<br>The extension cannot have the same first digit as a one-digit ARS or AAR feature access code (FAC).  |
| fac       | 0 to 9<br>*<br># | Characters can be one to four digits.<br>The characters "*" and "#" can only be used as a first digit.<br>A FAC must have the longest total length for a given dialed string when using mixed numbering.<br>Otherwise, problems might occur when, for example, three-digit FACs and four-digit extensions begin with the same first digit and the FAC is an abbreviated dialing list access code.<br>However, if the entry in the dial plan that defines the FAC is used to define the AAR or ARS access code, then it must have the longest total length in the dial plan. |
| pext      | 0 to 9           | The prefix is the first digit (0–9) and an extension number of up to five digits in length.<br>The maximum length of a prefix and extension combination is six digits.<br>A prefixed extension cannot have the same first digit as a dial access code.<br>A prefixed extension cannot have the same dialed string as the ARS or AAR FAC.  |

| Call Type | Valid Entry | Usage                        |
|-----------|-------------|------------------------------|
| udp       | 0 to 9      | Can be used with any length. |

**Location**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 250    | (Depending on your server configuration, see <i>Avaya Aura™ Communication Manager System Capacities Table</i> , 03-300511.) The location of the endpoint that is dialing the digits. Available only if <b>Multiple Locations</b> is enabled for the system. See the Location sections in <i>Avaya Aura™ Communication Manager Feature Description and Implementation</i> , 555-245-205, for the other ways, and for a list of features that use location. |
| all         | Indicates that this table is the default for all port network (cabinet) locations. Available only if <b>Multiple Locations</b> is disabled for the system.  |

**Related topics:**

[Multiple Locations](#) on page 948

**Percent Full**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 100    | The percentage of system memory resources that have been allocated for the dial plan currently used. |

**Total Length**

The number of digits for this call type. Must be greater than or equal to the number of digits in the Dialed String.

| Valid Entry | Usage |
|-------------|-------|
| 1 to 2      | attd  |
| 1 to 4      | dac   |
| 1 to 4      | fac   |
| 1 to 7      | ext   |
| 2 to 6      | pext  |

**Related topics:**

[Dialed String](#) on page 531

## Dial Plan Parameters

The Dial Plan Parameters screen works with the Dial Plan Analysis Table to define the system dial plan.

It also controls the appearance of digit extensions on station displays. These multi-digit extensions can be hard to read as a block. Communication Manager allows you to select the display format for 6- to 13-digit extensions.

Example command: `change dialplan parameters`

### AAR/ARS Internal Call Prefix

The digits entered here get concatenated with the calling or called extension. Accepts up to eight digits that does *not* include \* or #. Available only when **ARS/AAR Dialing Without FAC** is enabled for the system. Requires administration of **AAR/ARS Internal Call Total Length**.

#### Related topics:

[AAR/ARS Internal Call Total Length](#) on page 533

[ARS/AAR Dialing without FAC](#) on page 943

### AAR/ARS Internal Call Total Length

Available only if **ARS/AAR Dialing Without FAC** is enabled for the system.

| Valid Entry      | Usage   |
|------------------|---|
| 6 to 10<br>blank | The total length of the internal call digit string, including the Internal Call Prefix and the calling or called extension. Requires administration of an <b>AAR/ARS Internal Call Prefix</b> . |



#### Note:

The longest extension length on the Dial Plan Analysis table, plus the length of the **ARS/AAR Internal Call Prefix**, must be equal to or greater than the **ARS/AAR Internal Call Total Length** value.

#### Related topics:

[ARS/AAR Dialing without FAC](#) on page 943

### ETA Node Number

| Valid Entry       | Usage   |
|-------------------|---|
| 1 to 999<br>blank | The number of the destination server for Extended Trunk Access (ETA) calls. ETA calls are unrecognized numbers you can send to another switch for analysis and routing. Such numbers can be Facility Access Codes, Trunk Access Codes, or extensions that are not in the UDP table. |

### ETA Routing Pattern

| Valid Entry | Usage  |
|-------------|--|
| 1 to 999    | The number of the routing pattern to reach the destination server. |

### Local Node Number

| Valid Entry | Usage  |
|-------------|--|
| 1 to 63     | Identifies a specific node in a server network. Must match the DCS switch node number and the CDR node number if they are specified. |
| blank       | Leave blank if automatic restoration, DCS, and CDR are not used.   |

### Retry ARS Analysis if All-Location Entry Inaccessible

Available with Communication Manager Release 4.0.x or later.

| Valid Entry | Usage  |
|-------------|--|
| y           | The system finds and uses the best possible entry in the per-location ARS table, if the all-location table points to a trunk group that cannot be accessed because the network has fragmented. |
| n           | The system does not retry ARS analysis when a trunk group cannot be accessed, because the network has fragmented.  |

### UDP Extension Search Order

Specifies the first table to search to match a dialed extension. If the dialed extension is not found in the specified place, it searches for it in the alternate place. Available if **Uniform Dialing Plan** is enabled for the system.

| Valid Entry            | Usage  |
|------------------------|--|
| local-extensions-first | Searches the local server first to match a dialed extension; if not found, then uses the UDP tables to route the call.       |
| udp-table-first        | Searches the UDP tables for an off-switch conversion; if not found, then searches the local server for the dialed extension. |

#### Related topics:

[Uniform Dialing Plan](#) on page 950

### EXTENSION DISPLAY FORMATS

#### *Extension display format*

Specifies how the system punctuates extensions for display. The punctuation field is divided into two columns, one for Inter-Location/SAT displays, and one for Intra-Location displays.

In Communication Manager 6.0, the Inter-Location/SAT column is divided into two columns. You can insert a dial prefix in the Inter-Location column, if appropriate, before an enbloc extension. This allows called stations store a dialable number in their call logs.

**\* Note:**

The maximum length of a displayed extension (including punctuation) is 13 characters. You need to trade off a punctuation mark so that you can insert a prefix digit. You cannot insert a prefix digit or a punctuation into the inter-location format for a 13 digits extension.

Blank spaces are sometimes used in telephone extensions, especially outside of the U.S. Dots (.) are used on SAT screens in place of blanks. The following table gives the maximum number of punctuation marks permitted for each extension length.

The number of punctuation marks that the system allows is determined by the number of “x” s in the format.

- If the format contains fewer than six “x”s, no punctuation marks can be entered.
- If the format contains six or more “x”s, the maximum number of punctuation marks is determined by the following table.

| Extension Length | Maximum Punctuation Marks | Maximum Total Length |
|------------------|---------------------------|----------------------|
| 6                | 2                         | 8                    |
| 7                | 1                         | 8                    |
| 8                | 3                         | 11                   |
| 9                | 3                         | 12                   |
| 10               | 3                         | 13                   |
| 11               | 2                         | 13                   |
| 12               | 1                         | 13                   |
| 13               | 0                         | 13                   |

| Valid Entry | Usage  |
|-------------|--|
| xx.xx.xx    | Can contain all “x” characters (no punctuation) or a combination of “x” characters and 0 to 2 hyphens (-), spaces, or periods (.) to depict how extensions display. A format must be specified or the default takes effect. This field cannot be left blank. The default values for the 8-, 9-, 10-, 11-, 12-, and 13-digit fields are shown in the following example. |

EXTENSION DISPLAY FORMATS

|                     | SAT            | Inter-Location | Intra-Location |
|---------------------|----------------|----------------|----------------|
| 6-Digit Extension:  | xx.xx.xx       | xx.xx.xx       | xx.xx.xx       |
| 7-Digit Extension:  | xxx-xxxx       | xxx-xxxx       | xxx-xxxx       |
| 8-Digit Extension:  | xx.xx.xx.xx    | xx.xx.xx.xx    | xx.xx.xx.xx    |
| 9-Digit Extension:  | xxx-xxx-xxx    | xxx-xxx-xxx    | xxx-xxx-xxx    |
| 10-Digit Extension: | xxx-xxx-xxxx   | xxx-xxx-xxxx   | xxx-xxx-xxxx   |
| 11-Digit Extension: | xxxx-xxx-xxxx  | xxxx-xxx-xxxx  | xxxx-xxx-xxxx  |
| 12-Digit Extension: | xxxxxx-xxxxxx  | xxxxxx-xxxxxx  | xxxxxx-xxxxxx  |
| 13-Digit Extension: | xxxxxxxxxxxxxx | xxxxxxxxxxxxxx | xxxxxxxxxxxxxx |

## Digit Absorption

Implements up to five-digit absorption lists. Digit Absorption is required for each local telephone company central office (CO) and for a Foreign eXchange (FX) trunk group connected to a CO. Each outgoing digit string from the server running Communication Manager to the CO is treated according to entries in the Absorption Treatment Assignment section of the screen.

Available only if Digit Absorption is administered for the trunk group.

Example command: `change digit-absorption n`, where *n* is the absorption digit.

### Related topics:

[Digits](#) on page 995

## Absorption Treatment Assignment

| Valid Entry | Usage  |
|-------------|--|
| A to F      | The chosen treatment letter. All choices for the digits 0 through 9 must be taken from the same group (Group I or Group II). |

## Absorption Treatment Information

Shows how Digit Absorption treats each digit, 0 through 9, depending on the assignment of A through C for Group I, and A, D, E, and F for Group II.

## List Number

| Valid Entry | Usage  |
|-------------|--|
| 0 to 4      | The Digit Absorption List number that is referenced from the associated trunk group. |

## Display Parameters

Establishes how extensions of 6 to 13 digits are punctuated.

Example command: `change display-parameters`

### Related topics:

[Extension display format](#) on page 534

## EXTENSION DISPLAY FORMATS

The fields in this section of the screen override similar fields on the Dial Plan Parameters screen. If you leave these fields blank, the values on the Dial Plan Parameters screen apply.

### *Default Call Appearance Display Format*

Affects call appearances only on telephones that support downloadable call appearance buttons, such as the 2420 and 4620 telephones. Bridged call appearances are not affected.

| Valid Entry    | Usage  |
|----------------|--|
| inter-location | The complete extension on downloadable call appearance buttons. This is the default. |
| intra-location | A shortened version of the extension on downloadable call appearance buttons.        |

### **Extension Display Format**

Specifies how the system punctuates extensions for Inter-Location displays, and for Intra-Location displays. Blank spaces are sometimes used in telephone extensions, especially outside of the U.S. Dots (.) are used on SAT screens in place of blanks.

The number of punctuation marks that the system allows is determined by the number of “x”s in the format:

- If the format contains fewer than six “x”s, there can be no punctuation marks.
- If the format contains six or more “x”s, the maximum number of punctuation marks is determined by the following table.

| Extension Length | Maximum Punctuation Marks | Maximum Total Length |
|------------------|---------------------------|----------------------|
| 6                | 2                         | 8                    |
| 7                | 1                         | 8                    |
| 8                | 3                         | 11                   |
| 9                | 3                         | 12                   |
| 10               | 3                         | 13                   |
| 11               | 2                         | 13                   |
| 12               | 1                         | 13                   |
| 13               | 0                         | 13                   |

| Valid Entry       | Usage  |
|-------------------|--|
| xx.xx.xx<br>blank | For six or more “x”s, characters can contain: <ul style="list-style-type: none"> <li>• All “x” characters without punctuation</li> <li>• A combination of “x” characters and up to two hyphens</li> <li>• Spaces</li> <li>• Periods</li> </ul> |

### **Inter-Location**

Specifies punctuation for calls between locations. This is the default.

### **Intra-Location**

Specifies punctuation for calls within a location.

## DS1 Circuit Pack

Administers all DS1 circuit packs.

Example command: `add ds1 n`, where *n* is the board location.

### DS1 Circuit Pack: page 1

#### Bit Rate



**Note:**

TN464C and later release circuit packs have an option switch that must be set to match this **Bit Rate** value.

| Valid Entry | Usage   |
|-------------|---|
| 1.544       | The maximum transmission rate for DS1 circuit packs that support T-1 service. |
| 2.048       | The maximum transmission rate for DS1 circuit packs that support E-1 service. |

#### Channel Numbering

The ETSI and ISO QSIG specifications require that B-channels on an E1 be encoded as 1 to 30 in the Channel ID IE. Prior to the existence of this field, Avaya Communication Manager only used this scheme for Country Protocols 2a (Australia) and 13a (Germany 1TR6). Available only with ISDN-PRI signaling on a private network. The interface must be peer master or peer slave.

2.048 bit rate options:

- timeslot
- sequential

If Communication Manager is connected via QSIG trunks to a switch or server supporting the ETSI QSIG or ISO QSIG specifications, this field must be sequential.

#### Related topics:

[Bit Rate](#) on page 538

[Connect](#) on page 538

[Interface](#) on page 542

[Signaling Mode](#) on page 550

#### Connect

To control communications at layers 2 and 3 of the ISDN-PRI protocol, this field specifies what is on the far end of this DS1 link.

Available only for ISDN-PRI signaling.

| Valid Entry | Usage  |
|-------------|--|
| pbx         | The DS1 link is connected to another switch in a private network.  |
| line-side   | Communication Manager is acting as the network side of an ISDN-PRI interface. Used to connect to Roll About Video equipment. |
| network     | The DS1 link connects Communication Manager to a local telephone company central office or any other public network switch.  |
| host        | The DS1 link connects Communication Manager to a computer.   |

**Related topics:**

[Signaling Mode](#) on page 550

**Country Protocol**

The country protocol used by the far-end server. For connections to a public network, your network service provider can tell you which country protocol they are using.

Available only with ISDN-PRI and CAS signaling.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 25     | The country protocol used by the local telephone company central office at which this link terminates.   |
| etsi        | The network service provider uses the European Telecommunications Standards Institute (ETSI) protocol and the <b>Signaling Mode</b> is isdn-pri. |

**Related topics:**

[Signaling Mode](#) on page 550

[Country options table](#) on page 935

**CRC**

Indicates whether a cyclic redundancy check (CRC) will be performed on transmissions that the DS1 circuit pack receives.

| Valid Entry | Usage   |
|-------------|---|
| y           | The <b>Signaling Mode</b> is CAS and the DS1 link is providing E-1 service. |
| n           | All other applications.   |

**Related topics:**

[Signaling Mode](#) on page 550

**D-Channel**

Available only with a Japanese 2-Mbit trunk circuit pack and the ISDN-PRI **Signaling Mode**.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 31     | The Japanese 2-Mbit trunk circuit pack, when administered to support ISDN-PRI signaling, assigns the D-channel to any channel from 1 to 31 in an E-1 facility. |

**Related topics:**

[Signaling Mode](#) on page 550

**DCP/ANALOG Bearer Capability**

Sets the information transfer capability in a bearer capability IE of a setup message to speech or 3.1kHz. Available only with the ISDN-PRI **Signaling Mode**.

| Valid Entry | Usage   |
|-------------|---|
| 3.1kHz      | Provides 3.1 kHz audio encoding in the information transfer capability. |
| speech      | Provides speech encoding in the information transfer capability.        |

**Related topics:**

[Signaling Mode](#) on page 550

**Disable Restarts**

Controls whether outgoing RESTART messages are sent. Also used to disable QSIG restarts. Available when:

- Country Protocol is 3 (Japan)
- Country Protocol is ETSI
- Peer Protocol is QSIG

| Valid Entry | Usage  |
|-------------|--|
| y           | Outgoing restarts are disabled. In other words, RESTART messages are not sent. |
| n           | Outgoing RESTART messages are sent. This is the default.                       |

**DMI-BOS**

The DMI/BOS protocol is used for high-speed digital communications between a host computer and Communication Manager. With this 24-channel protocol, channels 1 to 23 of the DS1 link carry data and channel 24 carries control signaling. DMI/BOS has greater capacity than a robbed-bit 24-channel facility. Available only when **Signaling Mode** is common-chan.

| Valid Entry | Usage  |
|-------------|--|
| y           | Activates the Digital Multiplexed Interface-Bit Oriented Signaling (DMI-BOS) format. |
| n           | Uses an Avaya proprietary format.  |

**Related topics:**

[Signaling Mode](#) on page 550

**Framing Mode**

Selects either superframe or extended superframe for T1 service on the DS1 link. The framing mode must match the mode used on the other end of the link. Available only with T1 service.

 **Tip:**

Avaya recommends using ESF when the service provider supports it, especially if the facility gets upgraded to ISDN. The ESF format provides enhanced performance measurements and uses a sophisticated error-checking method to ensure data integrity.

| Valid Entry | Usage   |
|-------------|---|
| d4          | The basic DS1 superframe, or sf. Avaya recommends this mode only for voice traffic.   |
| esf         | The extended superframe format. Avaya recommends this mode for digital data traffic. A TN464F, TN767E, or a later suffix DS1 circuit pack requires the administration of ESF Data Link options. |

**Related topics:**

[Bit Rate](#) on page 538

[ESF DATA LINK OPTIONS](#) on page 554

**Idle Code**

 **Caution:**

The **Country Protocol** sets the default idle code. Do not change the default without assistance from Avaya or your network services provider.

| Valid Entry                       | Usage  |
|-----------------------------------|--|
| Any 8-digit string of 0's and 1's | Sets the signal sent out over idle DS0 channels. The string must be compatible with the protocol used by the far-end switch or server. |

**Related topics:**

[Country Protocol](#) on page 539

**Interconnect**

For E1 service using channel-associated signaling, tells Communication Manager whether the DS1 circuit pack is using a public or private network protocol. This value must agree with the **Group Type** value administered for the trunk group.

Available only if the **Signaling Mode** is CAS.

| Valid Entry | Usage   |
|-------------|---|
| pbx         | The board operates as a tie trunk circuit pack. |

| Valid Entry | Usage   |
|-------------|---|
| CO          | The board operates as a local telephone company central office (CO) or DID circuit pack. Use for Enterprise Mobility User (EMU)/EC500 administration. |

**Related topics:**

[Signaling Mode](#) on page 550

[Group Type](#) on page 725

**Interface**

Controls how the server negotiates glare with the far-end switch. The servers at either end of the DS1 link must have complementary settings in this field. Otherwise, the D-channel cannot function. For example, if the Avaya S8XXX server at one end of the link is administered as network, the other end must be administered as user. Available only when this DS1 link is providing an ISDN-PRI connection in a private network.

**Related topics:**

[Connect](#) on page 538

Private network applications in the U.S.

| Valid Entry | Usage  |
|-------------|--|
| network     | The server overrides the other end when glare occurs, and when connecting the server to a host computer.                               |
| user        | The server releases the contested circuit and looks for another when glare occurs, and when connecting the server to a public network. |

Private network applications outside the U.S.

| Valid Entry | Usage  |
|-------------|--|
| peer-master | The switch overrides the other end when glare occurs.                              |
| peer-slave  | The switch releases the contested circuit and looks for another when glare occurs. |

**Interface Companding**

The companding algorithm expected by the system at the far end.

| Valid Entry | Usage   |
|-------------|---|
| a-law       | Algorithm expected at the far-end for E1 service. |
| mu-law      | Algorithm expected at the far-end for T1 service. |

**Interworking Message**

Determines what message Communication Manager sends when an incoming ISDN trunk call is routed over a non-ISDN trunk group.

| Valid Entry | Usage  |
|-------------|--|
| PROGress    | Requests the public network to cut through the B-channel and let the caller hear tones such as ringback or busy tone provided over the non-ISDN trunk. Normally-selected value.  |
| ALERTing    | Causes the public network in many countries to play ringback tone to the caller. This value is used only if the DS1 is connected to the public network, and it is determined that callers hear silence (rather than ringback or busy tone) when a call incoming over the DS1 interworks to a non-ISDN trunk. |

### ITN-C7 Long Timers

Controls the T302 and T303 timers.

Available only if the **Signaling Mode** is isdn-pri.

| Valid Entry | Usage                                    |
|-------------|--|
| y           | Increases the length of the long timers. |
| n           | Uses the default long timers.            |

#### Related topics:

[Signaling Mode](#) on page 550

### Line Coding

Selects the type of line coding used on this facility. The setting in this field must match the setting on the far-end of the link, or there must be an intervening CSU to convert the line coding protocols. Voice calls work even if line coding does not match, but a single data call brings down the DS1 facility.



#### Caution:

If you change this field, you must busy out the DS1 circuit pack. You must also change the administration for: Route-Pattern, Access Endpoint, PRI Endpoint, Signaling-Group, and Trunk-Group.



#### Note:

When the DS1 circuit pack is used for ISDN service, the ISDN D-channel data is inverted when ami-basic or ami-zcs is used and not inverted when b8zs or hdb3 is used.

| Valid Entry | Usage  |
|-------------|--|
| b8zs        | Bipolar eight zero substitution. For T1 facilities that support voice or data traffic. Provides a 64K clear channel.   |
| ami-zcs     | Alternate mark inversion - zero code suppression. For T1 facilities that carry voice traffic. Avaya does not recommend this for digital-data applications. Use if this facility is going to be upgraded to ISDN. |
| ami-basic   | Alternate mark inversion-basic. For unrestricted E1 facilities.  |

| Valid Entry | Usage   |
|-------------|---|
| hdb3        | High density bipolar 3. For restricted E1 facilities.   |
| cmi         | Coded mark inversion. Used in Japan as the only type of line coding used with the Japanese 2 Mbit trunk circuit pack. |

**Line Compensation**

The appropriate entry in this field varies with the type of cable used. Contact your network service provider for the correct setting.

**Cable lengths for a DSX-1 cross-connect**

The following valid entries are for the different lengths of 22-gauge ABAM cable terminated on a DSX-1 cross-connect.

| Valid Entry | Usage                                   |
|-------------|---|
| 1           | Length: 000 – 133 (ft), 000 – 40.5 (m)  |
| 2           | Length: 133 – 266 (ft), 40.5 – 81.0 (m) |
| 3           | Length: 266 – 399 (ft), 81.0 – 122 (m)  |
| 4           | Length: 399 – 533 (ft), 122 – 163 (m)   |
| 5           | Length: 533 – 655 (ft), 163 – 200 (m)   |

**Cable lengths for a DS1 interface**

The following valid entries are for the different lengths of 22-gauge ABAM cable directly connected to DS1 interfaces.

| Valid Entry | Usage                                   |
|-------------|---|
| 1           | Length: 0000 – 0266 (ft), 000 – 081(m)  |
| 2           | Length: 0266 – 0532 (ft), 081 – 162 (m) |
| 3           | Length: 0532 – 0798 (ft), 162 – 243 (m) |
| 4           | Length: 0798 – 1066 (ft), 243 – 325 (m) |
| 5           | Length: 1066 – 1310 (ft), 325 – 400 (m) |

**Location**

The port address.

**MMI Cabling Board**

Available only with the Multimedia Call Handling feature.

| Valid Entry | Usage  |
|-------------|--|
| xxxxx       | Location of the multimedia interface circuit pack that is connected to the Expansion Services Module (ESM). The location can be a the cabinet, carrier, or slot address. |

**Related topics:**

[Multimedia Call Handling \(Basic\)](#) on page 948

[Multimedia Call Handling \(Enhanced\)](#) on page 948

**MMI Interface**

Displays the type of multimedia interface if **MMCH** is enabled and there is a value for the **MMI Cabling Board** .

**Related topics:**

[MMI Cabling Board](#) on page 544

[Multimedia Call Handling \(Basic\)](#) on page 948

[Multimedia Call Handling \(Enhanced\)](#) on page 948

**Name**

Assigns a significant, descriptive name to the DS1 link. Use the vendor's circuit ID for the link in this field because that information helps troubleshoot problems with the link. This field can also be used to indicate the function or the destination of this DS1 facility. Accepts up to 15 characters.

**Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Peer Protocol**

Administers the peer level protocol that operates in a private network. Available only if **Interface** is peer-master or peer-slave.

| Valid Entry | Usage  |
|-------------|--|
| Q-SIG       | This implements QSIG Network Basic Call. Available only if Basic Call Setup is enabled for the system. |
| TTC         | For private networking. Requires a Digital Trunk (Japan 2 MB TTC) (TN2242) circuit pack.               |

**Related topics:**

[Interface](#) on page 542

[Basic Call Setup](#) on page 954

**Protocol Version**

Available only when:

The **Signaling Mode** is isdn-pri and the **Connect** type is network.

The **Signaling Mode** is isdn-pri, the **Connect** type is pbx, and the **Interface** type is user or network.

| Valid Entry | Usage  |
|-------------|--|
| a, b, c, d  | Selects the protocol that matches the network service provider's protocol in countries whose public networks allow multiple layer-3 signaling protocols for ISDN-PRI service. Contact the network service provider to verify that the protocols match. |



**Warning:**

The AT&T Switched Network Protocol does not support restricted displays of connected numbers. Display problems occur if you administer the 1a country-protocol/ protocol-version combination on the DS1 screen and administer the ISDN-PRI Trunk Group to restrict sending the connected number.

**Related topics:**

[Connect](#) on page 538

[Interface](#) on page 542

[Signaling Mode](#) on page 550

Public network signaling administration for ISDN-PRI Layer 3

The following table describes the Communication Manager public-network access connections for ISDN-PRI Layer 3.

| Admin Value | Country               | Protocol Supported   | B-channel mtce msg |
|-------------|-----------------------|--|--------------------|
| 1-a         | United States, Canada | AT&T TR 41449/ 41459 (tested with AT&T network, Canadian network, and MCI network) | Service            |
| 1-b         | United States         | Telcordia Technologies TR 1268; NIUF.302; ANSI T1.607                              | Restart            |
| 1-c         | United States         | NORTEL DMS-250 BCS36/ IEC01  | Service            |
| 1-d         | United states         | Telecordia Technologies SR-4287  | Service            |
| 2-a         | Australia             | AUSTEL TS014.1; Telecom Australia TPH 1856 National ISDN protocol                  | Restart            |
| 2-b         | Australia             | ETSI ISDN protocol   | Restart            |

| Admin Value | Country                  | Protocol Supported  | B-channel mtce msg |
|-------------|--------------------------|---|--------------------|
| 3           | Japan                    | NTT INS-NET   | Restart            |
| 4           | Italy                    | ETS 300 102   | Restart            |
| 5           | Netherlands              | ETS 300 102   | Restart            |
| 6           | Singapore                | ETS 300 102   | Restart            |
| 7           | Mexico                   | ETS 300 102   | Restart            |
| 8           | Belgium                  | ETS 300 102   | Restart            |
| 9           | Saudi Arabia             | ETS 300 102   | Restart            |
| 10-a        | United Kingdom           | ETS 300 102 (for connection to DASS II/ DPNSS through external converter) | Restart            |
| 10-b        | United Kingdom, Ireland  | ETS 300 102 (Mercury); British Telecom ISDN 30; Telecom Eireann SWD 109   | None               |
| 11          | Spain                    | Telefonica ISDN Specification   | Restart            |
| 12-a        | France                   | VN4 (French National PRI)   | None               |
| 12-b        | France                   | ETS 300 102 modified according to P10-20, called Euronumeris              | None               |
| 13-a        | Germany                  | FTZ 1 TR 6 (German National PRI)  | None               |
| 13-b        | Germany                  | ETS 300 102   | Restart            |
| 14          | Czech Republic, Slovakia | ETS 300 102   | Restart            |
| 15          | Russia (CIS)             | ETS 300 102   | Restart            |
| 16          | Argentina                | ETS 300 102   | Restart            |
| 17          | Greece                   | ETS 300 102   | Restart            |
| 18          | China                    | ETS 300 102   | Restart            |
| 19          | Hong Kong                | ETS 300 102   | Restart            |
| 20          | Thailand                 | ETS 300 102   | Restart            |
| 21          | Macedonia                | ETS 300 102   | Restart            |
| 22          | Poland                   | ETS 300 102   | Restart            |
| 23          | Brazil                   | ETS 300 102   | Restart            |
| 24          | Nordic                   | ETS 300 102   | Restart            |

| Admin Value | Country                   | Protocol Supported | B-channel mtce msg |
|-------------|---------------------------|--------------------|--------------------|
| 25          | South Africa              | ETS 300 102        | Restart            |
| ETSI-a      | Europe, New Zealand, etc. | ETS 300 102        | Restart            |
| ETSI-b      |                           | ETS 300 102        | None               |

**Received Digital Metering Pulse Maximum (ms)**

Available only when the **Signal Mode** is cas (Channel Associated Signaling), the **Interconnect** type is co or pbx, and the **Country Protocol** is administered for a protocol that uses periodic pulse metering (PPM).

| Valid Entry                          | Usage   |
|--------------------------------------|---|
| 20 to 1000 ms in increments of 10ms. | This value must be greater than the <b>Received Digital Metering Pulse Minimum</b> value and match the value used by the network services provider. |

**Related topics:**

[Country Protocol](#) on page 539

[Interconnect](#) on page 541

[Received Digital Metering Pulse Minimum \(ms\)](#) on page 548

[Signaling Mode](#) on page 550

**Received Digital Metering Pulse Minimum (ms)**

Available only when the **Signal Mode** is cas (Channel Associated Signaling), the **Interconnect** type is co or pbx, and the **Country Protocol** is administered for a protocol that uses periodic pulse metering (PPM).

| Valid Entry                         | Usage   |
|-------------------------------------|---|
| 20 to 1000 ms in increments of 10ms | This value must be greater than the <b>Received Digital Metering Pulse Maximum</b> value and match the value used by the network services provider. |

**Related topics:**

[Country Protocol](#) on page 539

[Interconnect](#) on page 541

[Received Digital Metering Pulse Maximum \(ms\)](#) on page 548

[Signaling Mode](#) on page 550

**Received Digital Metering Pulse Value**

Available only when the **Signal Mode** is cas (Channel Associated Signaling), the **Country Protocol** is 21, and the **Interconnect** type is co or pbx.

| Valid Entry | Usage  |
|-------------|--|
| 0, 1        | This value must match the value used by the network services provider. |

**Related topics:**

[Country Protocol](#) on page 539

[Interconnect](#) on page 541

[Signaling Mode](#) on page 550

## Incoming digital PPM

The following table provides the incoming digital PPM signaling default per country protocol code.

| Code | Country        | PPM Min (ms) | PPM Max (ms) | PPM Value |
|------|----------------|--------------|--------------|-----------|
| 0    | null           | NA           | NA           | NA        |
| 1    | U.S.           | NA           | NA           | NA        |
| 2    | Australia      | 80           | 180          | 0         |
| 3    | Japan          | NA           | NA           | NA        |
| 4    | Italy          | 120          | 150          | 1         |
| 5    | Netherlands    | 90           | 160          | 0         |
| 6    | Singapore      | NA           | NA           | NA        |
| 7    | Mexico         | 20           | 180          | 1         |
| 8    | Belgium        | 20           | 180          | 1         |
| 9    | Saudi Arabia   | NA           | NA           | NA        |
| 10   | UK             | NA           | NA           | NA        |
| 11   | Spain          | 20           | 220          | 0         |
| 12   | France         | NA           | NA           | NA        |
| 13   | Germany        | NA           | NA           | NA        |
| 14   | Czech Republic | 20           | 420          | 1         |
| 15   | Russia CIS     | NA           | NA           | NA        |
| 16   | Argentina      | 10           | 180          | 1         |
| 17   | Greece         | 100          | 180          | 1         |
| 18   | China          | NA           | NA           | NA        |
| 19   | Hong Kong      | NA           | NA           | NA        |
| 20   | Thailand       | 20           | 180          | 1         |
| 21   | Macedonia      | 120          | 180          | 1         |
|      | Croatia        | 20           | 80           | 1         |

| Code | Country      | PPM Min (ms) | PPM Max (ms) | PPM Value |
|------|--------------|--------------|--------------|-----------|
| 22   | Poland       | 100          | 150          | 0         |
| 23   | Brazil       | NA           | NA           | NA        |
| 24   | Nordic       | NA           | NA           | NA        |
| 25   | South Africa | 160          | 240          | 0, 1      |

**Side**

Controls how a server running Communication Manager resolves glare at layer 3 over an ISDN-PRI link in QSIG private networks. Available if the **Interface** type is peer-master or peer-slave.

 **Caution:**

It is critical that administration on this server correctly pairs with the administration of the far-end switch/server. If the far-end is administered as the “b” side, this field should be set to “a” regardless of whether the layer 2 designation is peer-master or peer-slave, and vice versa.

| Valid Entry | Usage  |
|-------------|--|
| a           | The <b>Interface</b> is peer-master. In other words, this server overrides the far-end when glare occurs.                                |
| b           | The <b>Interface</b> is peer-slave . In other words, this server releases the contested circuit and looks for another when glare occurs. |

**Related topics:**

[Interface](#) on page 542

**Signaling Mode**

Selects the signaling method used for the DS1 link. This mode must match the method used by the network services provider.

| Valid Entry | Usage  |
|-------------|--|
| CAS         | Channel Associated Signaling. Out-of band signaling with E1 service. This setting yields 30 64-kbps B-channels for voice or data transmission. Channel 0 is used for framing while channel 16 carries signaling. Used for Enterprise Mobility User (EMU)/EC500 administration. |
| robbed-bit  | In-band signaling with T1 service. This setting yields 24 56-kbps B-channels for voice transmission.   |
| isdn-pri    | Either T1 or E1 ISDN service. This setting supports both Facility Associated Signaling and Non-Facility Associated Signaling.  |
| isdn-ext    | Either T1 or E1 ISDN service. This setting supports only Non-Facility Associated Signaling.  |

| Valid Entry | Usage   |
|-------------|---|
|             |  <b>Note:</b><br>NFAS is primarily a feature for ISDN-T1 connections offered by service providers in North America and Hong Kong. However, it can also be used on private-network connections, and in that context it is possible to set up NFAS using ISDN-E1 interfaces. |
| common-chan | Out-of-band signaling with T1 service. This setting yields 23 64-kbps B-channels for voice or data transmission. Channel 24 is used for signaling.  |

**T303 Timer (sec)**

Available only if the **Group Type** is isdn-pri.

| Valid Entry | Usage  |
|-------------|--|
| 2 to 10     | The number of seconds the system waits for a response from the far end before invoking Look Ahead Routing. |

**Related topics:**

[Interface](#) on page 542

[Group Type](#) on page 725

**MAINTENANCE PARAMETERS****Alarm When PRI Endpoint Detached**

Enables or disables an alarm when the DS1 board detects a loss of signal. Used for DS1 circuit packs connected to Roll-About Video equipment.

Available only when the **Connect** type is line-side.

**Related topics:**

[Connect](#) on page 538

**Block Progress Indicator**

Blocks sending the progress indicator in the SETUP message.

Available only if the **Country Protocol** is set to 1 and the **Protocol Version** is set to b.

| Valid Entry | Usage   |
|-------------|---|
| y           | Prevents the progress indicator from being sent in the SETUP message. |
| n           | Allows the progress indicator to be sent.                             |

**Related topics:**

[Country Protocol](#) on page 539

[Protocol Version](#) on page 546

**EC Configuration**

The set of parameters used when cancelling echo. This information is stored in firmware on the UDS1 circuit pack.

Available only if echo cancellation is enabled for the DS1 circuit pack.

| Valid Entry  | Usage  |
|--------------|--|
| 1<br>5 to 15 | Provides the most rapid adaptation in detecting and correcting echo at the beginning of a call, regardless of the loudness of the talker's voice. For very loud talkers and severe echo, the far-end talker's speech is heard as clipped when both parties talk at the same time.  |
| 2            | Provides slightly slower adaptation to echo. Use if speech is often clipped when both parties talk at the same time.   |
| 3            | Provides slightly slower adaptation to echo but may result in a 2 or 3 second fade on strong echo for quiet talkers. Completely removes speech clipping.   |
| 4            | Used in cases of extreme echo, excessive clipping or breakup of speech. May result in slight echo or background noise.<br><br> <b>Note:</b><br>For the MM710, the values 1 and 4 are reversed. That is, 1 for the MM710 is the same as 4 for the TN464HP/ TN2464CP, and 4 for the MM710 is the same as 1 for the TN464HP/ TN2464CP. |

**Related topics:**

[Echo Cancellation](#) on page 552

**EC Direction**

Indicates the direction of the echo that is being cancelled.

Available only if echo cancellation is enabled for the DS1 circuit pack.

| Valid Entry | Usage  |
|-------------|--|
| inward      | Cancels echo energy coming back into Communication Manager . Energy from an outgoing call is reflected from an external reflection point. In other words, the party "inside" Communication Manager hears the echo. |
| outward     | Cancels echo energy going outside Communication Manager. Energy from an incoming call is reflected from an internal reflection point. In other words, the party "outside" Communication Manager hears the echo.    |

**Related topics:**

[Echo Cancellation](#) on page 552

**Echo Cancellation**

Enables or disables echo cancellation on the Universal DS-1 circuit pack.

Available only if DS1 echo cancellation is enabled on the system.

**Related topics:**

[DS1 Echo Cancellation](#) on page 945

## Near-end CSU

Available only when the DS1 circuit pack is a TN767D or TN464E or later suffix model, with a **Bit Rate** of 1.544 and a **Country Protocol** of 1 (U.S.).

| Valid Entry | Usage  |
|-------------|--|
| other       | No channel service unit is attached to the DS1 facility or the CSU is an external unit.  |
| integrated  | A 120A CSU module is attached to the DS1 board. This integrated channel service unit (ICSU) can accept software-administrable option downlinks. In other words, the ICSU can respond to test codes from technician's equipment and report its status. Requires administration of <b>Integrated CSU Options</b> . |

**Related topics:**

[Bit Rate](#) on page 538

[Country Protocol](#) on page 539

[INTEGRATED CSU OPTIONS](#) on page 555

## Slip Detection

Slips are synchronization errors that slow digital transmissions and can cause data loss. The server maintains a slip-count record for each DS1 interface to detect errors and evaluate their severity (the type of alarm). If as many as 50 percent of those spans administered for slip detection are experiencing slips (with respect to the primary), then a decision is made to switch to the secondary.

**Caution:**

Always enable slip detection for DS1 circuit packs that serve as primary or secondary synchronization references.

| Valid Entry | Usage  |
|-------------|--|
| y           | Maintenance software measures the slip-rate of this circuit pack and determines if it is excessive. Typically, for DS1 spans used for data applications and for spans used as synchronization references. This excludes all T1-spans connecting channel banks, unless the channel bank is externally timed. This entry enables switching between the primary and secondary synchronization references and an internal high-accuracy clock. |
| n           | For DMI-BOS links or when testing is not required. Typically used for DS1 spans that are used exclusively for voice and that do not serve as the primary or secondary synchronization source.  |

**DS1 circuit pack: page 2****Caution:**

Do not change fields on this page without assistance from Avaya or from the network service provider.

For those circuit packs that support it, this page is available only if the **Framing Mode** is esf or the **Near-end CSU** type is integrated.

**Related topics:**

[Framing Mode](#) on page 541

[Near-end CSU](#) on page 553

**CPE LOOPBACK JACK OPTIONS**

Supply CPE Loopback Jack Power

Enables or disables the DS1 board's ability to supply power to the equipment during loopback testing if a Customer Premise Equipment (CPE) Loopback Jack is installed.

**ESF DATA LINK OPTIONS**

Far-end CSU Address

Available only if the **Framing Mode** is esf.

| Valid Entry | Usage   |
|-------------|---|
| a, b        | Administers the transmit direction address used for the <b>ESF data Link</b> command with both integrated and external channel service units (CSU). |

**Related topics:**

[Framing Mode](#) on page 541

Network Management Protocol

Available only if the **Framing Mode** is esf.

| Valid Entry | Usage   |
|-------------|---|
| tabs        | Allows the data link to be remotely monitored. Used only with circuit packs that have an integrated channel service unit (CSU). |

**Related topics:**

[Framing Mode](#) on page 541

Send ANSI-T1.403 One-Second Performance Reports

Enables or disables sending error reports from the DS1 circuit pack to the far-end server or switch. These reports are useful for network management, and are sent at 1-second intervals when enabled.

Available only if the **Framing Mode** is esf. It is used only with circuit packs that have an integrated channel service unit (CSU).

Contact Avaya technical support to use these reports.

**Related topics:**

[Framing Mode](#) on page 541

**INTEGRATED CSU OPTIONS****Receive ALBO (Receive Automatic Line Build-Out)**

Increases the strength of incoming signals by a fixed amount to compensate for line losses. To set correctly, measure the signal loss on this specific facility.

| Valid Entry | Usage   |
|-------------|---|
| 26db        | Used for most applications.   |
| 36db        | Used for networks that do not conform to public telephone network standards, such as campus networks. |

**Transmit LBO (Transmit Line Build-Out)**

Reduces the outgoing signal strength by a fixed amount. The appropriate level of loss depends on the distance between your Communication Manager server (measured by cable length from the smart jack) and the nearest repeater. Where another server/switch is at the end of the circuit, as in campus environments, use the cable length between the two switches to select the appropriate setting from the table below.

Available only with an integrated near-end CSU.

| Valid Entry | Usage                               |
|-------------|-------------------------------------|
| 0db         | For distances of 2,001 – 3,000 feet |
| -7.5db      | For distances of 1,001 – 2,000      |
| -15db       | For distances of 0 – 1,000 feet     |
| -22.5db     | For mid-span repeaters              |

**Related topics:**

[Near-end CSU](#) on page 553

**Upon DTE LOS**

Tells Communication Manager what to do if the outgoing signal from the DS1 circuit pack, or Data Terminal Equipment (DTE), to the network is lost.

| Valid Entry | Usage  |
|-------------|--|
| loopback    | Returns the network signal to the network. This prevents any alarms from being generated at the far-end.   |
| ais         | Alarm Indicator Signal. Sends an unframed all-ones signal (the AIS or Blue Alarm) to the far-end server or switch. This option alerts the network service provider to the problem immediately and aids in troubleshooting. |

**Duplicate Station**

Adds telephones by copying the information from an existing telephone and modifying this information for each new telephone. For example, configure one telephone as a template for an entire work group, and then duplicate the template station to add all the other extensions

in the group. Only telephones of the same model can be duplicated. All the feature settings from the template telephone are copied to the new telephones.

Example command: `duplicate station n`, where *n* is the extension number.

**Related topics:**

[Station](#) on page 877

## Duplicate Vector

Duplicate vectors from an existing vector and edit the duplicate vectors to create vectors that are similar to the existing vector. You can use this functionality to configure one vector as a template that can be reused when creating similar vectors.

Example command: `duplicate vector n`, where *n* is the master vector.

### Assigned VDN

The first assigned VDN if a VDN was assigned to the master vector.

### More VDN's

Displays \* if there is more than one VDN assigned to the same vector. For example, if 5555 displays in **VDN Assigned** and \* displays in **More?**, this means that the master vector selected is already assigned to VDN 5555 as well as to other VDNs.

### Name

The first row displays the vector name for the master vector if assigned. The following lines define the vector names for the duplications. The use of vector names is optional.

### Vector

The first row displays the vector number for the master vector. The following lines define the vector numbers for the duplications. Any unassigned vector number is valid.

## Enable File Transfer

Enables SFTP on TN799BP (C-LAN) and VAL circuit packs.

Example command: `enable filexfer`

### Login

The login ID. Accepts from three to six alphanumeric characters.

### Password

Seven to 11 characters used as a password. The password must contain at least one number.

### Secure

Enables or disables SFTP instead of FTP or TFTP. If the circuit pack does not support a secure session, no session is enabled.

## Enable Session

Enables Secure SHell (SSH) instead of Telnet.

Example command: `enable session`

### Login

The login ID. Accepts from three to six alphanumeric characters.

### Password

Seven to 11 characters used as a password. The password must contain at least one number.

### Secure

Enables or disables SSH instead of Telnet.

### Time to Login

Available only if the board is a TN2302.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 255    | The number of minutes allowed for login before the session times out. |

## Extended Pick-Up Group

Organizes pickup groups into extended pickup groups. The extended group is a collection of pickup groups that can answer calls from other pickup groups in the same extended group. This allows users to answer calls outside their immediate group. The maximum number of groups that can be added to an extended pickup group is 25.

Example command: `change extended-pickup-group n`, where *n* is the group number.

### Extended Group Number

The number associated with a collection of pickup groups.

### Pickup Group Number

| Valid Entry        | Usage   |
|--------------------|---|
| 1 to 5000<br>blank | The number for call pickup groups that can answer calls in the extended pickup group. |

### Pickup Number

The pickup number assigned to the pickup group. Users dial the pickup number after the feature access code (FAC) to pick up calls in their extended pickup group.

## Extensions administered to have an MCT-Control button

Lists the extensions that can take control of a Malicious Call Trace (MCT) request. To give a user the ability to take control of such requests, you need to add their extension to this list and assign them a **mct-control** feature button.

Example command: `display mct-group-extensions`

### 1 to 100

The extension of a telephone or attendant console that can take control of a Malicious Call Trace (MCT). A **mct-control** button must be assigned to the extension station or attendant console.

## Extensions to Call Which Activate Features by Name

Assigns a dialed extension to a feature within Communication Manager. This extension is called a feature name extension (FNE). The FNE mapping must be administered and all extensions must fit the dial plan. These extensions are paired with feature access codes (FACs). When a user calls the extension, the feature access code activates the feature.

The Transfer to Voice Mail FNE is used when a user is active on a call and wants to transfer the other party to voice mail, or to the principal's voice mail, if this is a covered call. This FNE can also be used when a user goes off-hook for the first time and dials the Transfer to Voice Mail FNE to be connected to the voice mail administered in his coverage path. This is identical to dialing a Transfer to Voice Mail feature access code (FAC).

Example command: `change off-pbx-telephone feature-name-extensions`

### Extension

Any valid and assigned extension number for the Communication Manager feature that users use to access their Extension to Cellular telephones. A user dials the extension from their Extension to Cellular telephone to activate an FAC administered for that feature.

## Feature Access Code (FAC)

Assigns feature access codes (FACs) that, when dialed, activate or cancel system features.

Example command: `change feature-access-codes`

### Feature Access Code: page 1

#### ***Abbreviated Dialing List1 Access Code***

A feature access code (FAC) used to access AD list 1.

This value must conform to the FACs or dial access codes defined by the dial plan.

#### ***Abbreviated Dialing List2 Access Code***

A feature access code (FAC) used to access AD list 2.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Abbreviated Dialing List3 Access Code**

A feature access code (FAC) used to access AD list 3.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Abbreviated Dial - Prgm Group List Access Code**

FAC used to enter a group list from a telephone. The user's extension must be administered with permission to program the group list.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Program Ext](#) on page 425

**Announcement Access Code**

FAC used to record announcements.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Answer Back Access Code**

FAC used to retrieve parked calls. If no one answers the call before a system-wide expiration interval expires, the system redirects the call.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Auto Route Selection (ARS) Access Code 2**

Additional FAC used to access ARS.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Attendant Access Code**

FAC used to call the attendant. While only one attendant can be administered for the dial plan, more than one attendant FAC can be administered in a single distributed network. Attendant access numbers can start with any number from 0 to 9 and contain one or two digits. Available only if an attendant call type is not administered for the dial plan.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Call Type](#) on page 530

**Auto Alternate Routing (AAR) Access Code**

FAC used to access AAR. AAR routes calls to a different route than the first-choice route when facilities are unavailable.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Automatic Callback Activation/Deactivation***

FAC used to activate or cancel Automatic Callback. Automatic Callback enables internal callers, upon reaching a busy extension, to have the system automatically connect and ring both originating and receiving parties when the receiving party becomes available.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Auto Route Selection (ARS) Access Code 1***

FAC used to access ARS. ARS allows the system to automatically choose the least-expensive way to send a toll call. You can have one ARS access code for local and one for long distance, and route accordingly.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Call Forwarding Activation Busy/DA***

FAC used to forward calls to an administered number if the user is busy or does not answer.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Call Forwarding Enhanced Activation/Deactivation***

FAC numbers used to activate and deactivate Enhanced Call Forwarding. Enhanced Call Forwarding forwards incoming calls to different destinations depending on whether they are from internal or external sources. The FACs for activation and deactivation must be administered together.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Call Forwarding Enhanced Status***

FAC used to display the status of Enhanced Call Forwarding.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Call Park Access Code***

FAC used to park an active call that can then be retrieved from a different station using the answer back access code. The call park access code cannot have the same first digit as another feature access code that is longer in length.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Call Pickup Access Code***

FAC used to answer a call directed to a pickup group.

This value must conform to the FACs or dial access codes defined by the dial plan.

***CAS Remote Hold/Answer Hold-Unhold Access Code***

FAC used by a Centralized Attendant Service (CAS) attendant to place calls on hold and answer calls held at a remote server running Communication Manager. This FAC can also be used by an analog station. Flashing the switch-hook for the proper interval (between 200 and 1000 ms) while talking on an existing call causes the existing call to be placed on soft hold, allowing the analog user to dial the Answer Hold-Unhold FAC to Hard hold the call.

This value must conform to the FACs or dial access codes defined by the dial plan.

**CDR Account Code**

FAC used prior to entering an account code for Call Detail Recording (CDR) purposes. CDR is a feature that uses software and hardware to record call data.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Change COR Access Code**

FAC that allows users to change their class of restriction (COR) from a telephone. Available only if **Change COR by FAC** is enabled for the system.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Change COR by FAC](#) on page 944

**Change Coverage Access Code**

FAC used to change a coverage path from a telephone or remote station. The coverage path is the order in which calls are redirected to alternate answering positions.

An extension must have station **Security Codes** administered to use this FAC.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Security Code](#) on page 59

**Contact Closure Close Code**

FAC used to close a contact closure relay. Contact closures control electrical devices remotely. Users use an FAC to activate electrical devices such as electrical door locks. If **Contact Closure Open Code** is administered, then **Contact Closure Close Code** must also be administered.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Contact Closure Open Code](#) on page 561

**Contact Closure Open Code**

FAC used to open a contact closure relay. Contact closures control electrical devices remotely. Users use an FAC to activate electrical devices such as electrical door locks. If **Contact Closure Close Code** is administered, then **Contact Closure Open Code** must also be administered.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Contact Closure Close Code](#) on page 561

**Feature Access Code: page 2**

**Contact Closure Pulse Code**

FAC used to pulse a contact closure relay.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Data Origination Access Code**

FAC used to originate a data call from a voice station.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Data Privacy Access Code**

FAC used to isolate a data call from call waiting or other interruptions.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Directed Call Pickup Access Code**

FAC used to establish directed call pickup.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Directed Group Call Pickup Access Code**

FAC used to pickup a call from any pickup group if the user belongs to a pickup group.

This value must conform to the FACs or dial access codes defined by the dial plan.

**EC500 Self Administration Access Code**

FAC that allows users to self-administer their cell phone number for the Extension to Cellular feature. Users can add or change their cell phone number through this feature access code. An administrator can still enter or change cell phone numbers. The user calls the Self Administration Access Code access code and enters their cell phone number.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Emergency Access To Attendant Access Code**

FAC used to gain access to the attendant in an emergency. Such calls alert as emergency calls.

Available only if **Emergency Access to Attendant** is enabled for the system.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Emergency Access to Attendant](#) on page 945

**Enhanced EC500 Activation**

FAC used to allow users to activate Extension to Cellular remotely.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Enhanced EC500 Deactivation**

FAC used to deactivate Extension to Cellular remotely.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Enterprise Mobility User Activation**

FAC used to activate the Enterprise Mobility User feature for a particular user, associating the features and permissions of their primary telephone to a telephone of the same type anywhere within the customer's enterprise.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Enterprise Mobility User Deactivation**

FAC used to deactivate the Enterprise Mobility User feature.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Extended Call Fwd Activate All**

FAC used to activate call forwarding from a telephone or remote location.

An extension must have station **Security Codes** administered to use this FAC.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Security Code](#) on page 59

**Extended Call Fwd Activate Busy D/A**

FAC used to activate call forwarding from a telephone or remote location.

An extension must have station **Security Codes** administered to use this FAC.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Security Code](#) on page 59

**Extended Call Fwd Deactivation**

FAC used to deactivate call forwarding from a telephone or remote location.

An extension must have station **Security Codes** administered to use this FAC.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Security Code](#) on page 59

**Extended Group Call Pickup Access Code**

FAC used to answer a call directed to another pickup group. Users must enter a valid pickup number following this field to complete the operation.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Facility Test Calls Access Code**

FAC used to place a facility test call.

This value must conform to the FACs or dial access codes defined by the dial plan.



**Security alert:**

To ensure the security of your system, leave this field blank except when actually testing trunks.

***Flash Access Code***

FAC used to generate trunk flash. This code ensures that the flash signal is interpreted by the local telephone company central office switch, rather than by Avaya Communication Manager.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Group Control Restrict Activation/Deactivation***

FAC used to change the restriction level for all users with a given class of restriction. Requires console permissions.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Hunt Group Busy Activation/Deactivation***

FAC used by hunt group members to place themselves in a busy state and to become available again.

This value must conform to the FACs or dial access codes defined by the dial plan.

***ISDN Access Code***

FAC used to place an ISDN call without using ARS, AAR, or UDP.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Last Number Dialed Access Code***

FAC used to redial the last number dialed from this station.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Leave Word Calling Message Retrieval Lock***

FAC used to lock the display module on telephones. The lock function activates at a telephone by dialing this system-wide lock access code. This prevents unauthorized users from displaying, canceling, or deleting messages associated with the telephone. Available only if **Lock Messages** is administered for the station.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Lock Messages](#) on page 60

***Leave Word Calling Message Retrieval Unlock***

FAC used to unlock a telephones display module. The lock function is canceled at the telephone by dialing this unlock FAC followed by the SCC.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Feature Access Code: page 3*****Leave Word Calling Cancel A Message***

FAC used to cancel a leave word calling message.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Leave Word Calling Send A Message***

FAC used to send a leave word calling message that allows internal system users to leave a short pre-programmed message for other internal users.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Limit Number of Concurrent Calls Activation/Deactivation***

FAC used to limit concurrent calls on a station even when additional call appearances normally would be available.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Malicious Call Trace Activation***

FAC used to activate a trace request on a malicious call.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Meet-me Conference Access Code Change***

FAC that allows the controlling user of a Meet-me Conference VDN to change the access code. The Meet-me Conference feature is used to set up a dial-in conference of up to six parties.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Message Sequence Trace (MST) Disable***

Provides the ability to disable the MST traces using a Feature Access Code.

***PASTE (Display PBX data on telephone) Access Code***

FAC used to view call center data on display telephones. PASTE is used in conjunction with Avaya IP Agent.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Per Call CPN Blocking Code Access Code***

FAC used to turn on Calling Party Number (CPN) blocking for a trunk group if it has been disabled. When users dial this code, the calling party number is *not* sent to the public network.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Per Call CPN Unblocking Code Access Code***

FAC used to turn off Calling Party Number (CPN) blocking for a trunk group if it has been enabled. When users dial this code, the calling party number is sent to the public network.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Personal Station Access (PSA) Associate Code***

FAC used to associate a telephone with the telephone features assigned to a users extension.

Available only if **Personal Station Access (PSA)** is enabled for the system.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Personal Station Access \(PSA\)](#) on page 948

***Personal Station Access (PSA) Dissociate Code***

FAC used to remove the association between a physical telephone and an extension number.

Available only if **Personal Station Access (PSA)** is enabled for the system.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Personal Station Access \(PSA\)](#) on page 948

***PIN Checking for Private Calls***

FAC used to enable the PIN Checking for Private Calls feature that restricts users from making private internal or external calls by forcing them to enter a Personal Identification Number (PIN) after dialing this FAC. Available only if **PIN Checking for Private Calls** is enabled for the system.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[PIN Checking for Private Calls](#) on page 632

***Posted Messages***

FAC used to access the Posted Messages feature. The Posted Messages feature provide callers with a displayed message on the telephone that states why the user is unavailable to take a call.

Available only if the Posted Messages feature is enabled for the system.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Posted Messages](#) on page 949

***Priority Calling Access Code***

FAC used to enable priority calling, a special type of call alerting between internal telephone users, including the attendant. The called party hears a distinctive ringing when the calling party uses Priority Calling.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Program Access Code***

FAC used to program abbreviated dial buttons on an individual telephone.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Refresh Terminal Parameters Access Code**

Feature Access Code (FAC) is used to request a refresh of the terminal parameters on a telephone that supports downloadable parameters. This FAC is used after a DCP telephone is installed or replaced to ensure that all the terminal parameters, including button labels, are sent to the telephone.

**Remote Send All Calls Activation/Deactivation**

FAC used to activate or deactivate the Send All Calls feature. Requires console permissions.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Self Station Display Activation**

FAC used on a digital station to display its primary extension number when the FAC is entered.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Send All Calls Activation/Deactivation**

FAC used to activate or deactivate sending all calls to coverage with minimal or no alerting at the station.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Station Firmware Download Access Code**

FAC used for 2420/2410 DCP station firmware downloads.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Feature Access Code: page 4****Station Lock Activation/Deactivation**

FAC used to activate or deactivate Station Lock. The Station Lock feature locks a telephone to prevent others from placing outgoing calls from the telephone.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Station Security Code Change Access Code**

FAC used to change a Station Security Code (SSC). The SSC feature is used to deny other users access to the functions that are associated with the station. Each station user can change their own SSC if they know the current settings for the station. The SSC must be administered before the user can change it using this FAC.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Station User Admin of FBI Assign**

FAC used to activate or deactivate Facility Busy Indicators that provide visual indicators of the busy or idle status of any particular trunk group, hunt group member, or station user.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Station User Button Ring Control Access Code**

FAC used to control the ring behavior for each line appearance and bridged appearance from the station. Allows users to have their telephones ring either silently or audibly.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Terminal Dial-Up Test Access Code***

FAC used to perform tests on digital telephones to make sure that the telephone and the buttons are communicating properly with the server running Avaya Communication Manager. The Terminal Dial-Up test ensures that the terminal and each of its buttons can communicate with the server. This test is initiated by a user entering this feature access code. This test is mostly for use by terminal service personnel, but may be used by any station user.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Terminal Translation Initialization Merge Code***

FAC used to install, or merge, a station without losing any of its previous feature settings. The Terminal Translation Initialization Separation Code must already have been activated or the station administered without hardware, when the telephone was removed from its former location in order for the Terminal Translation Initialization Merge Code to be effective.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Terminal Translation Initialization Separation Code***

FAC used to remove, or separate, a station from a location without losing any of its feature settings.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Transfer to Voice Mail Access Code***

FAC used to allow coverage to transfer the caller to the original call recipient's voice mail where the caller can leave a message. This FAC cannot have the same first digit as another FAC that is longer in length.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Trunk Answer Any Station Access Code***

The FAC used to answer calls alerting on night bells.

This value must conform to the FACs or dial access codes defined by the dial plan.

***User Control Restrict Activation/Deactivation***

FAC used to activate and deactivate specific restrictions for an individual user or an attendant. Requires console permissions.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Voice Coverage Message Retrieval Access Code***

FAC used to retrieve voice messages for another user used as a coverage point, using a digital display module.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Voice Principal Message Retrieval Access Code***

FAC used by a user to retrieve their own voice messages for another user using a digital display module.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Whisper Page Activation Access Code***

FAC used to place a page to another user's telephone when active on a call. Only the paged user hears the page, not the other parties on the call.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Feature Access Code: page 5******Add Agent Skill Access Code***

FAC dialed by an agent to add a skill to their current skill set.

This value must conform to the FACs or dial access codes defined by the dial plan.

***After Call Work Access Code***

FAC dialed by an agent when the agent performs work-related Automatic Call Distribution (ACD) activities.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Assist Access Code***

FAC dialed by an agent to request assistance from the split supervisor. The split supervisor is someone working in a call center that uses various Communication Manager and Call Management System features to monitor split and agent performance and to provide assistance if necessary.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Auto-In Access Code***

FAC dialed when an agent is ready to process another call as soon as the current call is completed.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Aux Work Access Code***

FAC used when an agent is unavailable to receive ACD, or work-related, calls. Agents use this FAC for activities such as taking a break, going to lunch, or placing an outgoing call.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Login Access Code***

FAC dialed by an agent to gain access to the ACD functions. This is a system-wide code for all ACD agents.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Logout Access Code***

FAC dialed by the agent to exit ACD. This is a system-wide logout code for all ACD agents.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Manual-In Access Code***

FAC dialed when an agent is ready to process another call manually.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Remote Logout of Agent Access Code***

FAC typically used by a supervisor to logout an idle agent without being physically present at the agent station. The supervisor can be locally or remotely located. Available only if **Service Observing (Remote/By FAC)**, **Vectoring (Basic)**, and **Vectoring (Prompting)** are enabled on the system.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Service Observing \(Remote/By FAC\)](#) on page 952

[Vectoring \(Basic\)](#) on page 952

[Vectoring \(Prompting\)](#) on page 953

***Remove Agent Skill Access Code***

FAC dialed by an agent to remove a skill from their current skill set. Available only if **Service Observing (Remote/By FAC)** is enabled on the system.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Service Observing \(Remote/By FAC\)](#) on page 952

***Service Observing Listen Only Access Code***

FAC dialed to allow a station with Service Observing permission to listen to other agent ACD calls without being heard on the ACD call.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Service Observing Listen/Talk Access Code***

FAC dialed to allow a station with Service Observing permission to both listen and be heard on an ACD call.

This value must conform to the FACs or dial access codes defined by the dial plan.

***Service Observing No Talk Access Code***

FAC dialed to allow a station with Service Observing permission to listen only. Any attempt to toggle between listening and talking using the Service Observing button is denied. Available only if **Expert Agent Selection (EAS) Enabled** is administered for the system.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Expert Agent Selection \(EAS\) Enabled](#) on page 610

**Feature Access Code: page 6**

***Converse Data Return Code***

FAC used to pass values between a Voice Response Unit (VRU) and Communication Manager in order to play an announcement, collect digits from the caller, and so on.

**Vector Variable x**

FAC (# can be used as the first digit), used to change the value of defined variables.

**Related topics:**

[Variables for Vectors](#) on page 1046

**Feature Access Code: page 7****Automatic Wakeup Call Access Code**

FAC dialed to schedule or cancel a wakeup call.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Housekeeping Status (Client Room) Access Code**

FAC the housekeeper dials from a client room to provide room status. These codes are transmitted to the Property Management System (PMS) for processing.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Housekeeping Status (Station) Access Code**

FAC the housekeeper dials to provide room status. This access code must be dialed from designated telephones.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Verify Wakeup Announcement Access Code**

FAC dialed to verify a wakeup announcement.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Voice Do Not Disturb Access Code**

FAC dialed to enter or cancel a “do not disturb” request using voice prompting.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Feature Access Code: page 8****Basic Mode Activation**

FAC dialed to revert an Enhanced multimedia complex to a Basic multimedia complex.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Enhanced Mode Activation**

FAC used to convert a Basic multimedia complex to an Enhanced multimedia complex.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Multimedia Call Access Code**

FAC that indicates to Avaya Communication Manager that an Enhanced mode multimedia call is being made. This FAC originates a multimedia call according to system-wide default settings.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Default Multimedia Outgoing Trunk Parameter Selection](#) on page 579

**Multimedia Data Conference Activation**

FAC that when entered from any voice station that is participating in a multimedia call, alerts Avaya Communication Manager to enable data collaboration with the other parties on the call. If this FAC is entered a second time, multimedia data conference activation is denied since it is already active. This FAC only applies to voice stations on servers equipped with ESM adjuncts.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Multimedia Data Conference Deactivation**

FAC that when entered from the telephone that enabled data collaboration on a multimedia mode call, deactivates the data session and reverts to a voice and video call. If a user enters this FAC while participating in a data-collaboration multimedia call that the user did not initiate, the system denies the deactivation.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Multimedia Multi-Address Access Code**

FAC that allows origination of a multimedia call from a voice station. It is used when the destination being dialed requires a different address for each of the 2B-channels.

For example, ISDN-BRI provided by a local telephone company central office is provisioned with separate listed directory numbers for each B-channel. To make a 2B multimedia call to such a device, two sets of addresses must be entered.

Originating a multimedia call with the multimedia multi-address access code originates a call according to system-wide default settings.

This value must conform to the FACs or dial access codes defined by the dial plan.

**Related topics:**

[Default Multimedia Outgoing Trunk Parameter Selection](#) on page 579

**Multimedia Parameter Access Code**

FAC that prompts Avaya Communication Manager to initiate a multimedia mode call with a specific bearer capability. This FAC would be followed by a 1 or 2 to indicate the following parameter selections respectively: 2x64 (unrestricted initial system default), 2x56 (restricted).

This value must conform to the FACs or dial access codes defined by the dial plan.

**Feature Access Code: page 9**

**Precedence Calling Access Code**

FAC used to access the Multiple Level Precedence and Preemption (MLPP) feature that allows users to request priority processing of calls during critical situations.

This value must conform to the FACs or dial access codes defined by the dial plan.

**WNDP PRECEDENCE ACCESS CODES**

FAC used to determine the precedence level for a call when the Worldwide Numbering Dial Plan (WNDP) feature is active. The WNDP feature is compatible with the standard numbering

system that the Defense Communications Agency (DCA) established. Different feature access codes are assigned for each PRECEDENCE level.

This value must conform to the FACs or dial access codes defined by the dial plan.

#### Flash Access Code

FAC that corresponds to the Flash preemption level.

This value must conform to the FACs or dial access codes defined by the dial plan.

#### Flash Override Access Code

FAC that corresponds to the Flash Override preemption level.

This value must conform to the FACs or dial access codes defined by the dial plan.

#### Immediate Access Code

FAC that corresponds to the Immediate preemption level.

This value must conform to the FACs or dial access codes defined by the dial plan.

#### Priority Access Code

FAC that corresponds to the Priority preemption level.

This value must conform to the FACs or dial access codes defined by the dial plan.

#### Routine Access Code

FAC that corresponds to the Routine preemption level.

This value must conform to the FACs or dial access codes defined by the dial plan.

## Feature-related system parameters

This screen implements system parameters associated with various system features.



#### Note:

Call Coverage and Call Forwarding parameters are located on the System Parameters Call Coverage / Call Forwarding screen.

Example command: `change system-parameters features`

### Feature-related system parameters: page 1

#### **AAR/ARS Dial Tone Required**

Enables or disables a second dial tone that tells the user that additional dialing can occur. The second dial tone is provided on a incoming tie or DID trunk call routed through AAR/ARS. Available only when **Automatic Circuit Assurance (ACA) Enabled** is enabled for the system.

#### Related topics:

[Automatic Circuit Assurance \(ACA\) Enabled](#) on page 575

**Abbreviated Dial Programming by Assigned Lists**

| Valid Entry | Usage   |
|-------------|---|
| y           | Allows programming by the station-assigned list.  |
| n           | Indicates that a Program Access code is being used to indicate which personal list is to be programmed. |

**ACA Long Holding Time Originating Extension**

The extension number that the ACA feature uses when sending a long holding time referral call. This extension number must be different from the extension number used for **ACA Short Holding Time Originating Extension**. Available only for local or primary ACA Referral Calls.

**Related topics:**

[ACA Referral Calls](#) on page 574

[ACA Short Holding Time Originating Extension](#) on page 575

**ACA Referral Calls**

Indicates where Automatic Circuit Assurance (ACA) referral calls generate. The Automatic Circuit Assurance (ACA) feature is used to identify possible trunk malfunctions. If a possible trunk malfunction is identified, Communication Manager sends the attendant a referral call that consists of a display message or a voice-synthesized message indicating the problem and where the problem is located. Available only when **Automatic Circuit Assurance (ACA) Enabled** is enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| local       | Generate on and for the local switch.  |
| primary     | Generate on the local switch for remote servers and switches as well as the local switch.  |
| remote      | Generate at another server in a DCS network. In this case, the remote node number must also be entered. The remote node number is the same node number administered for the dial plan. Also, <b>ACA</b> button status transmits to other servers and switches when in a DCS network. |

**Related topics:**

[Automatic Circuit Assurance \(ACA\) Enabled](#) on page 575

**ACA Referral Destination**

The specified extension or attendant must be equipped with a display module. Available only for local or primary ACA Referral Calls.

| Valid Entry             | Usage   |
|-------------------------|---|
| <i>extension number</i> | The extension on a local server running Communication Manager receives the ACA referral call. |
| attd                    | The attendant receives the ACA referral call.   |

**Related topics:**

[ACA Referral Calls](#) on page 574

**ACA Remote PBX Identification**

Available only for remote ACA Referral Calls.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 63     | Identifies the switch in a DCS network that makes the referral call. The switch identified here cannot be the remote server or switch identified as <b>local</b> on the system Dial Plan. |

**Related topics:**

[ACA Referral Calls](#) on page 574

**ACA Short Holding Time Originating Extension**

The extension number that the ACA feature uses when sending a short holding time referral call. This extension number must be different from the extension number used for **ACA Long Holding Time Originating Extension**.

Available only for local or primary ACA Referral Calls.

**Related topics:**

[ACA Long Holding Time Originating Extension](#) on page 574

[ACA Referral Calls](#) on page 574

**Auto Abbreviated/Delayed Transition Interval (rings)**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 16     | The number of rings before an automatic abbreviated or delayed transition is triggered for a call. |

**Automatic Callback — No Answer Timeout Interval (rings)**

| Valid Entry | Usage   |
|-------------|---|
| 2 to 9      | The number of times the callback rings at the calling station before the callback is canceled. Automatic Callback allows internal users who place a call to a busy or an unanswered internal telephone to be called back when the called telephone becomes available. |

**Automatic Circuit Assurance (ACA) Enabled**

Enables or disables the ACA feature to measure the holding time of each trunk call in order to identify possible trunk malfunctions. Long duration thresholds are designed to detect trunks that have been connected beyond the limit. Short duration thresholds detect trunks that might be dropping. Requires that an **aca-halt** button is administered on the user station.

**Call Park Timeout Interval (minutes)**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 90     | The number of minutes a call remains parked before it cancels. The Call Park feature allows users to retrieve a call on hold from any other telephone within the system. |

**DID/Tie/ISDN/SIP Intercept Treatment**

| Valid Entry      | Usage   |
|------------------|---|
| <i>Extension</i> | <p>Toll charges do not apply to DID and private network calls routed to this recorded announcement extension.</p> <p> <b>Note:</b><br/>When entering a Multi-Location Dial Plan shortened extension in a field designed for announcement extensions, certain administration end validations that are normally performed on announcement extensions are not done, and resultant warnings or submittal denials do not occur. The shortened extensions also do not appear in any display or list that shows announcement extensions. Extra care should be taken to administer the correct type of announcement for the application if assigning shortened extensions.</p> |
| attd             | <p>Routes intercept calls to the attendant so that the attendant knows when a problem exists.</p> <p> <b>Security alert:</b><br/>Avaya recommends routing intercept calls to the attendant.</p>  |

**Display Calling Number for Room to Room Caller ID Calls**

Enables or disables displaying the calling number for room to room hospitality calls.

**Internal Auto-Answer of Attd-Extended/Transferred Calls**

The Internal Automatic Answer (IAA) feature allows users to answer internal calls on digital telephones (except BRI) using a speakerphone or a headset .

| Valid Entry   | Usage   |
|---------------|---|
| attd-extended | Enables IAA for only attendant-extended calls.                    |
| both          | Enables IAA for station-transferred and attendant-extended calls. |
| none          | Disables IAA for all calls.                                       |
| transferred   | Enables IAA for only station-transferred calls.                   |

**Music (or Silence) On Transferred Trunk Calls**

| Valid Entry | Usage   |
|-------------|---|
| all         | All transferred trunk calls receive music until the call is answered if the Music-on-Hold feature is available. |

| Valid Entry | Usage   |
|-------------|---|
| no          | Trunk callers hear music, or silence if Music-on-Hold is not administered, while waiting to be transferred, and then ringback as soon as the transfer is completed till the call is answered. |
| call-wait   | Trunk calls are transferred to stations that require the call to wait and hear music, if administered. All other transferred trunk calls receive ringback tone.                               |

### **Music/Tone on Hold**

Indicates what a caller hears while on hold. Available only if **Tenant Partitioning** is disabled for the system.

| Valid Entry | Usage                                   |
|-------------|---|
| music       | The caller hears music while on hold.   |
| tone        | The caller hears a tone while on hold.  |
| none        | The caller hears silence while on hold. |

#### **Related topics:**

[Tenant Partitioning](#) on page 949

### **Off-Premises Tone Detect Timeout Interval (seconds)**

| Valid Entry | Usage   |
|-------------|---|
| 5 to 25     | The number of seconds a call progress tone receiver (CPTR) tries to detect dial tone from a trunk during dialing. Once the time-out interval occurs, the call either outpulses on the trunk or gets intercept treatment depending on the <b>Outpulse Without Tone</b> settings administered for the system. |

#### **Related topics:**

[Outpulse Without Tone](#) on page 607

### **Port**

Available only when the music on hold type is port.

| Valid Entry                               | Usage   |
|---|---|
| 1 to 64                                   | First and second characters are the cabinet number. |
| A to E                                    | Third character is the carrier                      |
| 0 to 20                                   | Fourth and fifth character are the slot number.     |
| 01 to 04 (Analog TIE trunks).<br>01 to 31 | Sixth and seventh characters are the circuit number |
| 1 to 250                                  | Gateway   |

| Valid Entry | Usage   |
|-------------|---------|
| V1 to V9    | Module  |
| 01 to 31    | Circuit |

**Related topics:**

[Music/Tone on Hold](#) on page 577

[Type](#) on page 578

**Protocol for Caller ID Analog Terminals**

Determines the protocol or tones sent to a Caller ID telephone. The provider should have the correct protocol for each country.

| Valid Entry | Usage   |
|-------------|---|
| Bellcore    | Telcordia Technologies protocol with 212 modem protocol tones. Typically used in the U.S. |
| V23–Bell    | Telcordia Technologies protocol with V.23 modem tones. Typically used in Bahrain.         |

**Self Station Display Enabled**

Enables or disables the displaying of the primary extension associated with a digital display telephone when the **inspect** button is pressed or when a feature access code (FAC) is entered.

- When using an FAC, the display continues until the user picks up the telephone or receives an incoming call.
- When using the **inspect** button, the display continues until the user presses the **normal** or **exit** button, or until the user picks up the telephone or receives an incoming call.

**Trunk-to-Trunk Transfer**

Regulations in some countries control the settings for this field. See Avaya technical support representative for assistance.

| Valid Entry | Usage  |
|-------------|--|
| all         | Enables all trunk-to-trunk transfers. This allows telephone users to set up trunk-to-trunk transfer, go on-hook without disconnecting the call, and forward the call to a remote location. This value is required for SIP Enablement Services (SES) support. |
| restricted  | Restricts all public trunks (CO, WATS, FX, CPE, DID, and DIOD) from being transferred.   |
| none        | Restricts all trunks (except CAS and DCS) from being transferred.  |

**Type**

Indicates whether the source for Music on Hold is an announcement extension, an audio group, or a port on a VAL board.

Available only if music is administered as the treatment for calls placed on hold.

| Valid Entry | Usage  |
|-------------|--|
| ext         | Extension. Requires entry of the corresponding extension number of the announcement or audio source.   |
| group       | Analog group. Requires entry of the corresponding Music-on-Hold analog group number.   |
| port        | Analog/aux-trunk. Requires entry of the corresponding location of the Music-on-Hold analog or aux-trunk source.<br><br> <b>Note:</b><br>A source identifier (extension number, audio group number, or port number) must be administered with the source type. |

### Feature-related system parameters: page 2

#### **LEAVE WORD CALLING PARAMETERS**

Default Multimedia Outgoing Trunk Parameter Selection

Does not appear on S87XX Series IP-PNC.

| Valid Entry  | Usage  |
|--------------|--|
| 2x56<br>2x64 | Sets the default parameter for bandwidth and bearer for all video calls. |

#### Related topics:

[Multimedia Call Access Code](#) on page 571

Enhanced Abbreviated Dial Length (3 or 4)

Enhanced abbreviated dial lists are for users who need to store a vast quantity of speed-dialed numbers. The administrator might not be able to use all entry slots because of system capacity constraints.

| Valid Entry | Usage  |
|-------------|--|
| 3           | Makes 1000 enhanced list entries available to the administrator. |
| 4           | Makes 10,000 entries available.                                  |

Maximum Number of External Calls Logged Per Station

When an external call is not answered, the server running Communication Manager keeps a record of up to 15 calls, provided information on the caller identification is available, and the telephone message lamp lights. The telephone set displays the names and numbers of unsuccessful callers.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 15     | The maximum number of calls that can be logged for each user. The assigned number cannot be larger than the entry in <b>Maximum Number of Messages Per Station</b> . |

**Related topics:**

[Maximum Number of Messages Per Station](#) on page 580

Maximum Number of Messages Per Station

| Valid Entry | Usage   |
|-------------|---|
| 0 to 125    | The maximum number of Leave Word Calling (LWC) messages that can be stored by the system for a telephone at a given time. LWC allows internal system users to leave a short pre-programmed message for other internal users. When the message is stored, the Automatic Message Waiting lamp lights on the called telephone. |

Message Waiting Indication for External Calls

Enables or disables a station's ability to receive a message waiting indication when external calls are logged.

Prohibit Bridging Onto Calls with Data Privacy

| Valid Entry | Usage  |
|-------------|--|
| y           | Prohibits calls from getting bridged by any party, including Service Observing, Intrusion, Verify, and Bridging. |
| n           | Allows calls to be bridged.  |

Stations With System-wide Retrieval Permission (enter extension)

The server running Communication Manager refers to extensions with system-wide retrieval permission as “super-retrievers”.

| Valid Entry               | Usage  |
|---------------------------|--|
| <i>Assigned extension</i> | Up to ten telephone extension numbers that have permission to retrieve LWC Messages or External Call Log records for all other telephones. A VDN extension is not allowed. |
| attd                      | All attendants have retrieval permission.  |

 **Note:**

An extension must be removed from this list before the station can be removed from the system.

**Feature-related system parameters: page 3**

***TTI/PSA PARAMETERS***

CPN, ANI for Dissociated Sets

Specifies the ISDN calling party number (CPN), R2-MFC ANI, and CAMA CESID applied to calls made from PSA dissociated sets if no system-wide calling party information has been administered for those protocols. A dissociated set is a DCP telephone extension registered to another telephone or softphone. Available only if a default COR has been administered for dissociated sets. Accepts up to 20 digits.

**Related topics:**

[Default COR for Dissociated Sets](#) on page 581

**Customer Telephone Activation (CTA) Enabled**

Enables or disables the Customer Telephone Activation (CTA) feature that associates a physical telephone with a station translations switch. CTA applies only to DCP and analog phones.

**Default COR for Dissociated Sets**

Available only when Terminal Translation Initialization is enabled for the system.

| Valid Entry       | Usage  |
|-------------------|--|
| 0 to 995<br>blank | The Class of Restriction (COR) that the system uses for calls made from dissociated telephones. A dissociated set is a DCP telephone extension registered to another telephone or softphone. |

**Related topics:**

[Terminal Translation Initialization \(TTI\) Enabled](#) on page 581

**Enhanced PSA Location/Display Information Enabled**

Enables or disables the display of Personal Station Access (PSA) information used to disassociate and associate telephones.

When enabled, displays:

- PSA login and associated station information when a station is PSA associated
- PSA logout and the port when a station is PSA dissociated

Available only when Terminal Translation Initialization (TTI) is enabled for the system.

**Related topics:**

[Terminal Translation Initialization \(TTI\) Enabled](#) on page 581

**Hot Desking Enhancement Station Lock**

Administers the Hot Desking Enhancement (HDE) feature. "Hot desking" is a feature that can lock and unlock telephones or move a fully customized station profile to another compatible telephone.

| Valid Entry | Usage   |
|-------------|---|
| y           | Enables the Hot Desking Enhancement feature.    |
| n           | Disables the Hot Desking Enhancement feature.   |
| system      | Performs administration on a system-wide basis. |

**Terminal Translation Initialization (TTI) Enabled**

Technicians use the Terminal Translation Initialization (TTI) feature to disassociate and associate telephones. Available only if TTI is enabled for the system.

 **Caution:**

Contact Avaya technical support before making changes to TTI settings.

| Valid Entry | Usage  |
|-------------|--|
| y           | Starts ACTR, TTI, and PSA transactions for extension and telephone moves between ports.          |
| n           | Removes existing TTI port translations and prevents the generation of new TTI port translations. |

**Related topics:**

[Terminal Trans. Init. \(TTI\)](#) on page 950

TTI Security Code

Number that a TTI user uses to access TTI from a telephone or data terminal. Accepts up to seven digits. Available only if Terminal Translation Initialization (TTI) is enabled.

**Related topics:**

[Terminal Translation Initialization \(TTI\) Enabled](#) on page 581

TTI State

The type of port translation used for unadministered digital ports. Available only when Terminal Translation Initialization (TTI) is enabled.

| Valid Entry | Usage  |
|-------------|--|
| data        | A stand-alone data module is the TTI port translation for the system. The activation and deactivation sequence is entered at the data terminal.  |
| resume      | TTI is available after TTI has been manually suspended. The state of TTI returns to the state that it was in before TTI was manually suspended.  |
| suspend     | TTI voice or TTI data translations are temporarily unavailable. The system does not remove existing TTI translations.                            |
| voice       | A voice or voice/data terminal is the TTI port translation for the system. The activation and deactivation sequence is entered from a telephone. |

**Related topics:**

[Terminal Translation Initialization \(TTI\) Enabled](#) on page 581

Unnamed Registrations and PSA for IP Telephones

Allows or denies IP telephones access to the Personal Station Access (PSA) feature. If allowed, IP telephones can register into the following states:

- PSA dissociated
- TTI unmerged

- TTI state
- Unnamed Registered — for H.323 standards

### **EMU PARAMETERS**

#### EMU Inactivity Interval for Deactivation (hours)

A system-wide administrable interval for EMU de-registration at the visited switch. This timer is applicable to inter and intra-Communication Manager EMU registrations.

 **Note:**

If SES is enabled for the system, this field is used as the inactivity timer for SIP Visiting Users.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 24     | The interval in hours, after which a visiting user is dropped due to inactivity. Default is 1. An entry of 1 means that after 1 hour of inactivity, the telephone is dropped from the visited home server. |
| blank       | The timer is not used and the visited station remains active until de-registration by another means occurs.  |

### **CALL PROCESSING OVERLOAD MITIGATION**

#### Restrict Calls

Indicates the type of calls to block first during overload traffic conditions on the system.

| Valid Entry         | Usage  |
|---------------------|--|
| stations-first      | Deny new traffic generated by internal stations, allowing inbound calls only. This works best in call center environments. |
| all-trunk-first     | Deny all out-bound calls to trunks, tie-lines and stations, and all station-originated calls.                              |
| public-trunks-first | Deny all in-bound calls from trunks and tie-lines.   |

#### **Feature-related system parameters: page 4**

##### **Call Pickup Alerting**

Enables or disables system-wide Call Pickup Alerting. Call Pickup Alerting provides pickup group members with a visual indication on the Call Pickup status lamp of calls eligible to be answered using Call Pickup.

##### **Call Pickup on Intercom Calls**

Allows or denies the system-wide use of Call Pickup or Directed Call Pickup features on intercom calls.

##### **Controlled Outward Restriction Intercept Treatment**

The type of intercept treatment the caller receives when the call is outward restricted.

| Valid Entry  | Usage   |
|--------------|---|
| announcement | <p>Provides a recorded announcement to calls that cannot be completed as dialed. The calling party receives indication that the call is receiving Intercept Treatment. Requires an extension number for the announcement in the associated field.</p> <p> <b>Note:</b><br/>When entering a Multi-Location Dial Plan shortened extension in a field designed for announcement extensions, certain administration end validations that are normally performed on announcement extensions are not done, and resultant warnings or submittal denials do not occur. The shortened extensions also do not appear in any display or list that shows announcement extensions. Extra care should be taken to administer the correct type of announcement for the application if assigning shortened extensions.</p> |
| attendant    | Allows attendants to provide information and assistance to outgoing calls that cannot be completed as dialed or that are transferred to incomplete or restricted stations.  |
| extension    | Routes to an extension. Requires an extension number for the extension in an associated field. Cannot be a VDN extension.   |
| tone         | Provides a siren-type tone to internal calls that cannot be completed as dialed.  |

**Controlled Station-to-Station Restriction**

The type of intercept treatment the caller receives when the call is placed to a restricted telephone.

| Valid Entry  | Usage   |
|--------------|---|
| announcement | Provides an announcement. Requires entry of the announcement extension.   |
| attendant    | Intercepted calls are redirected to the attendant.  |
| extension    | Routes the call to an alternate extension. Requires entry of the station or individual attendant. This cannot be a VDN extension. |
| tone         | Intercepted calls receive intercept (siren) tone.   |

**Controlled Termination Restriction (Do Not Disturb)**

The type of intercept treatment the caller receives when the call is placed to a termination restricted telephone.

| Valid Entry  | Usage  |
|--------------|--|
| announcement | Redirects intercepted calls to an announcement. Requires an associated extension number. |
| attendant    | Redirects intercepted calls to the attendant.  |
| coverage     | Redirects intercepted calls to coverage.   |

| Valid Entry | Usage  |
|-------------|--|
| extension   | Redirects intercepted calls to an extension. Requires an associated extension number. Cannot be a VDN extension. |
| tone        | Provides a siren-type tone to calls that cannot be completed as dialed.  |

### ***Deluxe Paging and Call Park Timeout to Originator***

Enables or disables the Call Park feature that allows a user to retrieve a call that is on hold from any other telephone within the system. For example, a user can answer a call at one extension, put the call on hold, and then retrieve the call at another extension. Or the user can answer a call at any telephone after an attendant or another user pages the user. Paged calls that are to be parked require separate activation of the Call Park feature.

| Valid Entry | Usage   |
|-------------|---|
| y           | The system redirects a parked call to the user who parked the call. |
| n           | The system redirects a parked call to the attendant.                |

### ***Emergency Access Redirection Extension***

The assigned extension number or Vector Directory Number (VDN) where emergency queue overflow redirects.

### ***Extended Group Call Pickup***

Enables call pickup groups to answer calls directed to another call pickup group.

| Valid Entry | Usage   |
|-------------|---|
| flexible    | Flexible feature version supporting a one-to-n (pickup group-to-extended pickup group) mapping.   |
| simple      | Simple feature version with a one-to-one pickup group-to-extended pickup group mapping supported. |
| none        | Extended group call pickup not supported.   |

### ***Number of Emergency Calls Allowed in Attendant Queue***

| Valid Entry | Usage  |
|-------------|--|
| 0 to 75     | The number of emergency calls allowed in the attendant queue before additional calls are routed to the backup extension. |

### ***Reserved Slots for Attendant Priority Queue***

| Valid Entry | Usage  |
|-------------|--|
| 2 to 342    | The number of calls that can go in to the emergency queue. |

**Time Before Off-Hook Alert**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 3000   | The time in seconds that a telephone with an Off-Hook Alert Class of Service can remain off-hook (after intercept tone has started) before an emergency call is sent to the attendant. |

**AUTHORIZATION CODE PARAMETERS**

**Attendant Time Out Flag**

Applies only to remote users or incoming calls over trunks requiring an authorization code. Available only if authorization codes are enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| y           | A call is routed to the attendant if the caller does not dial an authorization code within 10 seconds or dials an invalid authorization code. |
| n           | The caller receives intercept tone.   |

**Related topics:**

[Authorization Codes Enabled](#) on page 587

**Authorization Code Cancellation Symbol**

The symbol a caller must dial to cancel the 10-second wait period during which the user can enter an authorization code. Available only if authorization codes are enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| (#)         | The main and tandem servers or switches are both of the same type. |
| (1)         | An Avaya server or switch is part of the complex or network.       |

**Related topics:**

[Authorization Codes Enabled](#) on page 587

**Authorization Code Length**

Available only if authorization codes are enabled for the system.



**Security alert:**

Enhance system security by using the maximum length for your authorization code.

| Valid Entry    | Usage  |
|----------------|--|
| 4 to 13 digits | The required length of the authorization code. All administered authorization codes must be this length. |

**Related topics:**

[Authorization Codes Enabled](#) on page 587

**Authorization Codes Enabled**

Enables or disables authorization codes on a system-wide basis.

Available only if authorization codes are enabled.

**Security alert:**

To maintain system security, Avaya recommends using authorization codes.

**Related topics:**

[Authorization Codes](#) on page 944

**Controlled Toll Restriction Intercept Treatment**

Applies an intercept treatment to a toll call during the call processing. Available only if the Controlled Toll Restriction feature is activated.

| Valid Entry  | Usage  |
|--------------|--|
| announcement | Intercepted calls are redirected to an announcement. Requires an assigned announcement extension.                      |
| attendant    | Intercepted calls are redirected to the attendant.   |
| extension    | Intercepted calls are redirected to an extension. Requires an extension assigned to a station or individual attendant. |
| tone         | Intercepted calls receive intercept (siren) tone.  |

**Related topics:**

[Controlled Toll Restriction Replaces](#) on page 587

**Controlled Toll Restriction Replaces**

Activates the Controlled Toll Restriction feature that allows the customer to use additional types of calling restrictions on guest room telephones.

| Valid Entry     | Usage   |
|-----------------|---|
| outward         | Guests cannot place calls to the public network.  |
| station-station | Guests cannot place or receive calls between guest rooms or administrative staff voice terminals. |
| termination     | Guests cannot receive any calls.  |
| total           | Guests cannot place or receive any calls.   |
| toll            | Guests cannot place toll calls, but can place local free calls.                                   |

**Display Authorization Code**

Enables or disables displaying authorization code digits on the set during dialing. Applies only to DCP, not to BRI or hybrid sets.



**Security alert:**

To enhance system security, do *not* display authorization code digits during dialing.

**Feature-related system parameters: page 5**

**SYSTEM PRINTER PARAMETERS**

The system printer is the printer dedicated to support scheduled reports.

Endpoint

| Valid Entry | Usage  |
|-------------|--|
| SYS_PRNT    | If the system printer is connected over a TCP/IP link, and the link is defined as SYS_PRNT for IP Services |
| blank       | Not administered   |

**Related topics:**

[Service Type](#) on page 718

Lines Per Page

| Valid Entry | Usage   |
|-------------|---|
| 24 to 132   | The number of lines per page required for the report. |

**SYSTEM-WIDE PARAMETERS**

COR to Use for DPT

The Class of Restriction used for the Dial Plan Transparency (DPT) feature.

| Valid Entry  | Usage  |
|--------------|--|
| station      | The Facility Restriction Level (FRL) of the calling station determines whether that station is permitted to make a trunk call and if so, which trunks it is eligible to access. This is the default. |
| unrestricted | The first available trunk preference pointed to by ARS routing is used.  |

Emergency Extension Forwarding (min)

If an emergency call disconnects, public safety personnel always attempt to call back. If the ELIN that was sent was not equivalent to the caller's extension number, the return call rings a set other than the one that dialed 911. To overcome this limitation, you can automatically forward that return call to the set that placed the emergency call for an administered period of time.

**Emergency Extension Forwarding** only applies if the emergency location extension number is an extension on the same switch as the extension that dialed 911. Customers who have several switches in a campus should assign emergency location extensions accordingly.

Sets the Emergency Extension Forwarding timer for all incoming trunk calls if an emergency call gets cut off.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 999    | The time in minutes that an incoming trunk call forwards to the extension that made the initial 911 call. The default value for both new installs and upgrades is 10. |

 **Note:**

If a user at the emergency location extension (the extension that made the initial 911 call) manually turns off the Call Forwarding feature, the feature is off no matter how many minutes remain on the timer.

#### Enable Dial Plan Transparency in Survivable Mode

Enables or disables Dial Plan Transparency (DPT) without changing or removing other feature administration associated with DPT. DPT is enabled if a media gateway registers with a Survivable Remote Server (Local survivable processor), or a port network registers with a Survivable Core Server (Enterprise Survivable Server).

#### Enable Inter-Gateway Alternate Routing

Enables or disables the Inter-Gateway Alternate Routing (IGAR) feature that provides a means of alternately using the public network when the IP-WAN is incapable of carrying the bearer connection.

#### IGAR Over IP Trunks

Appears when the **Enable Inter-Gateway Alternate Routing** field is set to y.

| Valid Entry | Usage   |
|-------------|---|
| allow       | The IGAR feature uses H.323 or SIP trunks when selecting a trunk from a Route Pattern.                                  |
| skip        | The IGAR feature skips H.323 and SIP trunks when selecting a trunk from a Route Pattern. By default, the value is skip. |

#### Related topics:

[Enable Inter-Gateway Alternate Routing](#) on page 589

[Incoming Dialog Loopbacks](#) on page 861

#### Switch Name

A name used for identifying the switch. Accepts up to 20 alphanumeric characters.

### **MALICIOUS CALL TRACE PARAMETERS**

#### Apply MCT Warning Tone

Enables or disables an audible tone to the controlling station when a Malicious Call Trace (MCT) recorder is actively recording a malicious call.

#### Delay Sending Release (seconds)

Available only if Malicious Call Trace is enabled for the system.

## Managing inventory

| Valid Entry | Usage   |
|-------------|---|
| 0 to 30     | The time in seconds the system waits before sending an ISDN release message in response to receiving an ISDN disconnect message. Available in increments of 10. |

### Related topics:

[Malicious Call Trace](#) on page 948

## MCT Voice Recorder Trunk Group

| Valid Entry | Usage  |
|-------------|--|
| 1 to 2000   | Assigns the trunk group number for Malicious Call Trace (MCT) voice recorders. |

## **SEND ALL CALL OPTIONS**

### Auto Inspect on Send All Calls

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows a user to be presented automatically with Calling Party information for calls that are silently alerting their station because of the Send-All-Calls feature. |
| n           | Calling Party display for calls sent directly to Coverage by the Send-All-Calls feature is not guaranteed.   |

### Send All Calls Applies to

| Valid Entry | Usage   |
|-------------|---|
| station     | Any call to a station, regardless of the number dialed, causes calls to that station's own extension to be sent immediately to Coverage, or causes calls to different extensions assigned to the station as bridged appearances to have Ring-Ping notification if redirect notification is enabled. |
| extension   | Only the calls sent to that extension are placed to coverage.   |

### Related topics:

[Redirect Notification](#) on page 72

## **UNIVERSAL CALL ID**

### Create Universal Call ID (UCID)

Enables or disables the generation of a UCID for each call when necessary.

## UCID Network Node ID

| Valid Entry       | Usage   |
|-------------------|---|
| 1 to 327<br>blank | A number unique to this server or switch in a network of switches. This number is an important part of the UCID tag and must be unique to the server or switch. |

**Feature-related system parameters: page 6*****7405ND Numeric Terminal Display***

Enables or disables allowing a 7405ND type of station. This is not an actual telephone type, but it can be used to define ports for certain types of voice messaging systems. This numeric display setting sends only numbers, and not names, to the messaging system.

**Related topics:**

[Type](#) on page 909

***7434ND***

Enables or disables allowing a 7434ND type of station. This is not an actual telephone type, but it can be used to define ports for certain types of messaging systems. Used if the voice messaging system operates in Bridged Mode.

**Related topics:**

[Type](#) on page 909

***Allow AAR/ARS Access from DID/DIOD***

Enables or disables allowing calls for DID and DIOD type trunk groups to complete calls using ARS or AAR.

***Allow ANI Restriction on AAR/ARS***

(For Russia only). Enables or disables allowing a call placed over a Russian shuttle trunk or a Russian rotary trunk using AAR or ARS to have the ANI requirement administered as restricted. In this case, when ANI is requested, if the request fails, the call immediately drops.

**Related topics:**

[ANI Req'd](#) on page 418

[ANI Req'd](#) on page 421

[Request Incoming ANI \(non-AAR/ARS\)](#) on page 795

***Attendant Tone***

Enables or disables providing call progress tones to the attendants.

***Auto Hold***

Enables or disables the Automatic Hold feature on a system-wide basis.

***Auto Start***

If enabled, the Start buttons on all attendant consoles are disabled and the Automatic Start feature is enabled.

**Bridging Tone**

Enables or disables providing a bridging tone when calls are bridged on primary extensions.

**Conference Parties without Public Network Trunks**

| Valid Entry | Usage  |
|-------------|--|
| 3 to 6      | The maximum number of parties allowed in a conference call involving no public network trunks. |

**Conference Parties with Public Network Trunks**

Available only if public network trunks are allowed on a conference call.

| Valid Entry | Usage   |
|-------------|---|
| 3 to 6      | The maximum number of parties allowed in a conference call involving a public network subscriber. |

**Related topics:**

[Public Network Trunks on Conference Call](#) on page 593

**Conference Tone**

Enables or disables providing a conference tone as long as three or more calls are in a conference call.

 **Note:**

Bridging and Conference Tones are not supported by all countries. If these tones are enabled for countries other than Italy, Belgium, United Kingdom, or Australia, the tones are equivalent to no tone (silence) unless the tone is independently administered or customized.

**Related topics:**

[Tone Generation](#) on page 975

**DID Busy Treatment**

Specifies how to handle a direct inward dialing (DID) call to a busy station.

| Valid Entry | Usage                        |
|-------------|------------------------------|
| attendant   | Call is routed to attendant. |
| tone        | Caller hears a busy tone.    |

**Intrusion Tone**

Enables or disables applying an intrusion tone (executive override) when an attendant intrudes on the call.

**Invalid Number Dialed Intercept Treatment**

The type of intercept treatment the end-user hears after dialing an invalid number.

| Valid Entry  | Usage  |
|--------------|--|
| announcement | Provides a recorded announcement when the end-user dials an invalid number. Administrators select and record the message. Requires the entry of the extension number for the announcement. |
| tone         | Provides intercept tone when the end-user dials an invalid number. This is the default.  |

### ***Line Intercept Tone Timer (seconds)***

| Valid Entry | Usage   |
|-------------|---|
| 0 to 60     | How long an analog station user can wait after hearing warning tone without going on hook, before the station is placed in the lockout state. |

### ***Long Hold Recall Timer (seconds)***

| Valid Entry | Usage  |
|-------------|--|
| 0 to 999    | The number of seconds a call can be on hold before the system re-alerts the user to remind them of the call. |

### ***Mode Code Interface***

Enables or disables the use of the Mode Code Voice Mail System Interface to connect the server running Communication Manager over a DTMF interface to other voice-mail systems.



#### **Note:**

After making changes, log off and log back on to access the **Mode Code Related System Parameters**.

### ***Night Service Disconnect Timer (seconds)***

| Valid Entry         | Usage  |
|---------------------|--|
| 10 to 1024<br>blank | The number of seconds a trunk call can be unanswered during night service before being disconnected. The trunk must not have Disconnect Supervision for this timer to apply. |

### ***Public Network Trunks on Conference Call***

| Valid Entry | Usage   |
|-------------|---|
| 0 to 5      | The number of public network trunks allowed on a conference call. |

### ***Recall from VDN***

Indicates whether or not a call that is transferred to a VDN and then routed to a station is recalled to the originating station after the Station Call Transfer Recall Timer expires. If enabled, calls are recalled from a VDN when the Station Call Transfer Recall Timer expires.

Available only if Basic Vectoring and Vectoring (Prompting) are enabled for the system.

**Related topics:**

[Station Call Transfer Recall Timer \(seconds\)](#) on page 594

[Vectoring \(Basic\)](#) on page 952

[Vectoring \(Prompting\)](#) on page 953

***Reset Shift Timer (seconds)***

| Valid Entry | Usage   |
|-------------|---|
| 0 to 255    | Specifies the number of seconds that reset shift dial tone is audible before busy tone is heard. Reset shift dial tone allows the user to dial a new extension by dialing one new digit that replaces the last digit of the extension previously dialed. The new digit replaces the last digit of the extension previously dialed. An entry of 0 disables this feature.<br>Used only for station-to-station calls or private network calls using ISDN trunks. |

***Short Interdigit Timer (seconds)***

| Valid Entry | Usage  |
|-------------|--|
| 3 to 9      | The time limit that digit analysis will wait for the next digit when it has predicted that all the digits have already been collected. |

***Special Dial Tone***

If enabled, allows the use of Special Dial Tone.

Special dial tone notifies an analog-telephone user if certain features are still active when the user goes off-hook. These features include:

- Call Forwarding
- Send All Calls
- Do Not Disturb

Requires a TN2182 circuit pack.

***Station Call Transfer Recall Timer (seconds)***

Allows a user-transferred call (station-to-station, a trunk call, or a DCS call) to re-terminate with priority ringing back to the station user who initiates the transfer operation if the transfer-to party does not answer the call within the administered Station Call Transfer Recall timer.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 999    | The time in seconds before a call redirects back to the station user who initiated the transfer operation. The entry 0 disables this feature. |

**Trunk Alerting Tone Interval (seconds)**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 60     | Specifies the interval at which the alerting tone is repeated on the call. By default, the value is 15 seconds. |

**Related topics:**

[Outgoing Trunk Alerting Timer \(minutes\)](#) on page 487

**Unanswered DID Call Timer (seconds)**

| Valid Entry | Usage   |
|-------------|---|
| 10 to 1024  | Limits how long a DID call can remain unanswered before routing to the DID/TIE/ISDN Intercept Treatment. This timer interacts with the nonadministrable 50-second Wait for Answer Supervision Timer (WAST). The WAST timer overrides this field. Thus if this field is set to a value equal to or greater than 50 seconds, the caller receives intercept tone instead of the normal attendant or announcement treatment that is given when the Unanswered DID Call Timer expires before the WAST. If the Unanswered DID Call Timer expires while the DID call is being processed by call vectoring, the timer is ignored. |
| blank       | Disables the timer.   |

**Related topics:**

[Wait Answer Supervision Timer](#) on page 609

**Use Trunk COR for Outgoing Trunk Disconnect/Alert**

Indicates whether the outgoing trunk disconnect timer or the outgoing trunk alerting timer is set based on the COR of the originating station or the trunk group. If enabled, the timer is based on the COR of the trunk, not the originating station. By default, this field is disabled.

**! Important:**

You must not enable outgoing trunk disconnect and outgoing trunk alerting timers at the same time. If you try to administer both timers, the system displays the following message:

```
Cannot enable both Outgoing Trunk Disc and Outgoing Trunk Alert
timers
```

**Related topics:**

[Outgoing Trunk Alerting Timer \(minutes\)](#) on page 487

[Outgoing Trunk Disconnect Timer \(minutes\)](#) on page 488

**DISTINCTIVE AUDIBLE ALERTING****Attendant Originated Calls**

Indicates which type of ringing applies to attendant-originated calls.

Available only if Tenant Partitioning is *not* enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| internal    | Internal ringing applies to attendant-originated calls.                      |
| external    | External ringing applies to attendant-originated calls. Default is external. |
| priority    | Priority ringing applies to attendant-originated calls.                      |

**Related topics:**

[Tenant Partitioning](#) on page 949

**Distinctive Audible Alerting (Internal, External, Priority)**

The number of rings for Internal, External, and Priority calls. For virtual stations, this applies to the mapped-to physical telephone.

| Valid Entry | Usage  |
|-------------|--|
| 1           | One burst of ringing signal per period. Default for internal calls.                |
| 2           | Two bursts of ringing signal per period. Default for external and attendant calls. |
| 3           | Three bursts of ringing signal per period. Default for priority calls.             |

**DTMF Tone Feedback Signal to VRU - Connection, Disconnection**

Available only if DTMF Feedback Signals for the Voice Response Unit (VRU) are enabled for the system.

| Valid Entry              | Usage  |
|--------------------------|--|
| 0 to 9, *, #, A, B, C, D | The code used to connect or disconnect the VRU. This can be a single digit, or a combination such as *99 to connect, #99 to disconnect. The tones must be programmed at the VRU as well. |
| blank                    | No tone is sent to the VRU.  |

**Related topics:**

[DTMF Feedback Signals For VRU](#) on page 951

**Feature-related system parameters: page 7**

**CONFERENCE/TRANSFER**

**Abort Conference Upon Hang-Up**

Allows DCP, hybrid, IP, wireless, or ISDN-BRI telephone users to abort the conference operation when they hang up. If enabled, this field changes a call placed on soft-hold in the conference-pending status to hard-held status if the user hangs up.

**Abort Transfer**

If enabled, stops the transfer operation whenever users press a non-idle call appearance button in the middle of the transfer operation, or when they hang up. If the system is configured to transfer calls upon hang-up, users can press the **Transfer** button, dial the complete transfer-to number, and hang-up to transfer the call. Users must select another non-idle call appearance to abort the transfer. Requires DCP, Hybrid, IP, ISDN-BRI or wireless telephones.

**Related topics:**

[Transfer Upon Hang-Up](#) on page 598

**External Ringing for Calls with Trunks**

Specifies ringing behavior on external trunk calls that are transferred or conferenced by stations or attendants, or extended by the attendant to an on-switch extension.

| Valid Entry | Usage  |
|-------------|--|
| all-calls   | All external trunk calls that are transferred or conferenced (either locally or remotely) receive external ringing.    |
| local-only  | External trunk calls that are transferred or conferenced locally receive external ringing.                             |
| none        | External ringing does not apply to external trunk calls that are transferred or conferenced.                           |
| remote-only | External trunk calls that are transferred or conferenced remotely receive external ringing. This is the default value. |

**Maximum Ports per Expanded Meet-me Conf**

Available only if ports are administered for the Expanded Meet-me Conference feature.

| Valid Entry | Usage  |
|-------------|--|
| 3 to 300    | The maximum number of conferees in an Expanded Meet-me Conference. This is a system-wide limit (that is, not administrable on a per Expanded-Meet-me VDN basis). |

**Related topics:**

[Maximum Number of Expanded Meet-me Conference Ports](#) on page 942

**No Dial Tone Conferencing**

If enabled, eliminates dial tone while setting up a conference when another line is on hold or is alerting.

**No Hold Conference Timeout**

| Valid Entry | Usage  |
|-------------|--|
| 20 to 120   | The number of seconds No Hold Conference call setup times out. The system <b>Answer Supervision</b> timer should be set to a value less than this. |

**Select Line Appearance Conferencing**

Allows the user to use the line appearance rather than the **Conference** button to include a call in a conference. If a user is on a call, and another line is on hold or an incoming call alerts on another line, the user can press the **Conference** button to bridge the calls together. Using the select line appearance capability, the user can press a **line appearance** button to complete a conference instead of pressing the **Conference** button a second time.

## Managing inventory

Enabling this field activates Select Line Appearance Conferencing.

### Transfer Upon Hang-Up

Enables or disables allowing users to transfer a call by pressing the **Transfer** button, dialing the desired extension, and then hanging up. The user can also wait to hang up, speak with the other party, then press **Transfer** again to complete the process. Users of the Call Park FAC can park a call without pressing the **Transfer** button a second time.

### Unhold

Allows the user to press the hold button on a telephone to release a hold (if no other line appearance is on hold or alerting). This does not apply to BRI telephones or attendant consoles.

Enabling this field activates this unhold capability.

## ***ANALOG BUSY AUTO CALLBACK***

If the Analog Busy Auto Callback Without Flash (ACB) feature is enabled, when a caller places a call through an analog station, and the called station is busy and has no coverage path or forwarding, then an announcement plays, announcing that the station is busy and prompting the caller to enter 1 for ACB or 2 to cover to a voice mail hunt group extension.

### Announcement

The extension of the announcement that plays for the Analog Busy Auto Callback Without Flash feature. This field cannot be left blank. Available only if Auto Callback Without Flash is enabled.

#### **Related topics:**

[Without Flash](#) on page 598

### Voice Mail Hunt Group Ext

A voice mail hunt group extension where the call is forwarded if the user enters 2 at the ACB announcement prompt. Available only if Auto Callback Without Flash is enabled.

#### **Related topics:**

[Without Flash](#) on page 598

### Without Flash

If enabled, provides automatic callback for analog stations without flashing the hook. It is applied only when the called station is busy and has no other coverage path or call forwarding. The caller can enable the automatic callback without flashing the hook or entering the feature access code.

## ***AUDIX ONE-STEP RECORDING***

On stations administered with this feature button, allows users to activate and deactivate the recording of active calls to their voice messaging system with the press of one button.

## Apply Ready Indication Tone To Which Parties In The Call

| Valid Entry              | Usage  |
|--------------------------|--|
| all<br>initiator<br>none | Administrators who hear the voice messaging recording ready tone. The default is all. This field cannot be left blank. |

## Interval For Applying Periodic Alerting Tone (seconds)

Available only if all parties on a call hear the voice messaging recording ready tone.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 60     | The number of seconds between alerting tones. The default value is a 15 second interval. Zero disables the tone. |

**Related topics:**

[Apply Ready Indication Tone To Which Parties In The Call](#) on page 599

## Recording Delay Timer (msecs)

| Valid Entry                          | Usage   |
|--------------------------------------|---|
| 0 to 4000 in<br>increments of<br>100 | The delay interval before starting a voice messaging recording. |

**Feature-related system parameters: page 8****ISDN PARAMETERS**

## Delay for USNI Calling Name for Analog Caller ID Phones (seconds)

For analog caller ID phones, Communication Manager is enhanced to wait for the FACILITY message (that contains the name information) before delivering an incoming call to the receiver. You can administer the time duration for which Communication Manager waits for the FACILITY message.

| Valid Entry      | Usage  |
|------------------|--|
| 0 to 6 (seconds) | Communication Manager waits for the administered time duration for the FACILITY message before delivering the incoming call to the receiver. By default, the timer is set to 0, indicating the feature is disabled. If the feature is enabled, the recommended timer value is 3 seconds. |

**Note:**

On page 3 of the ISDN Trunk Group screen, you must set **US NI Delayed Calling Name Update?** field to *y* for this feature to work.

**Related topics:**

[US NI Delayed Calling Name Update](#) on page 748

## Managing inventory

### Display Connected Name/Number for ISDN DCS Calls

If enabled, displays the connected name/number (if received) for ISDN DCS calls.

### Feature Plus Ext

An extension used for proper termination of Feature Plus signaling. For example, Message Waiting Indication (MWI) requires this extension to send the indication to the appropriate server running Communication Manager. Available only if ISDN Feature Plus signaling is enabled for the system.

#### **Related topics:**

[ISDN Feature Plus](#) on page 947

### International CPN Prefix

A number that allows you to apply prefixes to international calling numbers for display at receiving telephones. Accepts up to five digits and includes the characters \* and #. This number is useful for those telephones that use or implement call back features based on incoming call numbers.

When an ISDN-PRI call arrives, the incoming call setup is analyzed for:

- Whether the Type of Address (TOA) is national or international
- Whether the Numbering Plan Identifier (NPI) is Unknown or ISDN/Telephony

This administered prefix is applied to international calls.

Prefixing applies to any subsequent display on the same server when the call is transferred, covered, or forwarded. The same prefixing applies to outgoing ISDN-PRI calls when the connected number information is returned and meets the same TOA and NPI criteria. The prefix plus the calling/connected number digit string is limited to 15 digits, with truncation occurring at the least significant digits.

### Maximum Length

Available only if unknown numbers are administered as internal for the voice messaging system.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 20     | The maximum length of an unknown private number. Any unknown number longer than the administered value is considered external. This field cannot be blank. |

#### **Related topics:**

[Unknown Numbers Considered Internal for AUDIX](#) on page 602

### MWI - Number of Digits Per Voice Mail Subscriber

The number of digits per voice messaging system subscriber. Available only if Basic Supplementary Services or ISDN Feature Plus signaling is enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| 3 to 7      | The digit string length of subscribers translated in the Message Center entity. The value in this field must match the value administered for the voice messaging system. |

**Related topics:**

[ISDN Feature Plus](#) on page 947

[Basic Supplementary Services](#) on page 954

**National CPN Prefix**

Applies prefixes to national calling numbers for display at receiving telephones. This is useful for those telephones that use or implement call back features based on incoming call numbers. When an ISDN-PRI call arrives, the incoming call setup is analyzed for: (1) whether the Type of Address (TOA) is national or international, and (2) whether the Numbering Plan Identifier (NPI) is Unknown or ISDN/Telephony.

This administered prefix is applied to national calls. Prefixing applies to any subsequent display on the same server when the call is transferred, covered, or forwarded. The same prefixing applies to outgoing ISDN-PRI calls when the connected number information is returned and meets the same TOA and NPI criteria. The prefix plus the calling/connected number digit string is limited to 15 digits, with truncation occurring at the least significant digits.

| Valid Entry               | Usage   |
|---------------------------|---|
| 0 to 9<br>* or #<br>blank | A number consisting of up to five digits that allows the ability to apply prefixes to national calling numbers for display. |

**Pass Prefixed CPN to ASAI**

If enabled, passes Calling Party Number information (CPN) to ASAI. The prefixed number is not passed on to other adjuncts, Call Detail Recording, or servers/switches.

**Path Replacement While in Queue/Vectoring**

If enabled, allows Path Replacement after queue/vector processing has started. Depending on the version of CMS, some calls can go unrecorded if this capability is enabled. See Avaya technical support for more information.

**Path Replacement with Measurements**

If enabled, allows QSIG path replacement or DCS with Reroute to be attempted on measured calls.

**QSIG/ETSI TSC Extension**

The phantom endpoint extension for QSIG Call Independent Signaling Connections (CISCs) that are similar to NCA Temporary Signaling Connections (TSCs) (both incoming and outgoing). ETSI protocol TSCs as well as QSIG TSCs are supported.

**QSIG Path Replacement Extension**

The extension for the system used as part of the complete number sent in the Path Replacement Propose message.

**Send Custom Messages Through QSIG?**

If enabled, provides appropriate display information over QSIG links. Display information can include the Posted Messages feature.

**Send ISDN Trunk Group Name on Tandem Calls**

If enabled, provides consistent display information regardless of trunk type. Also provides only trunk group name.

**Send Non-ISDN Trunk Group Name as Connected Name**

If enabled, sends a name of the non-ISDN trunk group as the connected name when a call routes from ISDN to non-ISDN and the call is answered.

**Unknown Numbers Considered Internal for AUDIX**

Controls the treatment of an ISDN number whose numbering plan identification is “unknown” in a QSIG centralized voice messaging system arrangement. Available only if ISDN trunks are enabled for the system and if the hunt group is administered to send the calling party number to the voice messaging system.

| Valid Entry | Usage  |
|-------------|--|
| y           | The unknown number is considered “internal” and the voice messaging system tries to find a calling party name match for the digit string. If a name match is found, the voice messaging system provides the calling party’s name. If no name is found, the voice messaging system provides the calling party’s telephone number. |
| n           | The unknown number is considered “external” and the voice messaging system provides the calling party’s telephone number.  |

**Related topics:**

[Calling Party Number to INTUITY AUDIX](#) on page 662

**USNI Calling Name for Outgoing Calls?**

| Valid Entry | Usage   |
|-------------|---|
| y           | Sends a name on outgoing calls over NI PRI trunks.  |
| n           | Prevents sending calling name information with outgoing calls over NI PRI trunks.<br>Overrides the trunk group <b>Send Name</b> if enabled. |

 **Caution:**

The service provider’s local telephone company central office (CO) must be capable of accepting calling name information from Communication Manager in this way. For example, if the CO has a 5ESS, it must be a generic 5EXX or later. Failure to validate the CO capability might cause the CO to drop outgoing calls from the Avaya S8XXX Server. In this case, this field should be disabled.

**Related topics:**

[Send Name](#) on page 1021

## PARAMETERS FOR CREATING QSIG SELECTION NUMBERS

### Level 1 Code

The first level regional code of the Avaya S8XXX Server in the network.

Administer this field carefully. Communication Manager does not check to ensure you have entered a code that supports your entry in the **Network Level** field. Accepts up to five digits. Because blank regional codes are valid, an entry is not required if the **Network Level** field is 1 or 2.

In QSIG standards, this Level 1 code is called the Level 0 Regional Code.

Available only if the **Network Level** is set to 1 or 2.

### Level 2 Code

The second level regional code of the Avaya S8XXX Server in the network.

Administer this field carefully. Communication Manager does not check to ensure you have entered a code that supports your entry in the **Network Level** field. Accepts up to five digits. Because blank regional codes are valid, an entry is not required if the **Network Level** field is 2.

Available only if the **Network Level** is set to 2.

In QSIG standards, this Level 2 code is called the Level 1 Regional Code.

### Network Level

The value of the highest regional level employed by the PNP network. Use the following table to find the relationship between the network level and the Numbering Plan Identification/ Type of Number (NPI/TON) encoding used in the QSIG PartyNumber or the Calling Number and Connected Number IEs.

| Valid Entry | Usage   |
|-------------|---|
| 0           | NPI - PNP<br>TON - local  |
| 1           | NPI - PNP<br>TON - Regional Level 1   |
| 2           | NPI - PNP<br>TON - Regional Level 2   |
| blank       | If this field is blank and the <b>Send Calling Number and/or Send Connected Number</b> field is y or r with private specified for the <b>Numbering Format</b> field on the ISDN Trunk Group screen, the Calling Number and/or Connected Number IEs is not sent. If the field is left blank but private has been specified in the <b>Numbering Format</b> field on the ISDN Trunk Group screen, the Identification Number (PartyNumber data type) is sent for QSIG PartyNumbers encoded in ASN.1-defined APDUs. In this case, the ASN.1 data type containing the PartyNumber (PresentedAddressScreened, PresentedAddressUnscreened, PresentedNumberScreened, or PresentedNumberUnscreened) is sent marked as PresentationRestricted with NULL for the associated digits. |

**Feature-related system parameters: page 9**

**CPN/ANI/ICLID PARAMETERS**

CPN/ANI/ICLID Replacement for Restricted Calls

A text string used to replace the restricted numbers on the display. Accepts up to 15 characters.

CPN/ANI/ICLID Replacement for Unavailable Calls

A text string used to replace the unavailable numbers on the display. Accepts up to 15 characters.

**DISPLAY TEXT**

Extension only label for Team button on 96xx H.323 terminals

Available only if the **Team Btn Display Name** for the Class of Restriction is enabled.

| Valid entries | Usage  |
|---------------|--|
| y             | For 96xx H.323 telephones, displays the station extension without the team button label. 96xx H323 firmware version 2.0 or greater is recommended as it provides a special icon for team buttons. This field does not impact label customizations. |
| n             | For 96xx H.323 telephones, displays the station extension with the team button label.  |

**Related topics:**

[Team Btn Display Name](#) on page 490

Identity When Bridging

Determines whether the telephone display shows the literal identity of the bridged appearance or the virtual identity.

 **Note:**

When you choose the station option, you must update the Public/Unknown Numbering Format with the Extension Codes of the stations that display the caller's or answering party's assigned identification.

| Valid Entry | Usage   |
|-------------|---|
| principal   | The location from which the caller is bridging in. This is the default. |
| station     | The caller's and the answering party's assigned identification.         |

**Related topics:**

[Numbering — Public/Unknown Format](#) on page 814

User Guidance Display

If enabled, the telephone display shows user guidance messages. This field is disabled by default. x is an invalid entry.

## INTERNATIONAL CALL ROUTING PARAMETERS

### Local Country Code

A valid PSTN E.164 country code. For example, an SBS node in the United States uses a code of 1. For a list of country codes, see the International Telecommunications Union *List of ITU-T Recommendation E.164 Assigned Country Codes* . Accepts up to three digits.

#### Related topics:

[International Access Code](#) on page 605

[Carrier Medium](#) on page 722

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

[SBS](#) on page 744

### International Access Code

The access code required by the PSTN to route calls out of the country. This code is included with the telephone number received from the SBS terminating node if the Local Country Codes of the originating and terminating nodes are different. For example, an SBS node in the United States uses an access code of 011. Accepts up to five digits.

#### Note:

Once administered, this field cannot be cleared until all trunk groups administered for SBS signaling have been removed. If the international call routing parameters are not administered for the system and SBS is enabled for the trunk, a warning is displayed: `Must set INTERNATIONAL CALL ROUTING parameters on system-parameters features.`

#### Related topics:

[Local Country Code](#) on page 605

[Carrier Medium](#) on page 722

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

[SBS](#) on page 744

[Signaling group](#) on page 854

[Trunk Group](#) on page 977

## ENBLOC DIALING PARAMETERS

### Enable Enbloc Dialing without ARS FAC

Enables Enbloc Dialing without the need to dial a FAC. By default, this field is disabled.

### Minimum Digit Length

Available only if Enbloc Dialing without an ARS FAC is enabled.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 20     | The number of digits before Enbloc Calling Treatment is activated. Default is extension length plus 1. |

**Related topics:**

[Enable Enbloc Dialing without ARS FAC](#) on page 605

**CALLER ID ON CALL WAITING PARAMETERS**

Caller ID on Call Waiting Delay Timer (msec)

| Valid Entry | Usage   |
|-------------|---|
| 5 to 1275   | The desired delay in 5-millisecond intervals. Default is 200. |

**Feature-related system parameters: page 10**

***Allow Conference via Flash***

If enabled, allows an analog station to use flash to conference calls.

***Charge Display Update Frequency (seconds)***

Available only if Advice of Charge or Periodic Pulse Metering with display functions is used.

| Valid Entry       | Usage  |
|-------------------|--|
| 10 to 60<br>blank | The amount of time in seconds between charge-display updates. Frequent display updates might have considerable performance impact. If the duration of a call is less than the Charge Display Update Frequency, the display does not automatically show charge information. |

***Date Format on 607/2400/4600/6400 Terminals***

The format of the date as displayed on the telephones.

| Valid Entry | Usage            |
|-------------|------------------|
| mm/dd/yy    | (month/day/year) |
| dd/mm/yy    | (day/month/year) |
| yy/mm/dd    | year/month/day)  |

***Date Format on Terminals***

The date is in mm/dd/yy, dd/mm/yy, and yy/mm/dd formats.

***Edit Dialing on 96xx H.323 Terminals***

If enabled, allows an end-user to pre-dial a number when the telephone is on-hook. Disabled by default.

***Hear Zip Tone Following VOA?***

Enables or disables zip tone alerts to a telephone user when the announcement has completed and a caller is now connected. CallMaster set and attendant console users hear double zip tone following the announcement. All other telephone users hear single zip tone.

 **Note:**

This field does not effect auto-answer zip tone heard prior to the VDN of Origin Announcement (VOA).

**Intercept Treatment on Failed Trunk Transfers**

| Valid Entry | Usage  |
|-------------|--|
| y           | Provides intercept treatment to calls failing trunk transfers. |
| n           | Drops calls failing trunk transfers.                           |

**Level of Tone Detection**

Used only when users are having difficulty placing outgoing calls due to inaccurate detection of network dial tone.

| Valid Entry | Usage  |
|-------------|--|
| broadband   | This is the least exact of the levels of tone detection. If Avaya Communication Manager detects any tone at all, it interprets this as dial tone.  |
| medium      | The server running Avaya Communication Manager interprets any tone which has a continuous “on” period of longer than 1 second as dial tone. Otherwise, the server accepts whatever the tone detector circuit pack reports. |
| precise     | Communication Manager accepts whatever the tone detector circuit pack reports.   |

**Misoperation Alerting**

| Valid Entry | Usage   |
|-------------|---|
| y           | Enables misoperation recall alerting on multi-appearance stations, analog stations, and attendant consoles. |
| n           | Uses standard misoperation handling without recall alerting.  |

**Network Feedback During Tone Detection**

If enabled, provides audible feedback to the user while the system attempts to detect dial tone.

**On-hook Dialing on 607/2400/4600/6400/8400 Terminals**

If enabled, allows users to dial without lifting the handset. Users hear dial tone when they press the **Speaker** button, even if the handset is on-hook.

For 6400/8400, 607, 2420, 2410, and 4600 telephone users with speakerphones.

**Outpulse Without Tone**

| Valid Entry | Usage  |
|-------------|--|
| y           | The server outpulses digits even when a dial tone has not been received. |
| n           | The calling party receives intercept tone if no dial tone is detected.   |

**Pull Transfer**

Enables or disables the Pull Transfer feature on a system-wide basis. This allows either the transferring or transferred-to party to press the **Transfer** button to complete the transfer operation.

**Repetitive Call Waiting Interval (sec)**

Available only if the Repetitive Call Waiting Tone is enabled.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 99     | The number of seconds between call waiting tones. |

**Related topics:**

[Repetitive Call Waiting Tone](#) on page 608

**Repetitive Call Waiting Tone**

If enabled, a repetitive call waiting tone is provided to the called party for all types of call waiting access.

**Station Tone Forward Disconnect**

Applies to any station other than one administered as a data endpoint, an attendant console, a BRI telephone, an auto answer, or as an Outgoing Call Management (OCM) agent.

| Valid Entry                  | Usage   |
|------------------------------|---|
| busy<br>intercept<br>silence | The treatment given to a station that is the last party remaining off-hook on a call, until that station is placed on-hook, or until the tone has played for 45 seconds and is followed by silence. |

**System Updates Time On Station Displays**

If enabled, automatically updates the system time on display telephones when background maintenance is run (for example, when the set is plugged in). This does not apply to telephones, such as BRI telephones, where the user sets the time.

**Update Transferred Ring Pattern**

If enabled, changes the ringing pattern from internal to external when an internal station transfers an external call. Use this feature if most calls go through an attendant, so that users are able to distinguish an external call.

**Vector Disconnect Timer (min)**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 240    | Determines when the trunk gets disconnected if incoming or outgoing disconnect supervision is disabled for the trunk group. |
| blank       | Avaya Communication Manager does not initiate a disconnect.   |

**Related topics:**

[Disconnect Supervision-Out](#) on page 735

[Disconnect Supervision-In](#) on page 823

**Wait Answer Supervision Timer**

| Valid Entry | Usage   |
|-------------|---|
| y           | Calls to stations unanswered after 50 seconds are dropped.      |
| n           | Unanswered calls drop only when the calling party goes on-hook. |

**Related topics:**

[Unanswered DID Call Timer \(seconds\)](#) on page 595

**ITALIAN DCS PROTOCOL**

The next three fields control the Italian DCS Protocol feature.

**Apply Intercept Locally**

If enabled, DID/CO intercept treatment is applied locally instead of on the originating server or switch. Available only if **Italian Protocol** is enabled.

**Related topics:**

[Italian Protocol Enabled](#) on page 609

**Enforce PNT-to-PNT Restrictions**

If enabled, restrictions and denial of PNT-to-PNT connections are enforced when the EDCS message is unavailable. Available only if **Italian Protocol** is enabled.

**Related topics:**

[Italian Protocol Enabled](#) on page 609

**Italian Protocol Enabled**

Enables or disables the Italian DCS feature on a system-wide basis.

**Related topics:**

[Enforce PNT-to-PNT Restrictions](#) on page 609

**Feature-related system parameters: page 11****CALL CENTER SYSTEM PARAMETERS EAS****Delay**

Available only if Expert Agent Selection (EAS) or ASAI Link Core Capabilities are enabled for the system.

| Valid Entry      | Usage   |
|------------------|---|
| 0 to 99<br>blank | The number of seconds the caller hears ringback before the Direct Agent Announcement is heard by the calling party. |

**Related topics:**

[ASAI Link Core Capabilities](#) on page 943

[Expert Agent Selection \(EAS\)](#) on page 951

Managing inventory

#### Direct Agent Announcement Extension

The extension of the direct agent announcement.

#### Expert Agent Selection (EAS) Enabled

Enables or disables Expert Agent Selection (EAS). Enable only if ACD or vectoring hunt groups exist or if existing ACD or vectoring hunt groups are skill-based. Available only if EAS is enabled for the system.

**Related topics:**

[Expert Agent Selection \(EAS\)](#) on page 951

#### Message Waiting Lamp Indicates Status For

Available only if Expert Agent Selection (EAS) is enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| station     | The message waiting lamp on a telephone indicates the message is for the telephone extension. |
| loginID     | The message waiting lamp on a telephone indicates the message is for the agent login ID.      |

**Related topics:**

[Expert Agent Selection \(EAS\)](#) on page 951

#### Minimum Agent-LoginID Password Length

The minimum number of digits that must be administered as an EAS Agent's LoginID password. Accepts up to nine digits. Available only if Expert Agent Selection (EAS) is enabled for the system.

**Related topics:**

[Expert Agent Selection \(EAS\)](#) on page 951

### **VECTORING**

#### Available Agent Adjustments for BSR

Allows or disallows Best Service Routing (BSR) adjustments to available agents. Available only if Vectoring (Best Service Routing) is enabled for the system.

**Related topics:**

[Vectoring \(Best Service Routing\)](#) on page 952

#### BSR Tie Strategy

Available only if Vectoring (Best Service Routing) is enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| 1st-found   | BSR uses the first selection for routing. This is the default.  |
| alternate   | Allows alternating the BSR selection algorithm when a tie in Expected Wait Time (EWT) or available agent criteria occurs. Every other time a tie occurs for calls from the same active Vector Directory Number (VDN), |

| Valid Entry | Usage   |
|-------------|---|
|             | the selection from the consider step with the tie is used instead of the first selected split/skill or location to send the call. This helps balance the routing over the considered local splits/skills and remote locations when cost of routing remotely is not a concern. |

**Related topics:**

[Vectoring \(Best Service Routing\)](#) on page 952

## Converse First Data Delay

Available only if Vectoring (Basic) is enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 9      | The number of seconds data is prevented from being outputted as a result of a converse vector step from the system to Avaya IR before IR is ready. The delay commences when the IR port answers the call. |

**Related topics:**

[Vectoring \(Basic\)](#) on page 952

## Converse Second Data Delay

Available only if Vectoring (Basic) is enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 9      | Number of seconds used when two groups of digits are being outputted, as a result of a converse vector step, from the system to Avaya IR. Prevents the second set from being outputted before IR is ready. The delay commences when the first group of digits has been outputted. |

**Related topics:**

[Vectoring \(Basic\)](#) on page 952

## Converse Signaling Pause

The length in milliseconds of the delay between digits being passed. The optimum timer settings for Avaya IR are 60 msec tone and 60 msec pause.

Available only if Vectoring (Basic) and DTMF feedback signals are enabled for the system.

| Valid Entry                      | Usage  |
|----------------------------------|--|
| 40 to 2550 (in increments of 10) | <p>Values are rounded up or down depending upon the type of circuit pack used to output the digits.</p> <ul style="list-style-type: none"> <li>• <b>TN742B or later suffix analog board</b> — Rounds up or down to the nearest 25 msec. For example, a 130 msec tone rounds down to 125 msec, a 70 msec pause rounds up to 75 msec for a total of 200 msec per tone</li> <li>• <b>TN464F, TN767E or later suffix DS1 boards</b> — Rounds up to the nearest 20 msec. For example, a 130 msec tone rounds up to 140</li> </ul> |

| Valid Entry | Usage  |
|-------------|--|
|             | <p>msecs, a 70 msec pause rounds up to 80 msecs for a total of 220 msecs per tone.</p> <p>If a circuit pack has been used for end-to-end signaling to IR, and has then been used to send digits to a different destination, IR timers might stay in effect. To reset the timers to the system default, pull and reseal the circuit pack.</p> |

**Related topics:**

[DTMF Feedback Signals For VRU](#) on page 951

[Vectoring \(Basic\)](#) on page 952

Converse Signaling Tone

The length in milliseconds of the digit tone for digits being passed to Avaya IR. The optimum timer settings for IR are 60 msec tone and 60 msec pause.

Available only if Vectoring (Basic) and DTMF feedback signals are enabled for the system.

| Valid Entry                      | Usage  |
|----------------------------------|--|
| 40 to 2550 (in increments of 10) | <p>Values are rounded up or down depending upon the type of circuit pack used to outpulse the digits.</p> <ul style="list-style-type: none"> <li>• <b>TN742B or later suffix analog board</b> — Rounds up or down to the nearest 25 msecs. For example, a 130 msec tone rounds down to 125 msecs, a 70 msec pause rounds up to 75 msec for a total of 200 msecs per tone</li> <li>• <b>TN464F, TN767E or later suffix DS1 boards</b> — Rounds up to the nearest 20 msecs. For example, a 130 msec tone rounds up to 140 msecs, a 70 msec pause rounds up to 80 msecs for a total of 220 msecs per tone.</li> </ul> <p>If a circuit pack has been used for end-to-end signaling to IR, and has then been used to send digits to a different destination, IR timers might stay in effect. To reset the timers to the system default, pull and reseal the circuit pack.</p> |

**Related topics:**

[DTMF Feedback Signals For VRU](#) on page 951

[Vectoring \(Basic\)](#) on page 952

Interflow-qpos EWT Threshold

Available only if the Lookahead Interflow (LAI) is enabled for the system.

| Valid Entry     | Usage  |
|-----------------|--|
| 0 to 9<br>blank | <p>Number of seconds for this threshold. Any calls predicted to be answered before this threshold are not interflowed, therefore saving CPU resources.</p> |

**Related topics:**

[Lookahead Interflow \(LAI\)](#) on page 951

### Prompting Timeout (secs)

Available only if Vectoring (Prompting) is enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| 4 to 10     | The number of seconds before the <b>Collect Digits</b> command times out for callers using rotary dialing. |

**Related topics:**

[Vectoring \(Prompting\)](#) on page 953

### Reverse Star/Pound Digit for Collect Step

The "\*" is interpreted as a caller end-of-dialing indicator and the "#" is an indicator to clear all digits previously entered by the caller for the current collect vector step.

| Valid Entry | Usage   |
|-------------|---|
| y           | Reverses the star and pound digits for the collect vector step. This does not affect any other vector step or other non-ACD feature, such as ARS. |
| n           | The "*" and "#" digit-processing is unchanged.  |

### Store VDN Name in Station's Local Call Log

Enables or disables the sending of a message from Communication Manager telling the telephone to store the VDN name or the calling party's name in the station call log for any of the following telephones:

- 2420
- 4610
- 4620
- 4625

**SERVICE OBSERVING**

### Allow Two Observers in Same Call

| Valid Entry | Usage   |
|-------------|---|
| y           | Two service observers can monitor the same EAS Agent LoginID or station extension, and up to two service observers can be on the same two-party call or in a conferenced call having more than two parties. |
| n           | Only one service observer can monitor the EAS Agent LoginID or station extension.   |

### Service Observing: Warning Tone

Enables or disables a warning tone that is heard by telephone users and calling parties whenever their calls are being monitored using the Service Observing feature. Available only if Service Observing (Basic) is enabled for the system.

 **Warning:**

The use of Service Observing features might be subject to federal, state, or local laws, rules or regulations — or require the consent of one or both of the parties to the conversation. Customers should familiarize themselves and comply with all applicable laws, rules, and regulations before using these features.

**Related topics:**

[or Conference Tone](#) on page 614

[Service Observing \(Basic\)](#) on page 952

### or Conference Tone

Enables or disables a conference tone heard by telephone users and calling parties whenever their calls are being monitored using the Service Observing feature. Available only if Service Observing (Basic) is enabled for the system. Not available if a warning tone is administered for Service Observing.

 **Warning:**

The use of Service Observing features might be subject to federal, state, or local laws, rules or regulations — or require the consent of one or both of the parties to the conversation. Customers should familiarize themselves and comply with all applicable laws, rules, and regulations before using these features.

**Related topics:**

[Service Observing: Warning Tone](#) on page 614

[Service Observing \(Basic\)](#) on page 952

### Service Observing Allowed with Exclusion

Exclusion allows multi-appearance telephone users to keep other users with the same extension from bridging onto an existing call.

| Valid Entry | Usage   |
|-------------|---|
| y           | Allows Service Observing of a station with Exclusion active, either by Class Of Service or by manual activation of Exclusion.   |
| n           | Observing towards a station with Exclusion active is denied, or if Exclusion is activated by a station while being observed, all bridged parties including the observer are dropped. This is the default. |

**Feature-related system parameters: page 12****AGENT AND CALL SELECTION**

## ACW Agents Considered Idle

| Valid Entry | Usage   |
|-------------|---|
| y           | Include agents who are in After Call Work (ACW) mode in the Most-Idle Agent queue. This means that ACW is counted as idle time. |
| n           | Exclude ACW agents from the queue.  |

## Auto Reserve Agents

When a critical skill is not meeting its service level, auto-reserve puts agents in standby for their other skills to ensure that there is an available agent when the next call arrives for the critical skill. When an agent becomes available, all of his or her assigned skills are checked to see if any auto-reserve skills are not meeting their target service level. If so, the agent is made available only in those skills.

| Valid Entry    | Usage   |
|----------------|---|
| all            | Puts an agent on standby for all skills.            |
| none           | Agent is not on standby for any additional skills.  |
| secondary-only | Puts an agent on standby only for secondary skills. |

## Call Selection Measurement

Determines how Avaya Communication Manager selects a call for an agent when the agent becomes available and there are calls in queue.

| Valid Entry         | Usage  |
|---------------------|--|
| current-wait-time   | Selects the oldest call waiting for any of the agent's skills.   |
| predicted-wait-time | Uses the time a call is predicted to wait in queue instead of the time the call has already waited. Available only if Business Advocate features are enabled for the system. |

**Related topics:**

[Business Advocate](#) on page 951

## Copy ASAI UI During Conference/Transfer

Enables or disables copying user-to-user (UI) information during a conference call or during call transfers. Available only if ASAI Link Core Capabilities or Computer Telephony Adjunct Links are enabled for the system.

 **Note:**

The system copies all UI information, not just ASAI UI. Copying occurs only during a human-initiated conference or transfer. Communication Manager does *not* copy the UI if the conference or transfer is initiated by ASAI.

**Related topics:**

[ASAI Link Core Capabilities](#) on page 943

[Computer Telephony Adjunct Links](#) on page 944

**MIA Across Splits or Skills**

Enables or disables the removal of an agent from the Most Idle Agent (MIA) queue for all available splits/skills/hunt groups when answering a call from any of these groups.

**Service Level Maximizer Algorithm**

Selects an alternative algorithm for selecting agents and delivering calls in order to maximize service level targets. Available only if Service Level Maximizer is enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| actual      | The Actual Service Level (ASL) is determined as a percentage on a hunt group basis using the number of accepted calls in the current interval divided by the total calls in the current interval. A call is counted as accepted if it is answered within the target service level time period. |
| weighted    | The Weighted Service Level (WSL) is based on a weighting calculation that uses the difference between the target time and the estimated wait time.   |

**Related topics:**

[Service Level Maximizer](#) on page 952

**Service Level Supervisor Call Selection Override**

Determines whether Avaya Communication Manager changes agent call handling preferences when a skill using Service Level Supervisor exceeds its Level 1 threshold. Available only if Expert Agent Selection (EAS) and the Business Advocate features are enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| y           | Overrides the normal call handling preferences of a skill's assigned agents in this situation. |
| n           | Normal call handling preferences are in effect when the skill exceeds its Level 1 threshold.   |

**Related topics:**

[Business Advocate](#) on page 951

[Expert Agent Selection \(EAS\)](#) on page 951

**ASAI**

**Call Classification After Answer Supervision?**

For use with ASAI Outbound Call Management (OCM).

| Valid Entry | Usage  |
|-------------|--|
| y           | Forces the server running Communication Manager to rely on the network to provide answer/busy/drop classification to the server. After the |

| Valid Entry | Usage   |
|-------------|---|
|             | call has been answered, a call classifier can be added to perform answering machine, modem, and voice answering detection.                |
| n           | Always connects a classifier after call setup for determining call progress and answer. ISDN progress messages generally take precedence. |

Send UCID to ASAI

Enables or disables the transmission of Universal Call ID (UCID) information to ASAI.

### **CALL MANAGEMENT SYSTEMS**

#### REPORTING ADJUNCT RELEASE

CMS (appl mis)

| Valid Entry | Usage  |
|-------------|--|
| R12         | Call Management System R12 is connected to the mis1 link, and to the mis2 link for a second CMS. Do not use for Avaya IQ.  |
| R13         | CMS R13 is connected to the mis1 link, and to the mis2 link for a second CMS. Do not use for Avaya IQ.   |
| R13.1       | CMS R13.1 is connected to the mis1 link, and to the mis2 link for a second CMS. Reporting adjuncts CMS, Avaya IQ, or both can be connected. Only CMS R13.1 or R14 are allowed with Avaya IQ 4.0.   |
| R14.1       | CMS R14 is connected to the mis1 link, and to the mis2 link for a second CMS. This release or later is required to activate the Special Application SA9062 to allow permissive use with Communication Manager Expanded Dial Plan (EDP-allowing extensions greater than seven digits in the dial plan). This allows CMS to be connected with or without Avaya IQ. If any extensions greater than seven digits are received by CMS, the left-most digit in excess of seven is deleted, leaving the right-most seven digits for tracking and reporting. Avaya IQ tracks and reports on the full EDP extensions. |
| R15         | CMS R14 is connected to the mis1 link, and to the mis2 link for a second CMS.  |

#### **Related topics:**

[IQ \(appl ccr\)](#) on page 617

IQ (appl ccr)

Expert Agent Selection (EAS) and Universal Call ID (UCID) must be enabled before a connection can be established with Avaya IQ.

| Valid Entry | Usage   |
|-------------|---|
| 4.0<br>5.0  | The release of Avaya IQ connected to the ccr1 link, and to the ccr2 link for a second Avaya IQ. |
| blank       | Avaya IQ is not connected. This is the default.   |

**Related topics:**

[Create Universal Call ID \(UCID\)](#) on page 590

[Expert Agent Selection \(EAS\)](#) on page 951

**OTHER CALL MANAGEMENT SYSTEM FIELDS**

ACD Login Identification Length

Available only if Expert Agent Selection (EAS) is *not* enabled and BCMS/VuStats Login IDs are enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 9      | The number of digits for an ACD agent login ID that identifies an ACD agent to the Call Management System. This number must equal the number of characters in the agent's login ID and cannot be 0. |

**Related topics:**

[BCMS/VuStats LoginIDs](#) on page 618

[Expert Agent Selection \(EAS\)](#) on page 951

BCMS/VuStats Abandon Call Timer (seconds)

| Valid Entry      | Usage   |
|------------------|---|
| 1 to 10<br>blank | The number of seconds before calls are considered abandoned. Calls with talk time that is less than this number and are not held, are tracked by the Basic Call Management System (BCMS) and displayed by VuStats as ABAND calls. |

BCMS/VuStats LoginIDs

Enables or disables valid agent login IDs to monitor call activity by an agent. Basic Call Management System (BCMS) and VuStats login IDs are available in addition to Expert Agent Select (EAS) login IDs if EAS is enabled on the system. Both BCMS and CMS use the same login ID for an agent.

**Related topics:**

[Expert Agent Selection \(EAS\)](#) on page 951

BCMS/VuStats Measurement Interval

Available only if BCMS (Basic) or VuStats is enabled for the system.

| Valid Entry       | Usage  |
|-------------------|--|
| half-hour<br>hour | Selects measurement intervals for polling and reporting data. There are a maximum of 25 time slots available for measurement intervals. If hour is specified, an entire day of traffic information will be available for history reports. Otherwise, only half a day will be available. This does not affect daily summaries as they always reflect traffic information for the entire day. The interval can be changed at any time, but does not go into effect until the current interval completes. |

**Related topics:**

[BCMS \(Basic\)](#) on page 950

[VuStats](#) on page 953

## Clear VuStats Shift Data

| Valid Entry | Usage  |
|-------------|--|
| on-login    | Clears shift data for an agent when the agent logs in. |
| at-midnight | Clears shift data for all agents at midnight.          |

## Remove Inactive BCMS/VuStats Agents

| Valid Entry | Usage  |
|-------------|--|
| y           | Agents are removed from reports when they have no staff time during the previous seven days. |
| n           | Agents remain on the report even if they have no staff time for any period of time.          |

## Validate BCMS/VuStats Login IDs

| Valid Entry | Usage   |
|-------------|---|
| y           | Allows entry of only login-IDs that have been administered for the Basic Call Management System (BCMS). |
| n           | Allows entry of any ACD login of the proper length.   |

**Feature-related system parameters: page 13****CALL CENTER MISCELLANEOUS**

## Allow Ringer-off with Auto-Answer

Allows or disallows permission for an agent to use the ringer-off feature button that prevents ringing on Expert Agent Selection (EAS) auto-answer calls.

## Callr-info Display Timer (sec)

| Valid Entries | Usage   |
|---------------|---|
| 3 to 60       | Administer the timer to display the information which caller has dialed on IP (H.323) telephones. The default value is 10 secs. |

## Clear Callr-info

Specifies when the collected digits Callr-Info display is removed from the agent or station display.

| Valid Entry | Usage   |
|-------------|---|
| leave-ACW   | Leaves the display up while the agent is in After Call Work (ACW) mode. |
| next-call   | Clears the display when the next call is received. This is the default. |

## Managing inventory

| Valid Entry     | Usage   |
|-----------------|---|
| on-call-release | Clears the display on the second line of a two-line display as soon as the call is released, either because of receiving call disconnect or the agent/station user pressing the release button. |

## Interruptible Aux Deactivation Threshold (%)

| Valid Entry | Usage   |
|-------------|---|
| 50 to 100   | Specifies the maximum percentage level of service before the Interruptible Aux feature is deactivated. While the Interruptible Aux threshold is the lower limit below which the interruptible aux feature is activated, Interruptible Aux Deactivation Threshold is the upper limited above which the interruptible aux feature is deactivated. Two separate thresholds for activation and deactivation ensure that the interruptibility state does not bounce on and off due to small changes in agent availability or call arrivals. The default is 95. |

### Example

If the Service Level Target (activation threshold) is 75% and the Deactivation Threshold is 70%, the feature is deactivated when the Service Level gets to 82.5%. The interruptible aux feature resumes if the service level drops below 75% in the specified number.

## Interruptible Aux Notification Display

Specifies the interruptible Aux notification display message. The system displays this message to an agent when the agent is being interrupted. Default message is: *You are needed.* Accepts up to 30 alphanumeric characters.

## Interruptible Aux Notification Timer (sec)

| Valid Entry | Usage  |
|-------------|--|
| 1 to 9      | Specifies the number of seconds the endpoint interruptible aux notifications, the flashing lamp, display, or tone, are on before an auto-in-interrupt or manual-in-interrupt agent is made available. This delay makes sure that an agent is not immediately made available when he presses an interruptible aux button. Also, this delay provides a brief period to an agent already in interruptible Aux mode before that agent is made available automatically. Default is 3. |

## PC Non-Predictive Reports Skill

Administers a skill hunt group used for reporting associated with Proactive Contact non-predictive switch-classified calls on a per-system basis. Reports are generated as though the agent were in the ACD-OUT state. Available only if reporting for PC Non-Predictive Calls is enabled.

| Valid Entry | Usage                                     |
|-------------|---|
| 1 to 99     | Skill number for S8300 or S8400 switches. |

| Valid Entry | Usage                                |
|-------------|--------------------------------------|
| 1 to 8000   | Skill number for all other platforms |

**Related topics:**

[Reporting for PC Non-Predictive Calls](#) on page 621

**Reporting for PC Non-Predictive Calls**

Activates or deactivates improved integration with Proactive Contact Outbound Calling for non switch-classified outbound calling. For example, this feature improves Call Management System tracking for switch-classified and non-switch classified (agent classified) outbound calls placed by the Proactive Contact soft dialer through ASAI. Default is n.

**Service Level Algorithm for SLM**

Administers the algorithm used to determine service levels for Service Level Maximizer (SLM). Available only if Expert Agent Selection (EAS) has been enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| actual      | The Actual Service Level (ASL) based on an algorithm that is determined as a percentage on a hunt group (skill) basis using the number of calls answered within the target service level time period in the current interval, divided by the total calls in the interval. This is the default. |
| weighted    | The Weighted Service Level (WSL) algorithm based on a weighting calculation that uses the difference between the target time and the estimated wait time.  |

**Related topics:**

[Expert Agent Selection \(EAS\)](#) on page 951

**Feature-related system parameters: page 14****REASON CODES****Aux Work Reason Code Type**

| Valid Entry | Usage  |
|-------------|--|
| none        | An agent does not enter a Reason Code when entering AUX work.  |
| requested   | An agent can enter a Reason Code when entering AUX mode but is not forced to do so. Available only if Reason Codes and EAS are enabled for the system. |
| forced      | An agent is forced to enter a Reason Code when entering AUX mode. Available only if Reason Codes and EAS are enabled for the system.                   |

**Related topics:**

[Expert Agent Selection \(EAS\)](#) on page 951

[Reason Codes](#) on page 952

Logout Reason Code Type

| Valid Entry | Usage   |
|-------------|---|
| none        | An agent does not enter a Reason Code when logging out.   |
| requested   | An agent can enter a Reason Code when logging out but do not want to force the agent to do so. Available only if Reason Codes and EAS are enabled for the system. |
| forced      | An agent is forced to enter a Reason Code when logging out. Available only if Reason Codes and EAS are enabled for the system.                                    |

**Related topics:**

[Expert Agent Selection \(EAS\)](#) on page 951

[Reason Codes](#) on page 952

Two-Digit Aux Work Reason Codes

Enables or disables two-digit reason codes for agent state changes for AUX Work.

**REDIRECTION ON IP CONNECTIVITY FAILURE**

Auto-answer IP Failure AUX Reason Code

| Valid Entry | Usage  |
|-------------|--|
| 0 to 99     | The reason code assigned for auto-answer IP failure, as the reason the agent was put into AUX Work.. |

Switch Hook Query Response Timeout

| Valid Entry        | Usage   |
|--------------------|---|
| 500 to 5000 (msec) | The time that call processing waits for a response from the switch hook query before Return on IP Connectivity Failure (ROIF) is triggered. |
| blank              | ROIF is not active.   |

**MAXIMUM AGENT OCCUPANCY PARAMETERS**

The Maximum Agent Occupancy (MAO) threshold is a system-administered value that is applied across all administered agents and is based on the total percentage of agent time in call service. MAO data is derived from the same calculations that are used to derive Least Occupied Agent (LOA).

When an agent who exceeds the specified MAO threshold attempts to become available, he or she is automatically placed in AUX mode for the reason code administered for this purpose. When the occupancy for such pending agents drops below the MAO, they are released from AUX mode and made available.

## Maximum Agent Occupancy AUX Reason Code

| Valid Entry | Usage  |
|-------------|--|
| 0 to 99     | A reason code value. Avaya recommends that you do not use reason code 0. Default is 9. |

## Maximum Agent Occupancy Percentage

| Valid Entry | Usage  |
|-------------|--|
| 0 to 100    | The maximum percentage of time an agent can be taking calls. This time is based on Maximum Agent Occupancy (MAO) calculations. Default is 100. |

**Feature-related system parameters: page 15****FORCED AGENT LOGOUT PARAMETERS**

## ACW Forced Logout Reason Code

Available only if the Call Center Release is 3.0 or later and Expert Agent Selection (EAS) is enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9      | The reason for logging out the agent due to time-out in After Call Work (ACW). |

**Related topics:**

[Expert Agent Selection \(EAS\) Enabled](#) on page 610

[Call Center Release](#) on page 951

[Reason Codes](#) on page 952

## Clock Time Forced Logout Reason Code

| Valid Entry | Usage   |
|-------------|---|
| 0 to 9      | The reason code for the Forced Agent Logout by Clock Time feature that allows administrators to set a specific time when the system automatically logs out Expert Agent Selection (EAS) agents. |

## Maximum Time Agent in ACW before Logout (sec.)

Available only for Call Center Release 3.0 or later and if Expert Agent Selection (EAS) is enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| 30 to 9999  | A system-wide maximum time an agent can be in After Call Work (ACW). When this timer expires, the agent is logged out. |
| blank       | There is no time-out. This is the default.   |

**Related topics:**

[Call Center Release](#) on page 951

[Expert Agent Selection \(EAS\)](#) on page 951

**Feature-related system parameters: page 16**

***SPECIAL TONE***

Special Dial Tone

Enables or disables an audible tone indicating that the station is locked.

Special Dial Tone for Digital / IP Stations

| Valid Entry                | Usage  |
|----------------------------|--|
| all<br>none<br>non-display | Specifies the type of dial tone used for digital or IP stations. |

***REDIRECTION NOTIFICATION***

Chained Call Forwarding

Enables or disables Chained Call Forwarding. Chained Call Forwarding allows calls to be forwarded to as many as 10 calling stations using a pre-set coverage path.

Display Notification Enhanced Call Forward

Enables or disables display notification for Enhanced Call Forward.

Display Notification for a locked Station

Enables or disables display notification for a locked station.

Display Notification for Call Forward

Enables or disables display notification for Call Forward.

Display Notification for Do Not Disturb

Enables or disables display notification for Do Not Disturb.

Display Notification for Limit Number of Concurrent Calls

Enables or disables display notification for Limit Number of Concurrent Calls.

Display Notification for Posted Messages

Enables or disables display notification for posted messages.

Display Notification for Send All Calls

Enables or disables display notification for Send All Calls.

## Scroll Status messages Timer (sec.)

| Valid Entry | Usage  |
|-------------|--|
| 5 to 10     | The time in seconds for displaying scroll status messages. The status information shows the feature that has the highest priority and is enabled. The features in order of decreasing priority are: <ul style="list-style-type: none"> <li>• Do Not Disturb</li> <li>• Send All Calls</li> <li>• Call Forward</li> <li>• Posted Messages</li> <li>• Limit Number of Concurrent Calls (LNCC)</li> <li>• Station Lock</li> </ul> |
| blank       | Deactivates the scrolling. This is the default.  |

**Feature-related system parameters: page 17****AUTOMATIC EXCLUSION PARAMETERS**

## Automatic Exclusion by COS

| Valid Entry | Usage  |
|-------------|--|
| y           | Enables automatic exclusion by a class of service when a user goes off-hook on a station with an assigned <b>Exclusion</b> button. This works only for stations on the local server running Communication Manager. |
| n           | Exclusion operates normally.   |

## Automatic Exclusion Coverage/Hold

Available only when Automatic Exclusion by COS is enabled.

| Valid Entry | Usage   |
|-------------|---|
| y           | The principal can bridge onto the call by pressing the appropriate bridged appearance button. And, if the coverage point places the exclusion call on hold, the principal can retrieve the call.                                    |
| n           | If a coverage point has answered a call and there is active exclusion on the call, the principal cannot bridge onto the call. And, if the coverage point places the exclusion call on hold, the principal cannot retrieve the call. |

**Related topics:**

[Automatic Exclusion by COS](#) on page 625

## Automatic Exclusion with Whisper Page

Available only Automatic Exclusion by COS is enabled.

## Managing inventory

| Valid Entry | Usage  |
|-------------|--|
| y           | The whisper page goes through to an excluded call.   |
| n           | The whisper page is denied when a station attempts to whisper page to a station that is on an excluded call. |

### Related topics:

[Automatic Exclusion by COS](#) on page 625

## Duration of Call Timer Display

| Valid Entry | Usage  |
|-------------|--|
| 3 to 30     | The length of time in 3 second increments that the call information remains on display after the call is terminated. |

## Password to Change COR by FAC

If this field contains a value, a password option is required. Accepts from four to eight digits.

Available only if **Change COR by FAC** is enabled for the system. Avaya recommends using this password option.

### Related topics:

[Change COR by FAC](#) on page 944

## Recall Rotary Digit

| Valid Entry | Usage   |
|-------------|---|
| 0 to 9      | The digit used for rotary telephones to receive recall dial tone. Dialing this digit simulates switch-hook flash so that users of rotary telephones can use features such as conference and transfer. The telephone must also be administered to use the recall rotary. This should be a number that is not the first digit in normal dialing patterns. |

## **WIRELESS PARAMETERS**

### Radio Controllers with Download Server Permission

The port location of the circuit pack containing the radio controllers with download server permission.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 64     | First and second characters are the cabinet number |
| A to E      | Third character is the carrier.                    |
| 0 to 20     | Fourth and fifth characters are the slot number.   |

**IP PARAMETERS****Direct IP-IP Audio Connections**

Allows or denies direct audio connections between IP endpoints that saves on bandwidth resources and improves sound quality of voice over IP transmissions.

**IP Audio Hairpinning**

If enabled, allows IP endpoints connected through the IP circuit pack in the server in IP format to bypass the Communication Manager TDM bus.

**RUSSIAN MULTI-FREQUENCY PACKET SIGNALING****Re-try**

Enables or disables the resending of address information on outgoing Russian MFP trunks. Specifically, the server running Communication Manager resends Russian MFP calling party number and dialed number information to the local telephone company central office (CO). The server resends the information only once over another outgoing trunk port of the same trunk group if Communication Manager receives a message that the information was received incorrectly by the CO. The switch also sends Russian MFP information over another trunk port if Communication Manager does not receive a timely response for the information.

**T2 (Backward Signal) Activation Timer (secs)**

| Valid Entry | Usage  |
|-------------|--|
| 5 to 20     | The number of seconds Communication Manager waits to receive confirmation after sending calling party number and dialed number information on outgoing Russian MFP trunks. |

**Feature-related system parameters: page 18****INTERCEPT TREATMENT PARAMETERS****Intercept Treatment on Failed Trunk Transfers**

| Valid Entry | Usage  |
|-------------|--|
| y           | Provides intercept treatment to calls failing trunk transfers. |
| n           | Drops calls failing trunk transfers.                           |

**Invalid Number Dialed Display**

Used to display a name in either Latin or Asian characters for an invalid number calling in. This field supports both a NAME1 and a NAME2 value. A NAME1 value directs the system to use the table of names that contains Latin characters that can be displayed. A value of NAME2 directs the system to use the UTF-8 table of names that contains non-ASCII characters suitable for Asian language names. Accepts up to 15 alphanumeric characters.

**Invalid Number Dialed Intercept Treatment**

The type of intercept treatment the end-user hears after dialing an invalid number.

| Valid Entry  | Usage  |
|--------------|--|
| announcement | Provides a recorded announcement when the end-user dials an invalid number. You select and record the message. |

| Valid Entry | Usage   |
|-------------|---|
|             | Requires entering the extension number for the announcement.                            |
| tone        | Provides intercept tone when the end-user dials an invalid number. This is the default. |

**Restricted Number Dialed Display**

The string of alphanumeric characters assigned for calls that are denied because of COS, COR, or FRL restrictions. This field supports both a NAME1 and a NAME2 value. A NAME1 value directs the system to use the table of names that contains Latin characters. A value of NAME2 directs the system to use the UTF-8 table of names that contains non-ASCII characters suitable for Asian language names. Accepts up to 15 alphanumeric characters.

**Restricted Number Dialed Intercept Treatment**

The type of intercept treatment the caller hears after dialing a number restricted from them due to COS, COR, or FRL restrictions.

| Valid Entry  | Usage   |
|--------------|---|
| tone         | Provides intercept tone. This is the default.   |
| announcement | Provides a recorded announcement. You select and record the message. Requires entering the extension number for the announcement. |

**WHISPER PAGE**

**Whisper Page Tone Given To**

Determines who should hear a Whisper Page.

| Valid Entry | Usage  |
|-------------|--|
| all         | All parties hear the whisper page.                                       |
| paged       | The whisper page feature sends a beep to the paging and the paged party. |

**6400/8400/2420J LINE APPEARANCE LED SETTINGS**

 **Warning:**

The following fields change only the LED operation for 84xx and 64xx model telephones. When the LED operation is changed using any of these fields, then IP Agent and IP Softphone using a station type of 84xx or 64xx does not work. For station types other than 84xx or 64xx, a change to the LEDs using these fields does not affect either IP Agent or IP Softphone.

 **Note:**

The system generates a warning if the default values of the LED Settings field are changed. The warning message states  
 WARNING: Avaya Softphone will not operate correctly if this value is changed . This warning message displays for Avaya Communication Manager 3.1 or higher.

### Display Information With Bridged Call

Controls whether or not name and number for a bridged call are displayed on the telephone of the called party. This field does *not* control the content of the display.

#### Idle

 **Note:**

This field applies only to 8400 and 6400 series telephones. The 2400 series phone uses icons rather than LEDs.

| Valid Entry   | Usage  |
|---------------|--|
| steady<br>off | The LED flash rate for an idle station. Default is steady.<br>The correct value for the Japanese environment is off. |

### Other Stations When Call Is Active

Controls a DCP bridged appearance LED for those non-active parties with a bridged appearance that is active.

 **Note:**

This field applies only to 8400 and 6400 series telephones. The 2400 series phone uses icons rather than LEDs.

| Valid Entry  | Usage   |
|--------------|---|
| green<br>red | The LED color. Default is green.<br>Red is the correct value in the Japanese environment. |

### Other Stations When Call Is Put On-Hold

Controls LED options for the other stations with a Bridged Appearance that have been placed on hold, but the user of this station has not pushed the hold button.

 **Note:**

This field is for a DCP bridged appearance LED color and flash rate when a call on a bridged appearance is put on hold by another party on the DCP bridged appearance. Additionally, this field only applies to 8400 and 6400 series telephones. The 2400 series phone uses icons rather than LEDs. Correct operation in the Japanese environment requires the administrator to select the values red and flash for this field.

| Valid Entry   | Usage  |
|---|--|
| green<br>red  | The color of the LED. Default is green.      |
| off<br>wink<br>inverse-wink<br>flash<br>flutter<br>broken-flutter<br>steady | The flash rate for the LED. Default is wink. |

## Managing inventory

### Pickup on Transfer

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows bridged appearances of a station to pick up a call on hold because of a transfer.                       |
| n           | Bridged appearances of another station are <i>not</i> allowed to pick up a call on hold because of a transfer. |

### Ringling

Controls the LED color and flash rate while a call is ringing.

 **Note:**

This field only applies to 8400 and 6400 series telephones. The 2400 series phone uses icons rather than LEDs. Correct operation in the Japanese environment requires the administrator to select the values red and wink for this field.

| Valid Entry   | Usage                             |
|---|-----------------------------------|
| green<br>red  | The LED color. Default is green.  |
| off<br>wink<br>inverse-wink<br>flash<br>flutter<br>broken-flutter<br>steady | The flash rate. Default is flash. |

### Station Putting Call On-Hold

Controls the LED color and flash rate on the 8400 and 6400 series telephones for a call held on a Primary or Bridged Appearance.

| Valid Entry   | Usage   |
|---|---|
| green<br>red  | The color of the LED. The LED for the color not selected is turned OFF. Default is green. |
| off<br>wink<br>inverse-wink<br>flash<br>flutter<br>broken-flutter<br>steady | The flash rate for a call on hold. Default is wink.                                       |

### Station When Call is Active

Controls the red LED on the 8400 and 6400 series telephones, for a station active on a call.

| Valid Entry | Usage  |
|-------------|--|
| steady      | Communication Manager controls the red LED. This is the default. |
| off         | The red LED is always OFF.                                       |

## Feature-related system parameters: page 19

### IP PARAMETERS

#### Direct IP-IP Audio Connections

Allows or denies direct audio connections between IP endpoints that saves on bandwidth resources and improves sound quality of voice over IP transmissions.

#### IP Audio Hairpinning

If enabled, allows IP endpoints connected through the IP circuit pack in the server in IP format to bypass the Communication Manager TDM bus.

### CALL PICKUP

A pickup group is a collection, or list, of individual extensions used to connect each extension to one another.

#### Audible Notification

Enables or disables audible notification of Call Pickup calls.

#### Call Pickup Alerting

Enables or disables Call Pickup Alerting on a system-wide basis. Call Pickup Alerting provides pickup group members with a visual indication on the **Call Pickup** status lamp for calls eligible to be answered using Call Pickup.

#### Call Pickup on Intercom Calls

Allows or disallows system-wide users the ability to pickup an intercom call using the Call Pickup or Directed Call Pickup features.

#### Directed Call Pickup

Enables or disables the use of Directed Call Pickup, where users are allowed to specify what ringing telephone they want to answer.

#### Enhanced Call Pickup Alerting

Enables or disables Enhanced Call Pickup Alerting that provides enhanced Call Pickup Alerting features to display dynamic calling and called party information for all members of the pickup group.

#### Enhanced Call Pickup Delay Timer (sec.)

| Valid Entry | Usage                |
|-------------|----------------------|
| 1 to 15     | The time in seconds. |

#### Enhanced Call Pickup Delay Timer (sec.) Display

| Valid Entry | Usage  |
|-------------|--|
| 1 to 15     | The time in seconds the <b>Call Pickup</b> button flashes. |

### Extended Group Call Pickup

Selects how call pickup groups can answer calls directed to another call pickup group.

| Valid Entry | Usage   |
|-------------|---|
| flexible    | A one-to- <i>n</i> pickup group-to-extended pickup group mapping. |
| simple      | A one-to-one pickup group-to-extended pickup group mapping.       |
| none        | Extended group call pickup is not supported.                      |

### Maximum Number of Digits for Directed Group Call Pickup

| Valid Entry | Usage   |
|-------------|---|
| 1 to 4      | The maximum number of digits accepted for the pickup group number. The pickup group number is complete when it is followed by a # symbol. Default is 4. |

#### Related topics:

[Directed Call Pickup Access Code](#) on page 562

### PIN Checking for Private Calls

Enables or disables the PIN Checking for Private Calls feature that restricts users from making internal or external private calls by forcing them to enter a PIN code after dialing a PIN Feature Access Code (FAC).

### Temporary Bridged Appearance on Call Pickup

Allows or disallows a system-wide temporary bridged appearance for calls answered with the Call Pickup or Directed Call Pickup features.

## Firmware Station Download

This screen downloads firmware to multiple stations of the same telephone type, either 2420 or 2410 DCP telephones. Downloads firmware to as many as 1000 stations per download schedule. You can schedule a specific time for the download, or you can administer the download to run immediately.

Example command: `change firmware station-download`

### Beginning Station

The first extension number in the range of telephones used to download the firmware. Up to 1000 stations can be included in a scheduled download. Accepts up to eight digits.

### Continue Daily Until Completed

Enables or disables the execution of a firmware download each day at the scheduled time until all specified telephones have received the firmware.

## Download Set Type

| Valid Entry          | Usage   |
|----------------------|---|
| 2410 DCP<br>2420 DCP | The set type of DCP telephones to which firmware is to be downloaded. |

## Ending Station

The last extension number in the range of telephones used to download firmware. Up to 1000 stations can be included in a scheduled download. Accepts up to eight digits.

## Schedule Download

Enables or disables a request to schedule a time for a firmware download to multiple DCP stations.

## Source File

The name of the file used to retrieve the firmware download. Accepts up to 32 alphanumeric characters.

### Related topics:

[File to Retrieve](#) on page 970

## Start Date/Time

Available only if **Schedule Download** is enabled.

| Valid Entry             | Usage  |
|-------------------------|--|
| mm, dd, yyyy;<br>hh, mm | The month, day, year, and time for the firmware download to begin. |

### Related topics:

[Schedule Download](#) on page 633

## Stop Date/Time

Available only if **Schedule Download** is enabled.

| Valid Entry             | Usage  |
|-------------------------|--|
| mm, dd, yyyy;<br>hh, mm | The month, day, year, and time for the firmware download to end. |

### Related topics:

[Schedule Download](#) on page 633

## Group Paging Using Speakerphone

Assigns digital speakerphones to a paging group. Users can page all the telephones in the group simultaneously by dialing the group extension.

Example command: `change group-page n`, where *n* is the assigned group number.

**Alert**

| Value | Usage   |
|-------|---|
| y     | Enables to receive an alert at the station of each member of the group.                           |
| n     | Disables to receive an alert at the station of each member of the group. This is a default value. |

**ASAI**

| Value | Usage  |
|-------|--|
| y     | Enables ASAI events for paging groups. Enabling this functionality creates large spikes in the messaging traffic to the application. |
| n     | ASAI events are not forwarded to the application for any call that has a paging group as parties on the call.                        |

**COR**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 995    | A class of restriction (COR). To page the group, users' class of restriction must give them calling permission for the group's class of restriction. |

**Ext**

Assigns a telephone extension to the group.

**Group Extension**

The extension users dial to page the members of this group.

**Group Name**

A name for the group that is informative to users. The name appears on callers' telephone displays when they page the group. Accepts up to 27 alphanumeric characters.

 **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Group Number**

The identifying number the server running Communication Manager assigns to the group when it is created.

**Group Timeout (secs)**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 600    | Administer a timeout in seconds for the group page. After timeout, the paging party will be disconnected. The default value is 0 for no timeout. |

**Name**

The name assigned to each extension in the group.

 **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**TN**

The tenant number for this paging group. Allows group paging to be partitioned by tenant.

**Holiday Table**

Defines individual holidays or holiday ranges.

Example command: `change holiday-table n`, where *n* is the holiday table number.

**Description**

A phrase that describes the holiday. Accepts up to 27 characters.

**End Day**

| Valid Entry | Usage                          |
|-------------|--------------------------------|
| 1 to 31     | The ending day of the holiday. |

**End Hour**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 23     | The ending hour of the holiday using a 24-hour clock. |

**End Min**

| Valid Entry | Usage                             |
|-------------|-----------------------------------|
| 0 to 59     | The ending minute of the holiday. |

**End Month**

| Valid Entry | Usage                            |
|-------------|----------------------------------|
| 1 to 12     | The ending month of the holiday. |

**Name**

The name of the holiday table. Accepts up to 27 characters.

**Number**

| Valid Entry | Usage                     |
|-------------|---------------------------|
| 1 to 10     | The holiday table number. |

### Start Day

| Valid Entry | Usage                            |
|-------------|----------------------------------|
| 1 to 31     | The starting day of the holiday. |

### Start Hour

| Valid Entry | Usage   |
|-------------|---|
| 0 to 23     | The starting hour of the holiday using a 24-hour clock. |

### Start Min

| Valid Entry | Usage                               |
|-------------|-------------------------------------|
| 0 to 59     | The starting minute of the holiday. |

### Start Month

| Valid Entry | Usage                              |
|-------------|------------------------------------|
| 1 to 12     | The starting month of the holiday. |

## Hospitality

Implements the system parameters associated with the hospitality features. Available only if Hospitality features are enabled for the system.

Example command: `change system-parameters hospitality`

### Related topics:

[Hospitality \(Basic\)](#) on page 946

[Hospitality \(G3V3 Enhancements\)](#) on page 946

### Hospitality: page 1

#### ***Client Room Coverage Path Configuration***

Indicates the server and the Property Management System (PMS) exchange coverage path information for guest stations.

| Valid Entry | Usage  |
|-------------|--|
| act-nopms   | The message is acknowledged ( <code>MESSAGE ACK</code> ), but no action is taken.  |
| act-pms     | The server and PMS exchange and accept coverage path information. This field does not apply to normal PMS Protocol mode. |

#### ***Controlled Restrictions Configuration***

Indicates whether controlled restriction information is exchanged between the server and the PMS.

| Valid Entry | Usage  |
|-------------|--|
| act-nopms   | The message is acknowledged (MESSAGE ACK), but no action is taken.             |
| act-pms     | The server and the PMS exchange and accept controlled restriction information. |

### **Default Coverage Path for Client Rooms**

Applies only to stations with a client room class of service in the occupied mode. This field is used for transparent or ASCII mode. The value in this field is also used during a translation save as the coverage path for each station with client room class of service.

| Valid Entry        | Usage  |
|--------------------|--|
| 1 to 9999<br>blank | The coverage path assigned when the server receives a check-out message for a valid extension or a new check-in. |

### **Forward PMS Message to INTUITY Lodging**

This field is used only in ASCII mode.

| Valid Entry | Usage  |
|-------------|--|
| y           | PMS-to-INTUITY messages are sent through the server.                           |
| n           | PMS-to-INTUITY messages are sent directly to the Avaya INTUITY Lodging system. |

### **Housekeeper Information Configuration**

Indicates whether housekeeper information is exchanged between the server and the PMS.

| Valid Entry | Usage  |
|-------------|--|
| act-nopms   | The message is acknowledged (MESSAGE ACK), but no action is taken. |
| act-pms     | The server and PMS exchange and accept housekeeper information.    |

### **Journal/Schedule Endpoint**

| Valid Entry                        | Usage  |
|------------------------------------|--|
| <i>Valid data extension number</i> | A valid data extension number that is assigned to the data module connected to the Journal/Schedule printer. Cannot be a VDN extension. This extension can be the same as the PMS/ Log printer and both sets of reports can be printed on the same printer. This extension is dialed by the server to send journal information or schedule reports to the printer. |
| PMS_LOG                            | The printer is connected over a TCP/IP link, and this link is administered with a <b>PMS_LOG</b> service type for IP Services.   |
| PMS_JOURNAL                        | The printer is connected over a TCP/IP link, and this link is administered with a <b>PMS_JOURNAL</b> service type for IP Services.   |

**Related topics:**

[Service Type](#) on page 717

**Message Waiting Configuration**

Indicates whether message waiting notification requests and changes are being exchanged between the server and the PMS.

| Valid Entry | Usage  |
|-------------|--|
| act-nopms   | The message is acknowledged (MESSAGE ACK), but no action is taken.                                 |
| act-pms     | Message waiting is active on the server and information between the PMS and server is transmitted. |

**Number of Housekeeper ID Digits**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 6      | The number of digits that the housekeeper must dial for identification. |

**PMS Log Endpoint**

| Valid Entry            | Usage   |
|------------------------|---|
| <i>Valid extension</i> | The data extension number the server dials to access PMS. Cannot be a VDN extension.                      |
| PMS                    | The PMS is connected over a TCP/IP link. This link is administered with PMS service type for IP Services. |

**Related topics:**

[Service Type](#) on page 717

**PMS LINK PARAMETERS**

ASCII mode

Enables or disables ASCII-only mode used for the PMS message set. Available only with a transparent PMS protocol mode.

PMS Link Maximum Retransmission Requests

| Valid Entry | Usage  |
|-------------|--|
| 1 to 5      | The number of times that the server allows the PMS to request acknowledgment for a message that it sent. |

PMS Link Maximum Retransmissions

| Valid Entry | Usage   |
|-------------|---|
| 1 to 5      | The number of times that the server retransmits a message to the PMS in response to a negative acknowledgment, or sends an inquiry for acknowledgment from the PMS before giving up on the message. |

**Milliseconds Before PMS Link Acknowledgment Timeout**

Regulates how quickly the system responds to a message from the PMS, also known as “pace timing”. This value is also used as the inquiry message (ENQ) time-out value. Should be kept as short as possible.

| Valid Entry | Usage  |
|-------------|--|
| 100 to 1500 | The time in milliseconds the system waits for an acknowledgment from the PMS indicating it correctly received a message. |

**PMS Endpoint**

| Valid Entry            | Usage   |
|------------------------|---|
| <i>Valid extension</i> | The data extension number the server dials to access PMS. Cannot be a VDN extension.                      |
| PMS                    | The PMS is connected over a TCP/IP link. This link is administered with PMS service type for IP Services. |

**Related topics:**

[Service Type](#) on page 718

**PMS Protocol Mode**

| Valid Entry           | Usage   |
|-----------------------|---|
| normal<br>transparent | Indicates the message protocol mode used between the server and PMS. Coordinate this option with your PMS vendor. |

**Seconds Before PMS Link Idle Timeout**

| Valid Entry | Usage  |
|-------------|--|
| 5 to 20     | The idle time in seconds that the server waits for an acknowledgment from the PMS before the server enters link failure mode from the PMS transmission link. |

**Take Down Link for Lost Messages**

Enables or disables taking down the PMS link if messages are getting lost. The PMS error log should be monitored if disabled.

**Hospitality: page 2*****Announcement Ports***

Indicates the equipment location of two ports on the voice synthesizer circuit pack. Available only with a voice-synthesis announcement type.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 64     | First and second characters are the cabinet number. |
| A to E      | Third character is the carrier.                     |

| Valid Entry                              | Usage  |
|--|--|
| 0 to 20                                  | Fourth and fifth character are the slot number.    |
| 01 to 04 (Analog TIE trunks)<br>01 to 31 | Six and seventh characters are the circuit number. |
| 1 to 250                                 | Gateway  |
| V1 to V9                                 | Module   |
| 01 to 31                                 | Circuit  |

**Related topics:**

[Announcement Type](#) on page 640

**Announcement Type**

Indicates the type of automatic wake up announcement the hotel guest receives.

| Valid Entry     | Usage  |
|-----------------|--|
| external        | Applicable when using an announcement adjunct. Requires entry of the circuit connection to the external announcement equipment.  |
| integrated      | Applicable when using the TN750B or TN750C announcement circuit pack. Requires entry of an extension for the integrated announcement.  |
| mult-integ      | Multi-integrated is applicable when using the TN750B or TN750C announcement circuit pack. Allows the Automatic Wakeup feature to use integrated announcement circuit packs to play any one of multiple announcements to different extensions during a wake up call. Requires entry of an announcement extension. |
| voice-synthesis | A voice synthesis message is heard during the wake up announcement. Requires entry of port location information for the voice synthesizer circuit pack.  |
| music-on-hold   | Uses the Music-on-Hold feature to provide the wake up announcement.  |
| silence         | Silence is heard during the wake up announcement.  |

**Related topics:**

[Announcement Ports](#) on page 639

[Auxiliary Board for Announcement](#) on page 641

[Default Announcement Extension](#) on page 641

[Integrated Announcement Extension](#) on page 642

**Automatic Selection of DID Numbers**

Enables or disables the Automatic Selection of DID Numbers for Guest Rooms feature. This feature assigns a two- to five-digit extension from a predetermined list of numbers to a hotel room telephone number that is not associated with the room number.

**Auxiliary Board for Announcement**

The equipment location of an auxiliary trunk circuit that connects to the external announcement equipment. Available only for an external announcement type.

| Valid Entry                              | Usage   |
|--|---|
| 1 to 64                                  | First and second characters are the cabinet number. |
| A to E                                   | Third character is the carrier.                     |
| 0 to 20                                  | Fourth and fifth character are the slot number.     |
| 01 to 04 (Analog TIE trunks)<br>01 to 31 | Six and seventh characters are the circuit number.  |
| 1 to 250                                 | Gateway   |
| V1 to V9                                 | Module  |
| 01 to 31                                 | Circuit   |

**Related topics:**

[Announcement Type](#) on page 640

[Default Announcement Extension](#) on page 641

[Integrated Announcement Extension](#) on page 642

**Custom Selection of VIP DID Numbers**

Allows or disallows the selection of a DID number assigned to a room when a guest checks in. Available only if **Automatic Selection of DID Numbers** is enabled.

**Related topics:**

[Automatic Selection of DID Numbers](#) on page 640

**Daily Wakeup**

Allows or disallows each extension permission to request daily wake up calls.

**Default Announcement Extension**

The default wake up announcement extension when using the integrated announcement circuit pack.

Available only with a multi-integrated announcement type.

**Related topics:**

[Announcement Type](#) on page 640

[Auxiliary Board for Announcement](#) on page 641

[Integrated Announcement Extension](#) on page 642

**Digit to Insert/Delete**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9      | <p>The current PMS message set uses the extension number as the room identifier. In many customer configurations, the leading digit of the extension number is dropped to screen the room number. To accommodate PMS devices that are based on room number and not extension, this leading digit can be deleted on messages from Avaya Communication Manager to the PMS, and then inserted back on messages from the PMS to Communication Manager.</p> <p> <b>Note:</b><br/>The PMS interface supports three-, four-, or five-digit extensions, but prefixed extensions do not send the entire number across the interface. Only the assigned extension number is sent. Therefore, do not use prefixed extensions for numbers that are also going to use the Digit to Insert/Delete function.</p> |

**Display Room Information in Call Display**

Indicates the type of guest room information displayed on telephone displays.

| Valid Entry | Usage   |
|-------------|---|
| y           | Telephones display the name and room number. The extension number and room number are not always the same number. |
| n           | Telephones display the name and extension number.   |

**Dual Wakeup**

Allows or disallows each extension permission to request two wake up calls within one 24-hour period.

**Extension to Receive Failed Wakeup LWC Messages**

An extension that indicates where unsuccessful wake up LWC messages are stored. This is usually administered to an unassigned extension or to the attendant (attd). This extension cannot be a VDN extension. In addition, a LWC lamp for that extension is usually assigned to the attendant console as an indication of failed wake up calls.

**Integrated Announcement Extension**

The wake up announcement extension when using the integrated announcement circuit pack.  
Available only for integrated announcement types.

**Related topics:**

- [Announcement Type](#) on page 640
- [Auxiliary Board for Announcement](#) on page 641
- [Default Announcement Extension](#) on page 641

***Length of Time to Remain Connected to Announcement***

| Valid Entry | Usage   |
|-------------|---|
| 0 to 300    | The length of time in seconds that a hotel guest is connected to an announcement. Applies only after the guest has heard the announcement completely one time, but continues to listen. |

***Number of Digits from PMS***

The number of digits being sent from the PMS to the server to identify room numbers.

| Valid Entry | Usage                              |
|-------------|------------------------------------|
| 1 to 4      | For normal mode                    |
| 1 to 5      | For transparent or ASCII mode      |
| blank       | For mixed numbering in the server. |

***Number of Digits in PMS Coverage Path***

| Valid Entry | Usage                                      |
|-------------|--|
| 3 or 4      | The number of digits in the coverage path. |

***PMS Sends Prefix***

Enables or disables PMS Sends Prefix to Indicate if the PMS sends a prefix digit to the server as part of the room numbering plan.

***Room Activated Wakeup with Tones***

Enables or disables the activation of wake up calls with tones. Wake up calls can be activated with tones that prompt users for the time they wish to waken. This allows room activated wake up calls without the use of a speech synthesizer or a display telephone.

***Routing Extension on Unavailable Voice Synthesis***

| Valid Entry               | Usage  |
|---------------------------|--|
| <i>Assigned extension</i> | A call is placed to this extension or to the attendant if a voice synthesis port is not available during voice synthesis entry of wakeup requests. This extension cannot be a VDN extension. |
| attd                      | An attendant group code.   |

***Time of Scheduled Emergency Access Summary Report***

| Valid Entry | Usage   |
|-------------|---|
| hh:mm:am/pm | The time of day that the Emergency Access Summary Report gets printed on the Journal/ Schedule printer. |



**Caution:**

Set the report for a time other than when the system does its scheduled maintenance tests.

***Time of Scheduled Wakeup Activity Report***

| Valid Entry | Usage  |
|-------------|--|
| hh:mm:am/pm | The time of day that the Wakeup Activity Report gets printed on the Journal/ Schedule Printer. This report summarizes the wake up activity for each extension that had wake up activity for the past 24 hours. |



**Caution:**

Set the report for a time other than when the system does its scheduled maintenance tests.

***Time of Scheduled Wakeup Summary Report***

| Valid Entry | Usage   |
|-------------|---|
| hh:mm:am/pm | The time of day that the Wakeup Summary Report gets printed on the Journal/ Schedule printer. This report gives an hour-by-hour summary of the number of scheduled wake up calls and a list of extensions to which wake up calls were attempted but did not complete during the hour. |



**Caution:**

Set the report for a time other than when the system does its scheduled maintenance tests.

***VIP Wakeup***

Allows or disallows permission for each extension to request VIP wake up calls.

***VIP Wakeups Per 5 Minutes***

Available only if **VIP Wakeup** is enabled for each extension.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 50     | The number of VIP Wakeup calls allowed in a 5-minute interval. |

**Related topics:**

[VIP Wakeup](#) on page 644

**Hospitality: page 3**

***ROOM STATES***

Definition for Rooms in State 1 through 6

A definition for each room status. These definitions are only for **Attendant Room Status**.

Accepts up to 30 characters.

**Example**

State 1 could be “clean, ready to use” and state 2 could be “occupied, needs cleaning”.

## HOSPITALITY FEATURES

### Suite Check-in

Allows or disallows attendants permission to have the system automatically check-in several related extensions with one check-in command.

## Hunt Group

Hunt groups allow calls to be answered by users or agents at a predefined group of telephones or devices.

Use the Hunt Group screen to create a hunt group, identified by a hunt group number, and to assign hunt group member users by their extension numbers. This screen can also be used to implement associated features such as Automatic Call Distribution (ACD) and Hunt Group Queuing.

When a call comes into a hunt group, the system checks for the busy or idle status of extension numbers in the hunt group when answering. A Uniform Call Distribution (UCD) type hunt group selects the “most idle” extension in the group when answering a new call. A Direct Department Calling (DDC) type hunt group selects the first available extension (in the administered sequence) when answering a new call. Expert Agent Distribution (EAD), used only with Expert Agent Selection (EAS), selects the “most idle” agent or the “least occupied” agent with the highest skill level for the call’s skill.

### Note:

Vector controlled splits/skills can be called directly through the split/skill extension instead of calling a VDN mapped to a vector that terminates the call to a vector controlled split/skill. However, the calls will not receive any announcements, be forwarded, redirect to coverage, or intraflow/interflow to another hunt group.

Example command: `change hunt-group n`, where *n* is the assigned hunt group number.

### Hunt group: page 1

#### ACD

Indicates whether or not to use Automatic Call Distribution (ACD) for this hunt group. Available only if ACD is enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| y           | The hunt group functions as an ACD split/skill. Hunt groups used for voice messaging can function as ACD splits/skills.   |
| n           | The hunt group does not function as an ACD split/skill. This option should be used if this hunt group is on a remote server running Communication Manager and using voice messaging in a Distributed Communications System (DCS). |

#### Related topics:

[ACD](#) on page 950

**(Calls Warning) Extension**

Extension used by the Terminal Translation Initialization (TTI) feature to assign a port to this extension from the port itself. Once **Calls Warning Port** is assigned a valid port, then the extension is removed and considered unassigned.

This field cannot be blank.

Available only if a queue has been enabled for this hunt group, and if a port number is not administered for the calls warning and time warning ports.

**Related topics:**

[\(Calls Warning\) Port](#) on page 646

[Queue](#) on page 652

[\(Time Warning\) Port](#) on page 652

**(Calls Warning) Port**

The seven-character port number assigned to connect the optional external **Auxiliary Queue Call Warning Threshold** lamp that flashes when the number of calls in queue has exceeded the queue warning threshold (assigned in **Calls Warning Threshold**). Available only if a queue has been enabled for this hunt group.

| Valid Entry                              | Usage  |
|--|--|
| 1 to 64                                  | First and second characters are the cabinet number   |
| A to E                                   | Third character is the carrier   |
| 0 to 20                                  | Fourth and fifth character are the slot number   |
| 01 to 04 (Analog TIE trunks)<br>01 to 31 | Six and seventh characters are the circuit number<br>This port is assigned to an Analog Line circuit pack or given an x designation if an extension is used. |

**Example**

01A0612 is in cabinet 01, carrier A, slot 06, and circuit number (port) 12.

**Related topics:**

[Calls Warning Threshold](#) on page 646

[Queue](#) on page 652

**Calls Warning Threshold**

Available only if a queue has been enabled for this hunt group.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 999    | The number of calls that can be queued before the system flashes the queue status (feature buttons assigned on agents telephones) and the optional <b>Auxiliary Queue Call Warning Threshold</b> lamp assigned to the split/skill. These lamps are lighted steadily when at least one call is in |

| Valid Entry | Usage   |
|-------------|---|
|             | queue and the threshold has not yet been reached. This value must be less than or equal to the queue length or left blank.<br>This field must not be left blank if <b>Calls Warning Port</b> is administered. |

**Related topics:**

[\(Calls Warning\) Port](#) on page 646

[Queue](#) on page 652

**COR**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 995    | The class of restriction (COR) number that reflects the desired restriction for the hunt group. If this is a hunt group supporting voice messaging in a Distributed Communications System (DCS), the CORs on this screen for each server running Communication Manager must be the same. |

**Coverage Path**

The coverage path for the hunt group. Available only if the hunt group is not vector controlled.

| Valid Entry | Usage                   |
|-------------|-------------------------|
| 1 to 999    | A coverage path number. |
| t1 to t999  | Time of day table.      |

**Related topics:**

[Vector](#) on page 653

**Group Extension**

An unused extension number assigned to the hunt group. This field cannot be blank.

**Group Name**

A character string that uniquely identifies the hunt group. Accepts up to 27 characters.

 **Note:**

This field is supported by Unicode language display for the 4610SW, 4620SW, 4621SW, and 4622SW telephones.

For more information on Unicode language display, see *Administering Unicode*.

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Example**

“parts dept”, “purchasing”, or “sales dept”

**Related topics:**

[Display Character Set](#) on page 938

**Group Number**

The hunt group number.

**Group Type**

The group types available depend on what is enabled for your system. The table below shows what group types are available depending on your configuration.

|  | <b>circ</b> | <b>ddc</b> | <b>ucd-mia</b> | <b>ead-mia</b> | <b>ucd-loa</b> | <b>ead-loa</b> | <b>pad</b> | <b>sim</b> |
|--|-------------|------------|----------------|----------------|----------------|----------------|------------|------------|
| ACD=n  | x           | x          |                |                |                |                |            |            |
| ACD=y, Vector=n, skill=n                     |             | x          | x              |                |                |                |            |            |
| ACD=y, Vector=y, Skill=y, LOA=n              |             |            | x              | x              |                |                |            | x          |
| ACD=y, Vector=y, Skill=y, LDA=y, Advocate=y  |             |            | x              | x              | x              | x              |            | x          |
| ACD=y, Vector=y, Skill=y, Advocate=y         |             |            | x              | x              | x              | x              |            |            |
| ACD=y, Vector=y, Skill=y, Dynamic Advocate=y |             |            | x              | x              | x              | x              | x          |            |

Each option uses a different method to select an extension or agent for a call when two or more extensions or agents are available.

| <b>Valid Entry</b> | <b>Usage</b>  |
|--------------------|---|
| circ               | Circular is used when the call should be routed in a “round-robin” order. The order in which the extensions are administered determines the order that calls are directed. The server running Communication Manager keeps track of the last extension in the hunt group to which a call was connected. The next call to the hunt group is offered to the next extension in the circular list, independent of how long that extension has been idle. Cannot be used with ACD, queues, or vectors. This option is available only in a configuration where the ACD group type is disabled. |
| ddc                | Calls are routed to the first extension or ACD agent assigned in the ACD split. Group type ddc is also known as “hot seat” distribution. Not available when the group is administered as a skill. This option is available only with the following configurations: <ul style="list-style-type: none"> <li>• ACD disabled</li> <li>• ACD, Split, Vector enabled or disabled</li> </ul>   |
| ucd-mia            | Calls route to the most-idle agent based on when the agent finished the most recent call based on agent occupancy . Can be used if the hunt group has a voice message.  |

| Valid Entry | Usage   |
|-------------|---|
|             | <p>Required when supporting the Outbound Call Management feature. The <b>Controlling Adjunct</b> type must be asai.</p> <p>This option is available only with the following configurations:</p> <ul style="list-style-type: none"> <li>• ACD, Split, Vector enabled or disabled</li> <li>• ACD, Skill, Vector enabled or disabled</li> <li>• ACD, Skill Vector enabled — Advocate or Elite</li> <li>• ACD, Skill Vector enabled — Dynamic Advocate</li> </ul>   |
| ucd-loa     | <p>Calls route to the least occupied agent based on agent occupancy . Can be used if the hunt group has a voice message.</p> <p>Required when supporting the Outbound Call Management feature. The <b>Controlling Adjunct</b> type must be asai.</p> <p>This option is available only with the following configurations:</p> <ul style="list-style-type: none"> <li>• ACD, Skill Vector enabled — Advocate or Elite</li> <li>• ACD, Skill Vector enabled — Dynamic Advocate</li> </ul>  |
| ead-mia     | <p>Calls route to the available agent with the highest skill level for the call. If two or more agents with equal skill levels are available, Communication Manager routes the call to the most-idle agent based on when the agent finished the most recent call. This allows a call to be distributed to an agent best able to handle it if multiple agents are available.</p> <p>This option is available only with the following configurations:</p> <ul style="list-style-type: none"> <li>• ACD, Skill, Vector enabled or disabled</li> <li>• ACD, Skill Vector enabled — Advocate or Elite</li> <li>• ACD, Skill Vector enabled — Dynamic Advocate</li> </ul> |
| ead-loa     | <p>Calls route to the available agent with the highest skill level for the call. If two or more agents with equal skill levels are available, Communication Manager routes the call to the least occupied agent based on agent occupancy. This allows a call to be distributed to an agent best able to handle it if multiple agents are available.</p> <p>This option is available only with the following configurations:</p> <ul style="list-style-type: none"> <li>• ACD, Skill Vector enabled — Advocate or Elite</li> <li>• ACD, Skill Vector enabled — Dynamic Advocate</li> </ul>   |
| pad         | <p>Percent allocation distribution selects an agent from a group of available agents based on a comparison of the agent's work time in the skill and the agent's target allocation for the skill.</p> <p>This option is available only in configurations where the ACD, Skill, and Vector Dynamic Advocate group types are enabled.</p>   |

| Valid Entry | Usage   |
|-------------|---|
| slm         | <ul style="list-style-type: none"> <li>Compares the current service level for each SLM-administered skill to a user-defined call service level target and identify the skills that are most in need of agent resources to meet their target service level.</li> <li>Identifies available agents and assess their overall opportunity cost, and select only those agents whose other skills have the least need for their service at the current time.</li> </ul> <p>This option is available only in configurations where the ACD, Skill, and Vector group types are enabled or disabled.</p> |

**Related topics:**

[Controlling Adjunct](#) on page 654

[ACD](#) on page 950

[Business Advocate](#) on page 951

[Expert Agent Selection \(EAS\)](#) on page 951

***Interruptible Aux Threshold***

| Valid Entry             | Usage   |
|-------------------------|---|
| service-level-target    | (Allowed values: 1-99 for % of calls, 1-999 for seconds) Specifies which threshold triggers an event to interrupt agents interruptible for a skill. The Interrupt Aux feature is triggered if the service level drops below the administered percent calls in the specified seconds. For example, if the target is 90% calls in 30 seconds, the Interruptible Aux feature is triggered if the measure drops to 89% calls in 30 seconds. |
| calls-warning-threshold | (Allowed values: 1-999) Calls Warning Threshold activates Interruptible Aux if the number of calls in the queue for a hunt group exceeds a specified number. If Calls Warning Threshold is set to 20, interruptible agents in Aux start getting interrupted as soon as the number of calls in the queue goes to 21 or beyond.   |
| time-warning-threshold  | (Allowed values: 1- 999) Time Warning Threshold activates Interruptible Aux if the oldest call has been in the queue for longer than the specified number of seconds. If Time Warning Threshold is set to 60, interruptible agents start getting interrupted as soon as the duration of the oldest call in the queue for a hunt group exceeds 60 seconds.   |
| none                    | Interruptible Aux is not active for this hunt group.  |

***ISDN Caller Disp***

This field is required for **ISDN-PRI or ISDN-BRI Trunks**.

| Valid Entry | Usage  |
|-------------|--|
| grp-name    | The hunt group name is sent to the originating user. |
| mbr-name    | The member name is sent to the originating user.     |

| Valid Entry | Usage   |
|-------------|---|
| blank       | ISDN-PRI or ISDN-BRI trunks are not enabled for the system. |

 **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Related topics:**

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

### **Local Agent Preference**

Enables or disables Local Agent Preference that routes an incoming ACD call to an idle agent by matching the location number of the incoming caller's station or trunk to the location number of an idle agent. Available only with Call Center Release 3.0 or later when Expert Agent Selection (EAS) and multiple locations are enabled for the system. Also, the hunt group must be administered as a skill hunt group.

**Related topics:**

[Skill](#) on page 660

[Multiple Locations](#) on page 948

[Call Center Release](#) on page 951

[Expert Agent Selection \(EAS\)](#) on page 951

### **MM Early Answer**

Enables or disables MM Early Answer. The system begins to answer an H.320 call and establish an audio channel before offering the conversion call to the hunt group. This starts billing for the call when the call is first put into queue. This field applies only for systems using Multimedia Call Handling.

**Related topics:**

[Multimedia Call Handling \(Basic\)](#) on page 948

### **Night Service Destination**

Not available for vector-controlled hunt group.

| Valid Entry                         | Usage  |
|-------------------------------------|--|
| <i>An assigned extension number</i> | The destination where calls to this split redirect when the split is in the night service mode. This extension can be a VDN extension. Must be a local extension for all features to work correctly. |
| attd                                | An attendant group code.   |

**Related topics:**

[Vector](#) on page 653

**Queue**

Enables or disables a queue for the hunt group.

**Queue Limit**

Available only if a queue is enabled for the hunt group.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 999    | The limit to the number of calls that will queue.  |
| unlimited   | The system dynamically allocates the queue slots from a common pool on an as-needed basis. |

**Related topics:**

[Queue](#) on page 652

**Time Warning Extension**

Extension used by the Terminal Translation Initialization (TTI) feature to assign a port to this extension from the port itself. Once **Time Warning Port** is assigned a valid port, then the extension is removed and considered unassigned.

Available only if a queue is enabled for the hunt group. Required if a port number is not administered for the time warning port.

**Related topics:**

[Queue](#) on page 652

[\(Time Warning\) Port](#) on page 652

**(Time Warning) Port**

The port number assigned to the **Auxiliary Queue Time Warning** lamp that flashes when the Time Warning Threshold has been reached by a call in queue. Available only if a queue has been enabled for the hunt group.

| Valid Entry                              | Usage  |
|--|--|
| 1 to 64                                  | First and second characters are the cabinet number   |
| A to E                                   | Third character is the carrier   |
| 0 to 20                                  | Fourth and fifth character are the slot number   |
| 01 to 04 (Analog TIE trunks)<br>01 to 31 | Six and seventh characters are the circuit number<br>This port is assigned to an Analog Line circuit pack or given an X designation if an extension is used. |

**Example**

01A0612 is in cabinet 01, carrier A, slot 06, and circuit number (port) 12.

**Related topics:**

[Queue](#) on page 652

[Time Warning Threshold](#) on page 653

### **Time Warning Threshold**

Available only if a queue is enabled for the hunt group and if a port number is not administered for the call warning and time warning ports.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 999    | The time in seconds that a call can remain in the queue before the system flashes the <b>Queue</b> status lamps (feature buttons assigned members telephones) and the <b>Auxiliary Queue Time Warning</b> lamp assigned to this split/skill. An entry of 0 provides a warning whenever a call is queued. |

#### **Related topics:**

[Queue](#) on page 652

[\(Time Warning\) Port](#) on page 652

### **TN**

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

### **Vector**

Enables or disables this hunt group as vector controlled. Available only if Basic Vectoring is enabled for the system.

#### **Related topics:**

[Vectoring \(Basic\)](#) on page 952

### **Hunt group: page 2**

This screen can vary according to values for particular fields on the previous page.

If the **ACD** is not enabled for the system, this page is omitted.

### **AAS**

Enables or disables this hunt group serving as an Auto-Available Split (AAS). AAS allows members of an ACD split or skill to be in auto-in work mode continuously. An agent in auto-in work mode becomes available for another ACD call immediately after disconnecting from an ACD call. Available only if ACD is enabled for this hunt group.

#### **Related topics:**

[ACD](#) on page 645

### **Adjunct CTI Link**

The ASAI CTI Link. This field cannot be blank. Available only if ACD is enabled for this hunt group, and the **Controlling Adjunct** is asai or adjlk.

#### **Related topics:**

[ACD](#) on page 645

[Controlling Adjunct](#) on page 654

**Controlling Adjunct**

Available only if ACD is enabled for the hunt group. ASAI Link Core Capabilities and Computer Telephony Adjunct Links must be enabled for a value other than none.

| Valid Entry | Usage  |
|-------------|--|
| none        | Members of the split/skill or hunt group are not controlled by an adjunct processor.   |
| asai        | All agent logins are controlled by an associated adjunct and logged-in agents can use only their data terminal keyboards to perform telephone functions (for example, change work state). Use if the controlling adjunct is a CONVERSANT voice system. |
| adjlk       | Computer Telephony Adjunct Links   |
| asai-ip     | ASAI links administered without hardware.  |
| adj-ip      | ASAI adjunct links administered without hardware.  |

**Related topics:**

[ACD](#) on page 645

[ASAI Link Core Capabilities](#) on page 943

[Computer Telephony Adjunct Links](#) on page 944

**Dynamic Percentage Adjustment**

Enables or disables automatic adjustments to agents' target allocations as needed to help meet the administered service level targets. Available only if ACD is enabled for the hunt group and this is a Percent Allocation Distribution (PAD) hunt group. Requires Business Advocate software.

**Related topics:**

[ACD](#) on page 645

[Group Type](#) on page 648

[Business Advocate](#) on page 951

**Dynamic Queue Position**

Enables or disables dynamic queue operation to the calls queued to the skill. Dynamic Queue Position is a Business Advocate feature that allows the queuing of calls from multiple VDNs to a single skill, while maintaining different service objectives for those VDNs. Available only if ACD, Expert Agent Selection (EAS), and Skill are enabled for the hunt group. Requires Business Advocate software.

**Related topics:**

[ACD](#) on page 645

[Skill](#) on page 660

[Business Advocate](#) on page 951

**Dynamic Threshold Adjustment**

Enables or disables automatic adjustments to overload thresholds to engage reserve agents a bit sooner or a bit later to meet the administered service levels. Available only if ACD and Service Level Supervisor are enabled for the hunt group. Requires Business Advocate software.

**Related topics:**

[ACD](#) on page 645

[Service Level Supervisor](#) on page 658

[Business Advocate](#) on page 951

**Expected Call Handling Time (sec)**

Available only if ACD is enabled for the system and if either Vectoring (Advanced Routing) or Business Advocate is enabled for the system.

| Valid Entry                  | Usage   |
|------------------------------|---|
| 1 to 9999 in increments of 1 | Establishes the number of seconds for expected call handling. This value is used to initialize Expected Wait Time and is also used by the Business Advocate Percent Allocation feature. |

**Related topics:**

[ACD](#) on page 645

[Business Advocate](#) on page 951

[Vectoring \(G3V4 Advanced Routing\)](#) on page 952

**Inflow Threshold (sec)**

Available only if ACD and a queue are enabled for the system. Not available for a vector-controlled hunt group.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 999    | The number of seconds that a call can remain in the queue before no more calls are accepted by the queue. If 0 is entered, a call is redirected to this split/skill only if there is an available agent. |

**Related topics:**

[ACD](#) on page 645

[Queue](#) on page 652

[Vector](#) on page 653

**Level 1 Threshold (sec)**

Available only if ACD and Service Level Supervisor are enabled for the hunt group.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 60     | The number of seconds for the first Expected Wait Time (EWT) threshold. |

**Example**

If there are 45 calls whose EWT exceeds 45 seconds, threshold 1 will have been exceeded.

**Related topics:**

[Service Level Supervisor](#) on page 658

**Level 2 Threshold (sec)**

Available only if ACD and Service Level Supervisor are enabled for the hunt group.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 60     | The number of seconds for the second Expected Wait Time (EWT) threshold. |

**Example**

If there are 60 calls whose EWT exceeds 60 seconds, threshold 2 will have been exceeded.

**Related topics:**

[ACD](#) on page 645

[Service Level Supervisor](#) on page 658

**Maximum Auto Reserve Agents**

Available only if ACD is enabled for the hunt group and it is a Service Level Maximizer (SLM) type hunt group.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9      | The maximum number of Auto Reserve Agents available for this skill (hunt group). Any time an auto-reserve skill is in danger of falling below its target service level percent, some of this skill's agents are auto-reserved (kept idle in other skills) so that they are available when a new call arrives for this skill. Default is 0. |

**Related topics:**

[Group Type](#) on page 648

**Measured**

Provides measurement data for the ACD split/skill to VuStats or BCMS. Available only if ACD is enabled for the hunt group and VuStats or BCMS is enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| internal    | Provides measurements made by the Call Management System that are internal to the server running Communication Manager. |
| external    | Provides measurements made by the Call Management System that are external to the server running Communication Manager. |
| both        | Provides measurements collected both internally and externally.   |
| none        | Measurement reports for this hunt group are not required.   |

**Related topics:**

[ACD](#) on page 645

[BCMS \(Basic\)](#) on page 950

[VuStats](#) on page 953

**Multiple Call Handling**

Defines whether the hunt group can have multiple call handling capabilities, and if so, what type. Available only if ACD is enabled for the hunt group and Multiple Call Handling is enabled for the system.

| Valid Entry   | Usage  |
|---------------|--|
| none          | Agents who are members of that split/skill can only receive an ACD call from that split/skill when the telephone is idle.  |
| on-request    | Agents in the Multiple Call Handling split/skill can place a non-ACD or an ACD call on hold and select an available work mode. A queued ACD split/skill or direct agent call then is routed to the agent.  |
| many-forced   | An ACD call is delivered automatically to an idle line appearance if the agent is in the Auto-In/Manual-In (MI/AI) work mode and an unrestricted line appearance is available.   |
| one-forced    | An ACD call is delivered automatically to an idle line appearance if the agent has no other ACD call on the station, is in the Auto-In/Manual-In (MI/AI) work mode, and an unrestricted line appearance is available.  |
| one-per-skill | An ACD call is delivered automatically to an idle line appearance if the agent has no other ACD call for that skill on the station, is in the Auto-In/Manual-In (MI/AI) work mode, and an unrestricted line appearance is available. Valid in an EAS environment for a skill-enabled hunt group. |

**Related topics:**

[ACD](#) on page 645

[Skill](#) on page 660

[Multiple Call Handling \(Forced\)](#) on page 951

**Priority On Intraflow**

Enables or disables having calls intraflowing from this split to a covering split and given priority over other calls waiting in the covering split queue. Available only if ACD field is enabled for the hunt group. Not available for a vector-controlled hunt group.

**Related topics:**

[ACD](#) on page 645

[Vector](#) on page 653

**Service Level Interval**

The time interval when Actual Service Level (ASL) calculations run. ASL is one of the Service Level Maximizer (SLM) algorithms used for most situations, particularly for low staff or low traffic. The interval can be set to the same interval used when specifying the target objectives for the application. Available only if Actual is administered for the SLM algorithm feature and this is an SLM-type hunt group.

| Valid Entry | Usage   |
|-------------|---|
| hourly      | ASL algorithm calculations for accepted call and total call components are set to 0 at hourly intervals.  |
| daily       | ASL algorithm calculations for accepted call and total call components are set to 0 at daily intervals. This is the default.                                  |
| weekly      | ASL algorithm calculations for accepted call and total call components are set to 0 at weekly intervals. The weekly interval starts as 00:00 hours on Sunday. |

**Related topics:**

[Service Level Maximizer Algorithm](#) on page 616

[Group Type](#) on page 648

**Service Level Supervisor**

Enables or disables Service Level Supervisor for this skill. Service Level Supervisor is a Business Advocate feature that alleviates the need to move agents from skill to skill during emergencies or unanticipated peaks in call volume. Available only if ACD is enabled for the hunt group and this is an Expert Agent Selection (EAS) skill hunt group. Requires Business Advocate software.

**Related topics:**

[ACD](#) on page 645

[Skill](#) on page 660

[Business Advocate](#) on page 951

**Service Level Target (% in sec)**

Appears when the **ACD** field and the **Measured** field is not blank, and when one or more of the following features are active:

- **BCMS/VuStats Service Level** field on the System Parameters Customer-Options screen is active and the **Measured** field is set to internal or both. The service level target in

seconds is used as the acceptable level for reporting the percentage of calls answered within the specified time. The percentage can be set to the default of 80%.

- Business Advocate on the System Parameters Customer-Options screen is active. The service level target in seconds is used for the Business Advocate Service Level Supervisor service level objective. This service level target can also be used for the dynamic percentage adjustment when the **Dynamic Threshold Adjustment** field on the Hunt Group screen is y and for the dynamic percent adjustment when the **Group Type** field on the Hunt Group screen is pad and the **Dynamic Percent Adjustment** field on the Hunt Group screen is set to y.
- **Service Level Target** field appears when the **Group Type** field on the Hunt Group screen is slm, and on the System Parameters Customer-Options screen, the Service Level Maximizer is active, and the Business Advocate customer option license is not active. In this case the setting is also used as the service level target to trigger SLM.
- **Interruptible Aux Threshold** field on the Hunt Group screen is set to service-level-target. The Interrupt Aux feature is triggered if the service level drops below the administered percent calls in the specified seconds.

| Valid Entry                    | Usage  |
|--------------------------------|--|
| 1 to 99<br>(percentage)        | The percentage component of the service level target. The default value is 80%.  |
| 1 to 9999 (time<br>in seconds) | The time component of the service level target. The default value is 20 seconds. |

#### Related topics:

[ACD](#) on page 645

[Group Type](#) on page 648

[Interruptible Aux Threshold](#) on page 650

[Dynamic Percentage Adjustment](#) on page 654

[Dynamic Threshold Adjustment](#) on page 655

[BCMS \(Basic\)](#) on page 950

[Business Advocate](#) on page 951

[Service Level Maximizer](#) on page 952

[VuStats](#) on page 953

#### Service Objective

Available only if ACD is enabled for the hunt group and this is an Expert Agent Selection (EAS) skill hunt group. Requires Business Advocate software.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 9999   | Sets a service objective for a specific skill as the number of seconds the call gets answered. The default value is 20. |

**Related topics:**

- [ACD](#) on page 645
- [Skill](#) on page 660
- [Business Advocate](#) on page 951

**Skill**

Enables or disables this hunt group as an Expert Agent Selection (EAS) skill. Available only if ACD is enabled for the hunt group and EAS is enabled for the system.

**Related topics:**

- [ACD](#) on page 645
- [Group Type](#) on page 648
- [Expert Agent Selection \(EAS\)](#) on page 951

**SLM Count Abandoned Calls**

Available only if Actual is the administered Service Level Maximizer (SLM) algorithm for the feature and this is an SLM-type hunt group.

| Valid Entry | Usage  |
|-------------|--|
| y           | Abandoned calls are included in the Actual Service Level (ASL) algorithm calculations for SLM.   |
| n           | Abandoned calls are <i>not</i> included in the ASL algorithm calculations for SLM. This option is best used when reporting for this application does not account for calls that are abandoned while in skill queues. |

**Related topics:**

- [Service Level Algorithm for SLM](#) on page 621
- [Group Type](#) on page 648

**Supervisor Extension**

The extension number of the ACD split/ skill supervisor that agents reach when using the Supervisor Assist feature. The extension number cannot be a Vector Directory Number (VDN).

Available only if ACD field is enabled for the system.

**Related topics:**

- [ACD](#) on page 645

**Timed ACW Interval (sec)**

Available only if ACD is enabled for the hunt group and Timed ACW is enabled for the system.

 **Note:**

This field can be overridden by the settings administered for a vector. Coordinate the settings when setting up delays.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 9999   | The number of seconds an agent in auto-in work mode remains in After Call Work (ACW) mode after a call drops. After this time interval expires, the agent automatically becomes available. Timed ACW cannot be administered if the hunt group is adjunct controlled, is an AUDIX Message Center, or is an auto-available split. |

**Related topics:**

[ACD](#) on page 645

[Timed ACW](#) on page 952

**VuStats Objective**

Available only if ACD is enabled for the hunt group and VuStats is enabled for the system. Also, the hunt group must be administered to collect internal or both internal and external measurement data for VuStats.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 99999  | A numerical objective. An objective is a split or skill goal for the call. This could be an agent objective such as a specific number of calls handled or an average talk time. The objective could also be a percent within the service level. The objective appears on the VuStats display and allows agents and supervisors to compare the current performance against the value of the objective for the split or skill.<br>This value applies to customized VuStats display formats. |

**Related topics:**

[ACD](#) on page 645

[Measured](#) on page 656

[VuStats](#) on page 953

**Hunt group: page 3**

This screen can vary according to values for particular fields on the previous page.

If the **ACD** is not enabled for the system, this page is omitted.

**Forced Entry of Stroke Counts or Call Work Codes**

Enables or disables the requirement that either a Stroke Count or Call Work Code must be entered for each call answered by an agent when in the Manual-In mode. Available only if ACD is enabled for the hunt group and if the hunt group does *not* have a Controlling Adjunct.

**Related topics:**

[ACD](#) on page 645

[Controlling Adjunct](#) on page 654

**Redirect on IP/OPTIM Failure to VDN**

A blank in either field redirects the call back to the hunt group. VDN extension redirects to the specified VDN.

If **Redirect on IP/OPTIM Failure to VDN** is not assigned, the call is re-queued to the same skill at a high priority. If there are no queue slots available, the caller will hear a busy signal. If all fails, the caller receives ring back until the system receives a caller disconnect.

**Related topics:**

[ACD](#) on page 645

**Redirect on No Answer (rings)**

Available only if ACD is enabled for the hunt group.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 20     | The maximum number of rings before a call redirects back to the split/skill, or to the administered VDN. |
| blank       | Deactivates Redirect on No Answer.   |

**Related topics:**

[ACD](#) on page 645

**Redirect on No Answer to VDN**

The extension number of the VDN used to redirect a Redirect On No Answer (RONA) call to a VDN instead of to the split/skill. The administered VDN must be on-premises and must be administered on the system. The VDN can specify a vector that routes to an off-premises VDN.

Direct Agent calls go to the agent's coverage path if it is administered. If not, the calls go to a VDN.

Available only if ACD is enabled for the hunt group. Requires administration of the number of rings before a call will redirect.

**Related topics:**

[ACD](#) on page 645

[Redirect on No Answer \(rings\)](#) on page 662

**Hunt Group: page 4**

The Hunt Group Message Center screen can vary according to system configuration and values populating particular fields.

**AUDIX Name**

The name of the AUDIX machine. Must be the same name as the IP Node name and administered *after* the IP Node is configured.

**Related topics:**

[IP Node Names](#) on page 700

**Calling Party Number to INTUITY AUDIX**

Enables or disables INTUITY AUDIX for the calling party number. Available only if the messaging type is audix or rem-vm.

**Related topics:**

[Message Center](#) on page 664

**First Announcement Delay (sec)**

Available only if a queue is administered for the hunt group. Not available if the hunt group is vector controlled.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 99     | The number of seconds that a call remains in queue before the associated first announcement is given the calling party. The call retains its place in the queue while the caller is listening to the recorded announcement. If the call has not been answered after the announcement, the caller hears music for first announcement only if Music-on-Hold is provided, or ringing for as long as the call remains in queue.<br>When 0 is entered, the first announcement is provided immediately to the caller. This value is set automatically to 0 if there is no queue. |
| blank       | There is no first announcement.  |

**Related topics:**

[Queue](#) on page 652

[Vector](#) on page 653

**First Announcement Extension**

The recorded announcement extension number the caller receives after being in the queue for the time interval specified in First Announcement Delay. If the call hasn't been answered after the announcement, the caller hears music only after the first announcement if Music-on-Hold is provided, or ringing for as long as it remains in the queue. If this is the forced first announcement, the caller always hears ringback after the announcement. Otherwise, the caller hears music, if provided.

Available only if ACD and a queue is administered for the hunt group. Not available if the hunt group is vector controlled.

**Note:**

When entering a Multi-Location Dial Plan shortened extension in a field designed for announcement extensions, certain administration end validations that are normally performed on announcement extensions are not done, and resultant warnings or submittal denials do not occur. The shortened extensions also do not appear in any display or list that shows announcement extensions. Extra care should be taken to administer the correct type of announcement for the application if assigning shortened extensions.

**Related topics:**

[ACD](#) on page 645

**LWC Reception**

Indicates where Leave Word Calling (LWC) messages are stored.

| Valid Entry | Usage   |
|-------------|---|
| audix       | LWC messages are stored on the voice messaging system.                          |
| none        | LWC messages are not be stored.   |
| spe         | LWC messages are stored in the system or on the switch processor element (spe). |

**Related topics:**

[AUDIX Name](#) on page 662

**Message Center**

The type of messaging adjunct for the hunt group. Only one hunt group in the system can be administered as audix, one as qsig-mwi, one as fp-mwi, one as rem-audix, and as many as six as qsig-mwi.

| Valid Entry | Usage  |
|-------------|--|
| audix       | AUDIX located on this server running Communication Manager   |
| fp-mwi      | Public network allowing AUDIX to be located on another switch. Available only if ISDN Feature Plus is administered for the system. |
| msa         | Messaging Server Adjunct   |
| msa-vm      | A voice-mail system integrated using Mode Codes or Digital Station Emulation   |
| rem-vm      | DCS feature allowing voice mail to be located on another server  |
| qsig-mwi    | QSIG network allowing voice mail to be located on another server   |
| sip-adjunct | SIP message center server  |
| none        | The hunt group does not serve as a message hunt group.   |

**Related topics:**

[ISDN Feature Plus](#) on page 947

**Message Center AUDIX Name**

The name of the Message Center AUDIX. Available only if the messaging type is audix or rem-vm.

**Related topics:**

[Message Center](#) on page 664

**Message Center MSA Name**

The name of the Message Center Messaging Server Adjunct (MSA). Available only if the messaging type is msa.

**Related topics:**

[Message Center](#) on page 664

[Message Center AUDIX Name](#) on page 664

### **Primary**

Enables or disables the specified AUDIX as the primary adjunct. Available only if the messaging type is audix or rem-audix.

#### **Related topics:**

[Message Center](#) on page 664

### **Provide Ringback**

Enables or disables ringback to the calling party until a **Connect** is received for the call to the Messaging system. Ringback is discontinued upon receipt of the **Connect** indication. Used for an SBS trunk for the QSIG MWI hunt group. A call covering to the message center provides ringback to the caller during the coverage interval. Available only if the messaging type is fp-mwi or qsig-mwi.

#### **Related topics:**

[Message Center](#) on page 664

### **Routing Digits (e.g. AAR/ARS Access Code)**

A one- to four-digit AAR (qsig-mwi) or ARS (fp-mwi) access code. This access code is prepended to the AUDIX Complete Number to define a route to the Message Center switch hunt group containing the line ports to the AUDIX. Accepts characters \* and #.

Available only if the messaging type is qsig-mwi or fp-mwi.

#### **Related topics:**

[Message Center](#) on page 664

### **Second Announcement Delay (sec)**

Available only if ACD and queues are enabled for the hunt group. Not available if the hunt group is vector controlled.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 99     | The time in seconds before the call in the queue receives a second recorded announcement or that the second announcement is repeated. If this split/skill or hunt group is a coverage point for another split/skill, this delay should not be more than 15 seconds. |
| blank       | There is no second announcement.  |

#### **Related topics:**

[ACD](#) on page 645

[Queue](#) on page 652

[Vector](#) on page 653

### **Second Announcement Extension**

The extension number assigned to a second recorded announcement. Left blank if there is no second announcement.

Available only if ACD and queues are enabled for the hunt group. Not available if the hunt group is vector controlled.

 **Note:**

When entering a Multi-Location Dial Plan shortened extension in a field designed for announcement extensions, certain administration end validations that are normally performed on announcement extensions are not done, and resultant warnings or submittal denials do not occur. The shortened extensions also do not appear in any display or list that shows announcement extensions. Extra care should be taken to administer the correct type of announcement for the application if assigning shortened extensions.

**Related topics:**

[ACD](#) on page 645

[Queue](#) on page 652

[Vector](#) on page 653

### **Second Announcement Recurring**

Allows or disallows repeating the second announcement. Available only if ACD and queues are enabled for the hunt group. Not available if the hunt group is vector controlled.

**Related topics:**

[ACD](#) on page 645

[Queue](#) on page 652

[Vector](#) on page 653

### **Send Reroute Request**

Allows or disallows rerouting getting invoked when a call covers through a qsig-mwi hunt group. Available only if the messaging type is qsig-mwi and Supplementary Services with Rerouting is enabled for the system.

**Related topics:**

[Message Center](#) on page 664

[Supplementary Services with Rerouting](#) on page 955

### **TSC per MWI Interrogation**

Controls Temporary Signaling Connections (TSCs) used for message waiting interrogations for users that are “local” to the system in which the hunt group is administered. Available only if the messaging type is qsig-mwi.

| Valid Entry | Usage   |
|-------------|---|
| y           | Communication Manager brings the TSC up, executes the Interrogate operation, and then tears the TSC down. |

| Valid Entry | Usage  |
|-------------|--|
| n           | Communication Manager uses the existing TSC sending FACILITY messages to request MWI status if the TSC is already set up, or sets up a TSC. When the interrogation operation is complete, leaves the TSC up, subject to the existing timer. This is the default. |

**Related topics:**

[Message Center](#) on page 664

**Voice Mail Extension**

The UDP extension of the voice-mail hunt group on the host server running Communication Manager.

Available only if the messaging type is rem-vm.

**Related topics:**

[Message Center](#) on page 664

**Voice Mail Handle**

The SIP Enablement Services (SES) handle that can receive voice mail. Can be left blank if a Voice Mail Number has been assigned.

**Voice Mail Number**

The 1- to 17-digit voice mail dial-up number. The qsig-mwi selection shows the complete number of the AUDIX hunt group on the Message Center server for QSIG MWI. The fp-mwi selection shows the public network number of the AUDIX hunt group on the Message Center server.

Available only if Basic Call Setup and Basic Supplementary Services are enabled for the system, and the messaging type is qsig-mwi or fp-mwi.

**Related topics:**

[Message Center](#) on page 664

[Basic Call Setup](#) on page 954

[Basic Supplementary Services](#) on page 954

**Hunt Group: page 5 through X****Administered Members (min/max)**

The minimum and maximum member number administered for this hunt group. Available for all member pages.

**At End of Member List**

Displays the current page as also the last page.

**Group Extension**

The extension of the hunt group.

**Group Number**

Displays the number of the hunt group.

**Group Type**

Displays the type of hunt group.

**Member Range Allowed**

The range of allowed members. These values vary depending on the system or configuration.

**More Members Exist**

Statement that there are more members and more pages than currently displayed.

**Total Administered Members**

The total number of members administered for the hunt group.

**GROUP MEMBER ASSIGNMENTS**

Ext

The assigned station or attendant console extension. This extension cannot be a Vector Directory Number (VDN). The data module cannot be a member of an ACD split/skill. Administers the assigned station or attendant console extension only if the controlling adjunct is administered as none. Displays the assigned station or attendant console extension if the controlling adjunct is administered as asai.



**Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Related topics:**

[Controlling Adjunct](#) on page 654

Name

The name assigned to the extension number when it is administered in the system.

**Related topics:**

[Ext](#) on page 668

**Incoming Call Handling Treatment**

Specifies unique call treatment for different incoming calls on any ISDN trunk group. This screen is available only if digit handling is administered as overlap on the “in” side, and the direction is outgoing.

**Incoming Call Handling Treatment Table** entries with a predefined service or feature always appear before entries with a user-defined service or feature. To control the order in which certain entries appear, user-defined services or features must be used for those entries.

User-defined entries are always listed in the reverse order compared to the way they appear on the Network Facilities screen. Thus, given two user-defined services or features ABC and XYZ, you can force XYZ to appear before ABC in an **Incoming Call Handling Treatment Table** by putting XYZ after ABC on the Network Facilities screen.

 **Note:**

DCS features that use the **remote-tgs** button (on the remote server/switch) do not work when the local trunk group deletes or inserts digits on the incoming call. These buttons try to dial a local TAC. Adding or deleting digits defeats this operation and renders the remote feature inoperable. If digit manipulation is needed, use it on the outgoing side, based on the routing pattern.

Example command: `change inc-call-handling-trmt trunk-group n`, where *n* is the assigned ISDN or SIP trunk group.

### Called Len

| Valid Entry | Usage   |
|-------------|---|
| 0 to 21     | The number of digits received for an incoming call. Zero is used when the Public Switched Telephone Network (PSTN) provider does not provide any “Number Digits” within the received <b>Called Party IE</b> , such as in Japan. |
| blank       | When <b>Called Number</b> has also been set to blank, so that any length of digits associated with the <b>Called Party IE</b> of the Incoming SETUP message matches this field.   |

### Called Number

| Valid Entry | Usage  |
|-------------|--|
| 1 to 16     | The number of leading digits received for an incoming call.  |
| blank       | Used as a “wildcard”, so that any number associated with the specified service or feature can match in this field. |

### Del

| Valid Entry      | Usage  |
|------------------|--|
| 1 to 21<br>blank | The number of leading digits to be deleted from the incoming <b>Called Party Number</b> . Calls of a particular type can be administered to be routed to a single destination by deleting all incoming digits and then administering the <b>Insert</b> field with the desired extension. |

### Insert

| Valid Entry       | Usage   |
|-------------------|---|
| 1 to 16<br>*<br># | The number of digits prepended to the front of the remaining digits after any optional digit deletions have been performed. The resultant number formed from digit deletion and insertion is used to route the call, provided night service is not in effect. |

**Per Call CPN/BN**

Specifies when and how to request **Calling Party Number** (CPN) or **Billing Number** (BN) for calls of this type. Available only with ISDN trunk groups.

| Valid Entry | Usage   |
|-------------|---|
| cpn-only    | Calling party number only   |
| bn-only     | Billing number only   |
| bn-pref     | Prefers billing number, but accepts calling party number  |
| cpn-pref    | Prefers calling party number, but accepts billing number  |
| none        | Communication Manager will not request either CPN or BN for any incoming calls of this type.  |
| blank       | Leave blank when connected to another media server or switch, or when connected to a public network outside North America. Within North America, leave blank when connected to a public network that does not permit customer equipment to request CPN or BN for individual incoming calls. The AT&T Switched Network offers this service under the titles “CPN/BN to Terminating End on a Per-Call Basis” and “ANI (BN) on Request”. |

 **Note:**

A 4-second delay occurs in terminating the call to the far-end station if the connecting server or switch does not respond to the request.

**Night Serv**

Available only for ISDN trunk groups.

| Valid Entry  | Usage  |
|--|--|
| <i>Assigned extension</i><br><i>Attendant group access code</i><br>attd<br>blank | Specifies a night service extension per Service/Feature. A Vector Directory Number (VDN) is acceptable. This entry is overridden by the night service administered for an individual trunk or the trunk group. |

**Related topics:**

[Night](#) on page 758

[Night Service](#) on page 986

**Service/Feature**

Displays the number that corresponds to the server type administered for the trunk group or network facility. Administration is required for a call-by-call service type.

| Valid Entry  | Usage  |
|--|--|
| Valid pre-defined Service/ Feature values for cbc trunk groups | These values are administered for Network Facilities.  |
| User-defined facility type administered for the service type   | <ul style="list-style-type: none"> <li>• 0 = feature</li> <li>• 1 = servoce</li> <li>• 2 = incoming</li> <li>• 3 = outgoing</li> </ul> |

**Related topics:**

[Network Facilities](#) on page 812

[Facility Type](#) on page 812

## Integrated Announcement Boards

Moves integrated announcement boards that have been previously administered on the Announcements/Audio Sources screen to a new board location. Displays a list of all administered integrated announcement circuit packs.

Example command: `display integrated-annc-boards`

### Board Location

The physical location of the integrated announcement circuit pack (UUCSS).

### Checksum ID

Applies to TN750 only; not applicable to VAL.

### Last Board Location Saved

Displays last board location saved. Applies to TN750 only; not applicable to VAL.

### Number of Recordings

The number of non-zero-length announcement recordings or files on the circuit pack.

### Rate

The announcement's compression rate.

### Sfx

The circuit pack suffix letters.

### Time Remaining

The amount of recording time in seconds remaining on the circuit pack at the 64Kb rate.

## Integrated Announcement Translations

Changes board locations currently administered on the Announcements/ Audio Sources screen to a new board location.

Example command: `change integ-annc-brd-loc`

### Change all board location translations from board

| Valid Entry  | Usage   |
|--|---|
| board<br>cabinet 1 to 3<br>carrier A to E<br>slot 1 to 20<br>or gateway 1 to 10<br>module V1 to V9 | The VAL board that is currently administered. |

### to board

| Valid Entry  | Usage  |
|--|--|
| board<br>cabinet 1 to 3<br>carrier A to E<br>slot 1 to 20<br>or gateway 1 to 10<br>module V1 to V9 | The VAL board to which you want to move announcement translations. |

## Intercom Group

Assigns extensions to intercom groups.

Example command: `change intercom-group n`, where *n* is the assigned intercom group number.

### DC

Assigns a dial code to an extension. Accepts up to two digits. The dial code is the code users must dial to make intercom calls to the corresponding extension. The number of digits entered must exactly match the number administered for the length of the dial code. This field cannot be blank.

#### Example

If the length of the dial code is set to 2, type 1 as 01 in the **DC** field.

**Related topics:**

[Length of Dial Code](#) on page 673

**Ext**

Assigns an extension to the group. A Vector Directory Number (VDN) cannot be used as an extension.

**Group Number**

The group ID number.

**Length of Dial Code**

Sets the number of digits that users must dial to access an extension in the group.

| Valid Entry | Usage                      |
|-------------|----------------------------|
| 1           | For nine or fewer members. |
| 2           | For 10 or more members.    |

**Name**

The name associated with the extension that has been administered to join the group.

**Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Related topics:**

[Name](#) on page 898

## Inter-Exchange Carrier (IXC) Codes

Identifies the IXC in the Call Detail Recording (CDR).

Example command: `change ixc-codes`

**Inter-Exchange Carrier (IXC) Codes: page 1*****IXC Access Number***

The digits dialed or inserted by AAR/ARS into the outpulsed digit string to access the interexchange carrier. No duplicate access numbers are allowed in the table. Accepts from 2 to 11 digits and the \* character.

***IXC Name***

A description that identifies the IXC. Accepts up to 15 characters.

**Inter-Exchange Carrier (IXC) Codes: page 2*****IXC Code Format***

A one- to four-digit IXC code format. Includes \*, x, X, xxxx (for line 1), and xxx (for line 2).

### **IXC Prefix**

A one- to three-digit prefix. Includes \*, 101 (for line 1) and 10 (for line 2).

## **Intra-Switch CDR**

Administers extensions for which Intra-Switch Call Detail Recording (CDR) is enabled.



**Note:**

Attendants are not allowed to be optioned for the Intra-Switch CDR feature.

Example command: `change intra-switch-cdr n`, where *n* is the assigned extension number.

### **Assigned Members**

The number of extensions currently administered for Intra-switch CDR.

### **Extension**

The local extensions used to track with Intra-Switch CDR. The number of tracked extensions can vary by system.

## **IP Address Mapping**

Defines feature characteristics that depend on the IP address.

Example command: `change ip-network-map`

### **Emergency Location Extension**

The emergency location extension for this station. Accepts up to seven digits. Allows the system to properly identify the location of a caller who dials a 911 emergency call from this station. An entry in this field must be of an extension type included in the dial plan, but does not have to be an extension on the local system. It can be a Uniform Dial Plan (UDP) extension. A blank entry is typically used for an IP softphone dialing in through PPP from somewhere outside the network.

For administered emergency numbers, the feature functions as follows:

- If the emergency location extension for the station is the same as the emergency location extension administered here, the feature sends the extension to the Public Safety Answering Point (PSAP).
- If the emergency location extension for the station is different from the emergency location extension administered here, the feature sends the extension administered here to the PSAP.



**Caution:**

On the ARS Digit Analysis Table, administer 911 to be call type emer or alrt in order for the E911 Emergency feature to work properly.

**Related topics:**

[Emergency Location Ext](#) on page 59

**From IP Address**

The starting IP address. IPv6 format is supported.

**Network Region**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 250    | The network region for the IP address range. For SIP, the value for this field must correlate with the configured network region for this range of addresses. This field must contain a non-blank value if the corresponding <b>From IP Address</b> contains a non-blank value. |

**Subnet Bits**

| Valid Entry      | Usage  |
|------------------|--|
| 0 to 64<br>blank | The number of bits of the subnet mask. Used in conjunction with the <b>From IP Address</b> to specify the end of the ID address range if a <b>To IP Address</b> is not administered. |

**To IP Address**

The terminating IP address. IPv6 format is supported.

**VLAN**

Sends VLAN instructions to IP endpoints such as IP telephones and softphones. This field does not send VLAN instructions to the PROCR (S8300/S87XX Servers), CLAN, and Media Processor boards.

| Valid Entry | Usage                  |
|-------------|------------------------|
| 0 to 4094   | The virtual LAN value. |
| n           | Disabled               |

**IP codec set**

Specifies the type of codec used for voice encoding and companding (compression/decompression).

The default codec is set for G711MU. The G711MU provides the highest voice quality, but it uses the most bandwidth. The G711MU default setting can be changed to one of two other codecs if the G711MU does not meet your desired voice-quality/bandwidth trade-off specification.

Example command: `change ip-codec-set n`, where *n* is the codec set number.

**IP codec set: page 1**

Defines the allowed codecs and packet sizes used between VoIP resources. Enables silence suppression on a per-codec basis and dynamically displays the packet size in milliseconds for each codec in the set, based on the number of frames administered per packet.

**Audio Codec**

Specifies the audio codec used for this codec set.

- G.711A (a-law)
- G.711MU (mu-law)
- G.722-64k
- G.722.1-24k
- G.722.1-32k
- G.723-5.3
- G.723-6.3
- G.726A-32K
- G.729
- G.729A
- G.729B
- G.729AB
- SIREN14-24k
- SIREN14-32k
- SIREN14-48k
- SIREN14-S48k
- SIREN14-S56k
- SIREN14-S64k
- SIREN14-S96k



**Important:**

Include at least two codecs for every telephone in order to avoid incompatible codecs. Use the codecs specified in the following table for the telephones shown.

| Telephone                        | Codec to use                        |
|----------------------------------|-------------------------------------|
| All Avaya IP Telephones          | G.711, G.729B                       |
| 4601<br>4602<br>4602SW<br>4620SW | add G.726A (requires firmware R2.2) |

| Telephone        | Codec to use |
|------------------|--------------|
| 4621SW<br>4622SW |              |

**Codec Set**

The number assigned to this Codec Set.

**Frames Per Pkt**

Specifies the number of frames per packet up to a packet size of 60 milliseconds (ms).

| Valid Entry | Usage   |
|-------------|---|
| 1 to 6      | Default frame sizes for codecs: <ul style="list-style-type: none"> <li>• G.711 and G.729: 2 frames (20 ms)</li> <li>• G.723: 3 frames (30 ms)</li> <li>• G.726A: 1 frame (10 ms)</li> </ul> |

**Media Encryption**

Specifies a priority listing of the three possible options for the negotiation of encryption. Communication Manager attempts to provide bearer encryption per this administered priority order. The selected option for an IP codec set applies to all codecs defined in that set. Available only if Media Encryption over IP is enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| aes         | Advanced Encryption Standard (AES), a standard cryptographic algorithm for use by U.S. government organizations to protect sensitive (unclassified) information.<br>Use this option to encrypt these links: <ul style="list-style-type: none"> <li>• Server-to-gateway (H.248)</li> <li>• Gateway-to-endpoint (H.323)</li> </ul>  |
| aea         | Avaya Encryption Algorithm. Use this option as an alternative to AES encryption when: <ul style="list-style-type: none"> <li>• All endpoints within a network region using this codec set must be encrypted.</li> <li>• All endpoints communicating between two network regions and administered to use this codec set must be encrypted.</li> </ul> SRTP is a media encryption standard defined in RFC 3711 as a profile of RTP. Communication Manager 4.0 supports the following functionality as given in RFC 3711: <ul style="list-style-type: none"> <li>• Encryption of RTP (optional but recommended)</li> <li>• Authentication of RTCP streams (mandatory)</li> </ul> |

| Valid Entry                         | Usage   |
|-------------------------------------|---|
|                                     | <ul style="list-style-type: none"> <li>• Authentication of RTP streams (optional but recommended)</li> <li>• Protection against replay</li> </ul> <p> <b>Note:</b><br/>In Communication Manager 4.0, SRTP encryption is supported by 96xx telephones only.</p> |
| 1-srtp-aescm128-hmac80              | 1-Encrypted/Authenticated RTP with 80-bit authentication tag  |
| 2-srtp-aescm128-hmac32              | 2-Encrypted/Authenticated RTP with 32-bit authentication tag  |
| 3-srtp-aescm128-hmac80-unauth       | 3-Encrypted RTP but not authenticated   |
| 4-srtp-aescm128-hmac32-unauth       | 4-Encrypted RTP but not authenticated   |
| 5-srtp-aescm128-hmac80-unenc        | 5-Authenticated RTP with 80-bit authentication tag but not encrypted  |
| 6-srtp-aescm128-hmac32-unenc        | 6-Authenticated RTP with 32-bit authentication tag but not encrypted  |
| 7-srtp-aescm128-hmac80-unenc-unauth | 7-Unencrypted/Unauthenticated RTP   |
| 8-srtp-aescm128-hmac32-unenc-unauth | <p>8-Unencrypted/Unauthenticated RTP</p> <p> <b>Note:</b><br/>For stations, the only value supported is srtp-aescm128-hmac80. H.323 IP trunks support all eight of the listed algorithms.</p>  |
| none                                | Media stream is unencrypted. This is the default.   |

**Packet Size (ms)**

The packet size in milliseconds.

**Silence Suppression**

Enables or disables RTP-level silence suppression on the audio stream.

**IP codec set: page 2**

Assigns the following characteristics to a codec set:

- Whether or not Direct-IP Multimedia is enabled for videophone transmissions.
- Whether or not endpoints in the assigned network region can route fax, modem, or TTY calls over IP trunks.
- Which mode the system uses to route the fax, modem, or TTY calls.
- Whether or not redundant packets will be added to the transmission for higher reliability and quality.

These characteristics must be assigned to the codec set, and the codec set must be assigned to a network region for endpoints in that region to be able to use the capabilities established on this screen.

 **Caution:**

If users are using Super G3 fax machines as well as modems, do not assign these fax machines to a network region with an IP Codec set that is modem-enabled as well as fax-enabled. If its **Codec set** is enabled for both modem and fax signaling, a Super G3 fax machine incorrectly tries to use the modem transmission instead of the fax transmission.

Therefore, assign modem endpoints to a network region that uses a modem-enabled IP Codec set, and assign the Super G3 fax machines to a network region that uses a fax-enabled IP Codec set.

 **Note:**

Transporting modem tones over IP between Avaya Communication Manager systems is a proprietary implementation. Also, FAX transport implementations, other than T.38 are proprietary implementations.

***Allow Direct-IP Multimedia***

Allows or disallows direct multimedia using the following codecs:

- H.261
- H.263
- H.264 (video)
- H.224
- H.224.1 (data, far-end camera control).

***Clear-channel***

Enables or disables supporting this codec set for BRI data calls.

 **Note:**

Clear Channel data transmission is supported on the TN2602AP IP Media Resource 320 circuit pack and the TN2302AP circuit pack.

**FAX Mode**

| Valid Entry   | Usage  |
|---------------|--|
| off           | Turn off <b>special fax handling</b> when using this codec set. In this case, the fax is treated like an ordinary voice call.<br>With a codec set that uses G.711, this setting is required to send faxes to non-Avaya systems that do not support T.38 fax. |
| relay         | For users in regions using this codec, use Avaya relay mode for fax transmissions over IP network facilities.  |
| pass-through  | For users in regions using this codec, use pass-through mode for fax transmissions over IP network facilities. This mode uses G.711-like encoding.   |
| t.38-standard | For users in regions using this codec, use T.38 standard signaling for fax transmissions over IP network facilities.   |

 **Note:**

If you have a telephone that is on an IP trunk too close to a fax machine, the handset can pick up the tones from the fax machine and change itself into the fax mode. To prevent this, turn off FAX mode, and put the FAX machines in an ARS partition that uses only circuit switched trunks, even for IGW FAX calls.

**Maximum Bandwidth Per Call for Direct-IP Multimedia (value)**

Available only if **Allow Direct-IP Multimedia** is enabled.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 9999   | The bandwidth limit for Direct-IP Multimedia transmissions on this codec set. Default is 256. |

**Related topics:**

[Allow Direct-IP Multimedia](#) on page 679

**Maximum Bandwidth Per Call for Direct-IP Multimedia (units)**

Available only if **Allow Direct-IP Multimedia** is enabled.

| Valid Entry    | Usage  |
|----------------|--|
| kbits<br>mbits | The unit of measure corresponding to the value entered for bandwidth limitation. Default is kbits. |

**Related topics:**

[Allow Direct-IP Multimedia](#) on page 679

**Modem Mode**

| Valid Entry  | Usage  |
|--------------|--|
| off          | Turn off <b>special modem handling</b> when using this codec set. In this case, the modem transmission is treated like an ordinary voice call. This is the default for new installations and upgrades.<br>With a codec set that uses G.711, this setting is required to send modem calls to non-Avaya systems.   |
| relay        | For users in regions using this codec, use relay mode for modem transmissions over IP network facilities. Avaya V.32/FNBDT Modem Relay is supported when using modem relay mode.<br><br> <b>Note:</b><br>Modem over VoIP in relay mode is currently available only for use by specific analog telephones that serve as Secure Telephone Units (STUs). Contact your Avaya technical support representative for more information. |
| pass-through | For users in regions using this codec, use pass-through mode for modem transmissions over IP network facilities. Avaya V.8 Modem Pass-Thru is supported when using modem pass-through mode.  |

**Redundancy**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 3      | The number of duplicate or redundant packets that are sent in addition to the primary packet for all modes except pass-through and Clear-channel. The default is 0. |

**TDD/TTY Mode**

| Valid Entry  | Usage   |
|--------------|---|
| off          | Turn off special TTY handling when using this codec set. In this case, the TTY transmission is treated like an ordinary voice call. With a codec set that uses G.711, this setting is required to send TTY calls to non-Avaya systems. However, there might be errors in character transmissions. |
| US           | For users in regions using this codec, use U.S. Baudot 45.45 mode for TTY transmissions over IP network facilities. This is the default for new installations and upgrades.   |
| UK           | For users in regions using this codec, use U.K. Baudot 50 mode for TTY transmissions over IP network facilities.  |
| pass-through | For users in regions using this codec, use pass-through mode for TTY transmissions over IP network facilities.  |

## IP Interfaces

Assigns a network region to an IP interface device, or administers Ethernet options.

The appearance of the IP Interfaces screen can vary according to the interface type you are administering, and your system's configuration.

 **Note:**

After starting the process of administering the IP interface for the TN2602AP circuit pack, any active calls continue to use the TN2602AP circuit pack's physical IP address for the connection, not the virtual IP address administered here. Therefore, any calls that continue after administering the virtual address, drop in the event of an interchange.

Example command: `add ip-interface n`, where *n* is the board location.

### IP Interface: page 1

#### **Allow H.248 Gateways**

Controls whether or not H.248 media gateways (G700, G450, G430, G350, and G250) can register on the interface.

| Valid Entry | Usage   |
|-------------|---|
| y           | On a simplex main server, enables H.248 endpoint connectivity to the Processor Ethernet (PE) interface. Used for a Survivable Remote Server (Local Survivable Processor).                 |
| n           | Disables H.248 endpoint connectivity to the PE interface. H.248 endpoint connectivity using the PE interface on a Survivable Core Server (Enterprise Survivable Server) is not supported. |

#### **Allow H.323 Endpoints**

Controls whether or not IP endpoints can register on the interface.

| Valid Entry | Usage   |
|-------------|---|
| y           | On a simplex main server, enables H.323 endpoint connectivity to the Processor Ethernet (PE) interface. Used for a Survivable Remote Server (Local Survivable Processor).                 |
| n           | Disables H.323 endpoint connectivity to the PE interface. H.323 endpoint connectivity using the PE interface on a Survivable Core Server (Enterprise Survivable Server) is not supported. |

#### **Code/Sfx**

Circuit pack TN code and suffix.

 **Note:**

The 4606, 4612, and 4624 telephones do not support the bearer duplication feature of the TN2602AP circuit pack. If these telephones are used while an interchange from active to standby media processor is in process, calls might be dropped.

**Related topics:**

[Critical Reliable Bearer](#) on page 683

**Critical Reliable Bearer**

Enables or disables a duplicate TN2602 circuit pack in a port. Available only with the TN2602.

 **Note:**

The 4606, 4612, and 4624 telephones do not support the bearer duplication feature of the TN2602AP circuit pack. If these telephones are used while an interchange from active to standby media processor is in process, calls might be dropped.

**Enable Ethernet Interface**

| Valid Entry | Usage   |
|-------------|---|
| y           | Enables the Ethernet port associated with the TN2602AP circuit pack.  |
| n           | Disables when there is no standby, or when the standby has been disabled. Should be disabled before administering the IP interface. |

**Ethernet Link**

The administered link number for an Ethernet link.

**Gateway Node Name**

The gateway node name associated with the IP address of the LAN gateway associated with the TN2602AP. This entry also applies to the second TN2602AP circuit pack when Critical Reliable Bearer is enabled. Accepts up to 15 characters.

 **Note:**

The 4606, 4612, and 4624 telephones do not support the bearer duplication feature of the TN2602AP circuit pack. If these telephones are used while an interchange from active to standby media processor is in process, calls might be dropped.

**Related topics:**

[Critical Reliable Bearer](#) on page 683

**Gatekeeper Priority**

Available only if H.323 endpoints are enabled and the Communication Manager server is a main server or a Survivable Remote Server. Not available on a Survivable Core Server.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 9      | Sets a priority on the interface that affects where the interface appears on the gatekeeper list. The value in this field is used on the alternate gatekeeper list. The lower the number, the higher the priority. Default is 5. |

**Related topics:**

[Allow H.323 Endpoints](#) on page 682

**Network Region**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 250    | <p>The value of the network region where the TN2602AP resides. This entry also applies to the second TN2602AP circuit pack when Critical Reliable Bearer is enabled.</p> <p> <b>Note:</b><br/>The 4606, 4612, and 4624 telephones do not support the bearer duplication feature of the TN2602AP circuit pack. If these telephones are used while an interchange from active to standby media processor is in process, calls might be dropped.</p> |

**Related topics:**

[Critical Reliable Bearer](#) on page 683

**Network uses 1's for Broadnet Addresses**

Allows or denies using a broadcast address to send the same message to all systems or clients on a local area network.

**Node Name**

The node name associated with the IP address of the TN2602AP circuit pack. Accepts up to 15 characters.

**Related topics:**

[Name](#) on page 700

[Group Type](#) on page 860

[Near-end Node Name](#) on page 865

**Receive Buffer TCP Window Size**

| Valid Entry | Usage   |
|-------------|---|
| 512 to 8320 | The number of bytes allotted for the buffer that receives TCP data for a TN799 (CLAN) circuit pack. The default is 512. |

**Slot**

The slot location. Requires entry of the location of the second TN2602AP circuit pack for a non-duplicated board.

 **Note:**

The 4606, 4612, and 4624 telephones do not support the bearer duplication feature of the TN2602AP circuit pack. If these telephones are used while an interchange from active to standby media processor is in process, calls might be dropped.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 64     | First and second characters are the cabinet number. |
| A to E      | Third character is the carrier.                     |

| Valid Entry | Usage   |
|-------------|---|
| 0 to 20     | Fourth and fifth character are the slot number. |

**Related topics:**

[Critical Reliable Bearer](#) on page 683

**Subnet Mask**

A 32-bit binary number that divides the network ID and the host ID in an IP address. This is the subnet mask for TN2602AP. Also applies to the second TN2602AP circuit pack when the critical reliable bearer is enabled.

**Related topics:**

[Critical Reliable Bearer](#) on page 683

**Target socket load**

The maximum number of sockets targeted for this interface. The default is 80% of the platform maximum. Used for load balancing endpoint traffic across multiple IP interfaces. Controls the percentage of sockets allocated to each IP interface within the same Gatekeeper Priority. When all the IP interfaces within the same Gatekeeper Priority exceeds the target number allocated, the system continues to add sockets until the interface is at its maximum capacity. Available only with a procr type IP interface.

**Note:**

The 4606, 4612, and 4624 telephones do not support the load balancing feature of the TN2602AP circuit pack.

| Valid Entry | Usage                    |
|-------------|--------------------------|
| 1 to 3500   | S8510 and duplex servers |
| 1 to 2500   | S8400                    |
| 1 to 2000   | CHAWK/BOXTER             |
| 1 to 1700   | VM/BLADE                 |

**Related topics:**

[Type](#) on page 686

**Target socket load and Warning level**

Controls the percentage of sockets allocated to each IP interface within the same Gatekeeper Priority. When all the IP interfaces within the same Gatekeeper Priority exceeds the target number allocated, the system continues to add sockets until the interface is at its maximum capacity. If the targeted percentage is exceeded on a CLAN, a warning alarm is generated.

If there is only one IP interface within a priority, the target socket load and warning level is not used for load balancing. A value in this field can be used to receive an error or a warning alarm if the targeted value is exceeded. Available only with CLAN type IP interfaces.



**Note:**

The 4606, 4612, and 4624 telephones do not support the load balancing feature of the TN2602AP circuit pack.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 499    | The maximum number of sockets targeted for this interface. If the number of sockets exceeds the targeted number, a warning alarm is generated. The default is 400. |

**Related topics:**

[Type](#) on page 686

**Type**

The type of IP interface.

| Valid Entry | Usage                                       |
|-------------|---|
| clan        | Control Local Area Network (C-LAN) board    |
| VAL         | Voice Announcement LAN board                |
| medpro      | Media Processor board                       |
| procr       | Processor — S8300D and duplex media servers |

**VLAN**

Sends Virtual Local Area Network (VLAN) instructions to the PROCR (S8300D/duplex Media Servers), CLAN, and Media Processor boards. It does not send VLAN instructions to IP endpoints such as IP telephones and softphones. Not available for Voice Announcement over LAN (VAL) boards.

| Valid Entry | Usage                            |
|-------------|----------------------------------|
| 0 to 4095   | Specifies the virtual LAN value. |
| n           | Disabled. This is the default.   |

**IP Interface: page 2**

**ETHERNET OPTIONS**

The Ethernet port associated with the TN2602AP must be disabled before any changes can be made to these fields.

**Auto?**

| Valid Entry | Usage                                     |
|-------------|---|
| y           | Enables auto-negotiation. Default.        |
| n           | Applies manual speed and duplex settings. |

## Duplex

Available only if auto-negotiation is disabled.

| Valid Entry | Usage   |
|-------------|---|
| Full        | The full duplex setting for this IP board. Default when speed is set to 100 Mbps. |
| Half        | The half duplex setting for this IP board. Default.                               |

**Related topics:**

[Auto?](#) on page 686

## Speed

Available only if auto-negotiation is disabled.

| Valid Entry       | Usage   |
|-------------------|---|
| 10Mbps<br>100Mbps | The speed of the Ethernet connection.<br>The only speed option available for the TN2602AP circuit pack is 100Mbps. This is the default and cannot be changed. |

**Related topics:**

[Auto?](#) on page 686

**IPV6 PARAMETERS**

## Enable Ethernet Interface

| Valid Entry | Usage   |
|-------------|---|
| y           | Enables the Ethernet port associated with the TN2602AP circuit pack.  |
| n           | Disables when there is no standby, or when the standby has been disabled. Should be disabled before administering the IP interface. |

## Ethernet Link

The administered link number for an Ethernet link.

## Gateway Node Name

The gateway node name associated with the IP address of the LAN gateway associated with the TN2602AP. This entry also applies to the second TN2602AP circuit pack when Critical Reliable Bearer is enabled. Accepts up to 15 characters.

**Note:**

The 4606, 4612, and 4624 telephones do not support the bearer duplication feature of the TN2602AP circuit pack. If these telephones are used while an interchange from active to standby media processor is in process, calls might be dropped.

**Related topics:**

[Critical Reliable Bearer](#) on page 683

Node Name

The node name associated with the IP address of the TN2602AP circuit pack. Accepts up to 15 characters.

**Related topics:**

[Name](#) on page 700

[Group Type](#) on page 860

[Near-end Node Name](#) on page 865

Subnet Mask

A 64-bit binary number that divides the network ID and the host ID in an IP address. This is the subnet mask for TN2602AP. Also applies to the second TN2602AP circuit pack when the critical reliable bearer is enabled.

 **Note:**

The 4606, 4612, and 4624 telephones do not support the bearer duplication feature of the TN2602AP circuit pack. If these telephones are used while an interchange from active to standby media processor is in process, calls might be dropped.

**Related topics:**

[Critical Reliable Bearer](#) on page 683

**IP Interfaces: page 3**

**VOIP/NETWORK THRESHOLDS**

Enable VoIP/Network Thresholds

Enables or disables the recording of Voice/Network Statistics at a system level for a single media processor board. This applies to both TN2602 boards, if duplicated. Any changes to the value of this field, results in an updated message sent to the media processor board.

Jitter (ms)

Available only if VoIP/Network thresholds are enabled and the board type is a media processor.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9999   | The unacceptable jitter coming into the media processor board at which point data is captured and send to Communication Manager. Default is 50 milliseconds. |

**Related topics:**

[Type](#) on page 686

[Enable VoIP/Network Thresholds](#) on page 688

Packet loss (%)

Available only if VoIP/Network thresholds are enabled and the board type is a media processor.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 100    | The percentage of the unacceptable packet loss coming into the administered media processor board. Default is 5. |

| Valid Entry | Usage   |
|-------------|---|
|             |  <b>Note:</b><br>xxx indicates 100% packet loss. |

**Related topics:**

[Type](#) on page 686

[Enable VoIP/Network Thresholds](#) on page 688

## RT Delay (ms)

Available only if VoIP/Network thresholds are enabled and the board type is a media processor.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 9999   | Round Trip Delay is the unacceptable elapsed time for a packet to reach remote location and revert. Default is 500 milliseconds. |

**Related topics:**

[Type](#) on page 686

[Enable VoIP/Network Thresholds](#) on page 688

## IP network region

Configures within-region and between-region connectivity settings for all VoIP resources and endpoints within a given IP region. The first page is used to modify the audio and QoS settings. The **Codec Set** field on this page reflects the CODEC set that must be used for connections between telephones within this region or between telephones and MedPro/Prowler boards and media gateways within this region. The ability to do NAT shuffling for direct IP-to-IP audio connections is also supported.

Example command: `change ip-network-region n`, where *n* is the network region number.

### IP network region: page 1

#### **Authoritative Domain**

The domain for which this network region is responsible. This appears in the **From** header of any SIP Enablement Services (SES) messages. Accepts a name or IP address consisting of up to 20 characters.

#### **Name**

A description of the region. Accepts up to 20 characters.

#### **Region**

The number of the network region being administered.

**MEDIA PARAMETERS**

Codec Set

| Valid Entry | Usage  |
|-------------|--|
| 1 to 7      | The number for the codec set for the region. |

Intra-region IP-IP Direct Audio

Allows direct audio connections between IP endpoints within a network region.

| Valid Entry     | Usage  |
|-----------------|--|
| y               | Saves on bandwidth resources and improves sound quality of voice over IP transmissions.  |
| n               | Might be used if, for example, the IP telephones within the region are behind two or more firewalls.   |
| native(NAT)     | The IP address from which audio is to be received for direct IP-to-IP connections within the region is that of the telephone/ softphone itself (without being translated by NAT). IP telephones must be configured behind a NAT device before this entry is enabled. |
| translated(NAT) | The IP address from which audio is to be received for direct IP-to-IP connections within the region is to be the one with which a NAT device replaces the native address. IP telephones must be configured behind a NAT device before this entry is enabled.         |

Inter-region IP-IP Direct Audio

Allows direct audio connections between IP endpoints in different regions

| Valid Entry     | Usage  |
|-----------------|--|
| y               | Saves on bandwidth resources and improves sound quality of voice over IP transmissions.  |
| n               | Might be used if, for example, the IP telephones within the region are behind two or more firewalls.   |
| native(NAT)     | The IP address from which audio is to be received for direct IP-to-IP connections between regions is that of the telephone itself (without being translated by NAT). IP telephones must be configured behind a NAT device before this entry is enabled.    |
| translated(NAT) | The IP address from which audio is to be received for direct IP-to-IP connections between regions is to be the one with which a NAT device replaces the native address. IP telephones must be configured behind a NAT device before this entry is enabled. |

IP Audio Hairpinning

If enabled, allows IP endpoints connected through the IP circuit pack in the server in IP format to bypass the Communication Manager TDM bus.

## Location

\* **Note:**

If the Multinational Locations feature is enabled, and IP telephones derive their network region from the IP Network Map, administer this field with a valid value (1 to 250). This allows the IP endpoints to use the right VoIP resources.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 250    | (Depending on your server configuration, see <i>Avaya Aura™ Communication Manager System Capacities Table</i> , 03-300511.) Assigns the location number to the IP network region. Allows correct date and time information, and trunk routing based on IP network region. The IP endpoint uses this as its location number. See the Location sections in <i>Avaya Aura™ Communication Manager Feature Description and Implementation</i> , 555-245-205, for the other ways, and for a list of features that use location. |
| blank       | Obtains the location from the cabinet containing the CLAN or the media gateway where the endpoint is registered. By default, the value is blank.  |

## RTCP Reporting Enabled

If enabled, sends RTCP Reports to a special server, such as for the VMON tool.

\* **Note:**

Regardless of how this field is administered, RTCP packets are always sent peer-to-peer.

**UDP PORT RANGE**

## UDP Port Range Min

| Valid Entry   | Usage  |
|---------------|--|
| 1024 to 65534 | The minimum range of the UDP port number used for audio transport. Defaults to 2048 to 3028. |

## UDP Port Range Max

| Valid Entry   | Usage  |
|---------------|--|
| 1025 to 65535 | The maximum range of the UDP port number used for audio transport. Defaults to 2048 to 3028. |

**RTCP MONITOR SERVER PARAMETERS**

## RTCP Report Period (secs)

Available only if RTCP Reporting is enabled and if Default Server Parameters are not enabled.

| Valid Entry | Usage   |
|-------------|---|
| 5 to 30     | The report period for the RTCP Monitor server in seconds. |

**Related topics:**

[RTCP Report Period \(secs\)](#) on page 691

[Use Default Server Parameters](#) on page 692

**Server IP Address**

The IP address for the RTCP Monitor server.

Available only if RTCP Reporting is enabled and if Default Server Parameters are not enabled.

**Related topics:**

[Use Default Server Parameters](#) on page 692

**Server Port**

Available only if RTCP Reporting is enabled and if Default Server Parameters are not enabled.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 65535  | The port for the RTCP Monitor server. Default is 5005. |

**Related topics:**

[RTCP Reporting Enabled](#) on page 691

[Use Default Server Parameters](#) on page 692

**Use Default Server Parameters**

If enabled, uses the system-wide default RTCP Monitor server parameters. Available only if RTCP Reporting is enabled.

**Related topics:**

[RTCP Reporting Enabled](#) on page 691

***DIFFSERV/TOS PARAMETERS***

**Audio PHB Value**

Provides scalable service discrimination in the Internet without per-flow state and signaling at every hop.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 63     | The decimal equivalent of the DiffServ Audio PHB value. Default is 46. |

**Call Control PHB Value**

Provides scalable service discrimination in the Internet without per-flow state and signaling at every hop.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 63     | The decimal equivalent of the Call Control PHB value. Default is 34. |

## Video PHB Value

| Valid Entry | Usage  |
|-------------|--|
| 0 to 63     | The decimal equivalent of the DiffServ Video PHB value. Default is 26. |

**802.1P/Q PARAMETERS**

## Audio 802.1p Priority

| Valid Entry | Usage  |
|-------------|--|
| 0 to 7      | Provides Layer 2 priority for Layer 2 switches. Changes take effect after circuit pack reset, phone reboot, or system reset. |

## Call Control 802.1p Priority

| Valid Entry | Usage  |
|-------------|--|
| 0 to 7      | Provides Layer 2 priority for Layer 2 switches. Changes take effect after circuit pack reset, phone reboot, or system reset. |

## Video 802.1p Priority

| Valid Entry | Usage   |
|-------------|---|
| 0 to 7      | The Video 802.1p priority value. Changes take effect after circuit pack reset, phone reboot, or system reset. |

**AUDIO RESOURCE RESERVATION PARAMETERS**

## Retry upon RSVP Failure Enabled

Enables or disables retries when RSVP fails.

Available only if RSVP is enabled.

**Related topics:**

[RSVP Enabled](#) on page 693

## RSVP Enabled

Enables or disables RSVP.

## RSVP Profile

Available only if RSVP is enabled.

Set this field to what you have configured on your network.

| Valid Entry        | Usage  |
|--------------------|--|
| guaranteed-service | Limits end-to-end queuing delay from sender to receiver. This setting is best for VoIP applications. |

## Managing inventory

| Valid Entry     | Usage   |
|-----------------|---|
| controlled-load | This subset of guaranteed-service provides for a traffic specifier, but not end-to-end queuing delay. |

### RSVP Refresh Rate (secs)

Available only if RSVP is enabled.

This field only appears if the **RSVP Enabled** field is set to y.

| Valid Entry | Usage                             |
|-------------|-----------------------------------|
| 1 to 99     | The RSVP refresh rate in seconds. |

### Related topics:

[RSVP Enabled](#) on page 693

### RSVP unreserved (BBE) PHB Value

| Valid Entry | Usage   |
|-------------|---|
| 0 to 63     | The BBE codepoint is used whenever an RSVP reservation is being obtained (pending), or has failed in some way, to provide better-than-best service to the voice stream. |

## H.323 IP ENDPOINTS

### H.323 Link Bounce Recovery

Enables or disables the H.323 Link Bounce Recovery feature for this network region. The default is enabled.

### Idle Traffic Interval (seconds)

| Valid Entry | Usage  |
|-------------|--|
| 5 to 7200   | The maximum traffic idle time in seconds after which a TCP Keep-Alive (KA) signal is sent from the endpoint.. Default is 20. |

### Keep-Alive Interval (seconds)

| Valid Entry | Usage  |
|-------------|--|
| 1 to 120    | Sets the interval between TCP Keep-Alive re-transmissions. When no ACK is received for all retry attempts, the local TCP stack ends the TCP session and the associated socket is closed. Default is 5. |

### Keep-Alive Count

| Valid Entry | Usage   |
|-------------|---|
| 1 to 20     | Sets the number of times the Keep-Alive message is transmitted if no ACK is received from the peer. Default is 5. |

**IP network region: page 2**

This page covers the information for Inter-Gateway Alternate Routing (IGAR), backup server names in priority order, and security procedures.

**INTER-GATEWAY ALTERNATE ROUTING/DIAL PLAN TRANSPARENCY**

If **Inter-Gateway Alternate Routing** (IGAR) is enabled for any row on subsequent pages, the following fields for each network region must be administered to route the bearer portion of an IGAR call.

## Conversion to Full Public Number - Delete

| Valid Entry | Usage                |
|-------------|----------------------|
| 0 to 7      | The digits to delete |

## Conversion to Full Public Number - Insert

| Valid Entry      | Usage   |
|------------------|---|
| 0 to 13<br>blank | <p>The number of digits to insert. International numbers should begin with “+”.</p> <p> <b>Note:</b><br/>The optional “+” at the beginning of the inserted digits is an international convention indicating that the local international access code must be dialed before the number.</p> |

## Dial Plan Transparency in Survivable Mode

| Valid Entry | Usage  |
|-------------|--|
| y           | Enables the Dial Plan Transparency feature when a media gateway registers with a Survivable Remote Server (Local survivable processor), or when a port network registers with a Survivable Core Server (Enterprise Survivable Server). |
| n           | Default is n.  |

## Incoming LDN Extension

An extension used to assign an unused Listed Directory Number for incoming IGAR calls.

## Maximum Number of Trunks to Use for IGAR

It is necessary to impose a limit on the trunk usage in a particular port network in a network region when Inter-Gateway Alternate Routing (IGAR) is active. The limit is required because if there is a major IP WAN network failure, it is possible to use all trunks in the network region(s) for IGAR calls.

| Valid Entry           | Usage   |
|-----------------------|---|
| 1 to 999, or<br>blank | The maximum number of trunks to be used for Inter-gateway alternate routing (IGAR). |

**BACKUP SERVERS IN PRIORITY ORDER**

Lists the backup server names in priority order. Backup server names should include Survivable Remote Server names, but should not include Survivable Core Server names. Any valid node name is a valid entry. Valid node names can include names of Customer LANs, ICCs, and Survivable Remote Servers.

**H.323 SECURITY PROCEDURES**

Selects the permitted security profile(s) for endpoint registration in this network region. At least one security procedure entry must be entered; otherwise, no endpoint will be permitted to register from the region.

| Valid Entry | Usage   |
|-------------|---|
| challenge   | Includes the various methods of PIN-based challenge/response schemes in current use; relatively weak.       |
| pin-eke     | The H.235 Annex H SP1.  |
| strong      | Permits use of any strong security profile; at present, only the pin-eke profile fits in this category.     |
| all         | Includes all of the above security profiles.  |
| none        | No security profile is required; permits use of an endpoint without user authentication (use with caution). |

**Allow SIP URI Conversion**

Administers whether or not a SIP URI should be permitted to change. Degrading the URI from sips//: to sip//: may result in a less secure call. This is required when SIP SRTP endpoints are allowed to make and receive calls from endpoints that do not support SRTP.

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows conversion of SIP URIs. Default is y.   |
| n           | No URI conversion. Calls from SIP endpoints that support SRTP made to other SIP endpoints that do not support SRTP will fail. However, if you enter y for the <b>Enforce SIPS URI for SRTP</b> field on the signaling group screen, URI conversion takes place independent of the value set for the <b>Allow SIP URI conversion</b> field on the IP Network Region screen. |

**TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS**

**Near End Establishes TCP Signaling Socket**

Indicates whether Communication Manager (the near end) can establish the TCP socket for H.323 IP endpoints in this network region.

| Valid Entry | Usage   |
|-------------|---|
| y           | Communication Manager determines when to establish the TCP socket with the IP endpoints, assuming the endpoints support this capability. This is the default. |

| Valid Entry | Usage  |
|-------------|--|
| n           | The IP endpoints always attempt to set up the TCP socket immediately after registration. This field should be disabled only in network regions where a non-standard H.323 proxy device or a non-supported network address translation (NAT) device would prevent the server from establishing TCP sockets with H.323 IP endpoints. |

## Near End TCP Port Min

| Valid Entry   | Usage   |
|---------------|---|
| 1024 to 65531 | The minimum port value used by the Control Lan (C-LAN) circuit pack or processor Ethernet when establishing the TCP signaling socket to the H.323 IP endpoint. The range of port number must be at least 5 (Max-Min+1). Default is 61440. |

**Related topics:**

[Near End TCP Port Max](#) on page 697

## Near End TCP Port Max

| Valid Entry   | Usage   |
|---------------|---|
| 1028 to 65535 | The maximum port value to be used by the Control Lan (C-LAN) circuit pack or processor Ethernet when establishing the TCP signaling socket to the H.323 IP endpoint. The range of port number must be at least 5 (Max-Min+1). Default is 61444. |

**Related topics:**

[Near End TCP Port Min](#) on page 697

**IP network region: page 3**

Each subsequent page shows the inter-region connectivity for 15 region pairs.

**AGL**

The maximum number of destination region IP interfaces included in alternate gatekeeper lists (AGL).

| Valid Entry | Usage  |
|-------------|--|
| 0 to 16     | Communication Manager uses the numeric value of gatekeeper addresses.  |
| all         | Communication Manager includes all possible gatekeeper addresses in the endpoint's own network region and in any regions to which the endpoint's region is directly connected. |
| blank       | The administration field is ignored.   |

**Audio WAN-BW limits (units)**

| Valid Entry  | Usage  |
|--|--|
| Calls<br>Dynamic<br>Kbits/sec<br>Mbits/sec<br>blank for<br>NoLimit | The unit of measure corresponding to the value entered for bandwidth limitation. Bandwidth should be limited by the number of connections, bandwidth in Kbits/sec, or bandwidth in Mbits/sec, or left blank. Default is blank. |

**codec-set**

| Valid Entry             | Usage   |
|-------------------------|---|
| 1 to 7<br>pstn<br>blank | The codec set used between the two regions. This field cannot be blank if this route through two regions is being used by some non-adjacent pair of regions. If the two regions are not connected at all, this field should be blank. |

**direct-WAN**

Indicates whether the two regions (source and destination) are directly connected by a WAN link. The default value is enabled if a **codec-set** is administered.

**Related topics:**

[codec-set](#) on page 698

**dst rgn**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 250    | The destination region for this inter-network connection. |

**Dynamic CAC Gateway**

Available only if the **Audio WAN-BW- limit** is dynamic. The gateway must be configured to be a CAC (Call Admission Control) gateway.

| Valid Entry       | Usage   |
|-------------------|---|
| 1 to 250<br>blank | The gateway that reports the bandwidth-limit for this link. Default is blank. |

**Related topics:**

[Audio WAN-BW limits \(units\)](#) on page 697

**IGAR**

Allows pair-wise configuration of Inter-Gateway Alternate Routing (IGAR) between network regions.

| Valid Entry | Usage   |
|-------------|---|
| y           | Enables IGAR capability between this network region pair. Default for a pstn codec set. |

| Valid Entry | Usage  |
|-------------|--|
| n           | Disable IGAR capability between this network region pair. Default, except for a pstn codec set.  |
| f           | Forced. Moves all traffic onto the PSTN. This option can be used during initial installation to verify the alternative PSTN facility selected for a network region pair. This option can also be used to temporarily move traffic off of the IP WAN if an edge router is having problems or an edge router needs to be replaced between a network region pair. |

### ***Intervening-regions***

Allows entry of intervening region numbers between the two indirectly-connected regions.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 250    | Up to four intervening region numbers between the two indirectly-connected regions.<br><br> <b>Note:</b><br>Entry is not allowed for indirect region paths until all direct region paths have been entered. In addition, the order of the path through the regions must be specified starting from the source region to the destination region. |

### ***src rgn***

| Valid Entry | Usage  |
|-------------|--|
| 1 to 250    | The source region for this inter-network connection. |

### ***Video (Norm)***

| Valid Entry  | Usage  |
|--|--|
| 0 to 9999 for Kbits<br>0 to 65 for Mbits<br>blank for<br>NoLimit | The amount of bandwidth to allocate for the normal video pool to each IP network region. |

### ***Video (Prio)***

| Valid Entry  | Usage  |
|--|--|
| 0 to 9999 for Kbits<br>0 to 65 for Mbits<br>blank for<br>NoLimit | The amount of bandwidth to allocate for the priority video pool to each IP network region. |

### Video (Shr)

Specifies whether the normal video pool can be shared for each link between IP network regions.

### WAN-BW limits (value)

| Valid Entry        | Usage   |
|--------------------|---|
| 1 to 9999<br>blank | The bandwidth limits for direct WAN links. Values for this field can be entered in the number of connections, bandwidth in Kbits/sec, or bandwidth in Mbits/sec, or left blank. Default is blank. |

### WAN-BW limits (units)

| Valid Entry                                | Usage   |
|--|---|
| Calls<br>Kbits/sec<br>Mbits/sec<br>NoLimit | The unit of measure corresponding to the value entered for bandwidth limitation. Limits bandwidth by number of connections, bandwidth in Kbits/sec, bandwidth in Mbits/sec, or NoLimit. Default is NoLimit. |

## IP Node Names

Administers node names and IP addresses for the switch and the terminal server media processors administered on the IP Interfaces screen.

 **Note:**

The Processor Ethernet interface node name (procr) automatically appears on the IP Node Names screen. The PE interface node name cannot be added to the IP Node Names screen. The line containing the keyword procr displays the IP address.

Example command: `change node-names ip`

### Name

The name of the adjunct, server, or switch node used as a label for the associated IP address. The node names must be unique for each server or switch. Uses up to 15 alpha-numeric characters.

 **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

### IP Address

A unique IP address assigned to each port on any IP device that is used for a connection. Also supports IPv6 address format.

**Note:**

The Converged Communications Server for SIP Enablement Services (SES) Instant Messaging requires an IP address for the SIP Enablement Services (SES) Proxy Server for the network.

## IP options system parameters

Example command: `change system-parameters ip-options`

### IP options system parameters: page 1

#### **AUTOMATIC TRACE ROUTE ON**

##### Link Failure

Enables or disables the automatic trace route command. If enabled, to diagnose network problems, especially to determine where a network outage exists, Communication Manager initiates an automatic trace-route command when the connectivity between a server and its port networks, media gateways, or IP trunks is lost.

**Note:**

If disabled, any automatic trace-route currently in progress finishes, and no subsequent trace-route commands are launched or logged. In other words, the link failure buffer is cleared.

#### **H.248 MEDIA GATEWAY**

##### Link Loss Delay Timeout (minutes)

| Valid Entry | Usage  |
|-------------|--|
| 1 to 30     | The number of minutes to delay the reaction of the call controller to a link bounce. Assists with the H.248 link bounce recovery mechanism of the Avaya G700 Media Gateway. Specifically, prevents the call controller from removing all boards and ports prematurely in response to a link bounce. Default is 5 |

#### **H.323 IP ENDPOINT**

##### Link Loss Delay Timer (minutes)

| Valid Entry | Usage   |
|-------------|---|
| 1 to 60     | The number of minutes to delay the reaction of the call controller to a link bounce. Specifies how long the Communication Manager server preserves registration and any stable calls that might exist on the endpoint after it has lost the call signaling channel to the endpoint. If the endpoint does not re-establish connection within this period, the system tears down the registration and any calls of the endpoint. This timer does not apply to soft IP endpoints operating in telecommuter mode. Default is 5. |

Periodic Registration Timer (min)

This timer is started when an IP telephone registration is taken over by another IP endpoint. When the timer expires, the telephone tries to reregister with the server. Default timer value is dependent on the number of unsuccessful periodic registration attempts. Sample field values apply unless the endpoint is interrupted, such as by power loss, or the user takes manual action to override this automatic process:

- 20 means once every 20 minutes for two hours, then once an hour for 24 hours, then once every 24 hours continually.
- 60 means once an hour for two hours, then once an hour for 24 hours, then once every 24 hours continually.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 60     | The number of minutes before an IP telephone registration is taken over by another IP endpoint attempts to re-register with the server. Default is 60. |

Primary Search Time (seconds)

| Valid Entry | Usage  |
|-------------|--|
| 15 to 3600  | The maximum number of seconds the IP endpoint attempts to register with its current Communication Manager server while the telephone is hung up before going to a Survivable Remote Server. This timer allows the customer to specify the maximum time that an IP endpoint spends on trying to connect to the C-LANS before going to a Survivable Remote Server.<br>When the IP telephone's receiver is lifted, the endpoint continues trying to re-establish connection with the current server until the call ends. Default is 75. |

Short/Prefixed Registration Allowed

Appears if the **IP Stations** field on the System Parameters Customer Options screen is set to y.

| Valid Entry | Usage  |
|-------------|--|
| y           | Call Processing allows an IP endpoint to register using a short extension, for the extensions that have <b>Short/Prefixed Registration Allowed</b> field set to default on the Station screen. The default value is y. |
| n           | Call Processing does not allow an IP endpoint to register using a short extension, for the extensions that have <b>Short/Prefixed Registration Allowed</b> field set to default on the Station screen.                 |

**Related topics:**

[Short/Prefixed Registration Allowed](#) on page 905

**IP MEDIA PACKET PERFORMANCE THRESHOLDS****Enable Voice/Network Stats**

Enables or disables the recording of voice and network statistics at a system level for all TN2302/TN2602 media processor boards in the network. The default value is disabled.

**Number of Pings Per Measurement Interval**

| Valid Entry | Usage  |
|-------------|--|
| 10 to 100   | the number of test pings that comprise a measurement from which the performance values (delay and loss) are calculated. Default is 10. |

**Packet Loss (%)**

Specifies thresholds to be applied to packet loss rates (as measured by ping) for determining activation or deactivation of signaling group bypass.

**High:**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 100    | The high value cannot be less than the minimum value. Default is 40. |

**Low:**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 100    | The low value cannot be more than the maximum value. Default is 15. |

**Ping Test Interval (sec)**

| Valid Entry | Usage   |
|-------------|---|
| 10 to 999   | The time between performance test pings for each testable signaling group. Default is 20. |

**Roundtrip Propagation Delay (ms)**

Specifies thresholds to be applied to roundtrip packet propagation delays as measured by ping, for use in activating or clearing signaling group bypass.

**High:**

| Valid Entry | Usage   |
|-------------|---|
| 10 to 9999  | The high value cannot be less than the minimum value. Default is 800. |

**Low:**

| Valid Entry | Usage  |
|-------------|--|
| 10 to 9999  | The low value cannot be more than the maximum value. Default is 400. |

### **MEDIA GATEWAY ANNOUNCEMENT SERVER PARAMETERS**

#### Announcement Server IP Address

The IP address of the Announcement Server that is a unique IP address assigned to each port on any IP device that is used for a connection.

#### Announcement Storage Path Name

The directory path name on the Announcement Server where the announcements are stored. Accepts up to 40 characters.

#### Login

The login used by the Media Gateway to access the Announcement Server. Accepts up to 10 characters.

#### Password

The password used by the Media Gateway to access the Announcement Server. Accepts up to 10 characters.

### **RTCP MONITOR SERVER**

The RTCP monitor is a separate computer that receives RTCP packets from many devices. Communication Manager pushes these values to IP telephones, IP softphones and VoIP media modules, such that they know where to send the data.

#### Default RTCP Report Period (secs)

| Valid Entry | Usage  |
|-------------|--|
| 5 to 99     | The number of seconds IP telephones, IP softphones, and VoIP media modules send RTCP packets to the RTCP server. |

#### Default Server IP Address

The default IP address of the RTCP server used for each administered region. A unique IP address is assigned to each port on any IP device that is used for a connection.

#### **Related topics:**

[Server IP Address](#) on page 692

#### Default Server Port

| Valid Entry | Usage  |
|-------------|--|
| 1 to 65535  | The default TCP/IP port of the RTCP server. Default is 5005. |

#### Link Failure

Enables or disables the automatic trace route command. If enabled, to diagnose network problems, especially to determine where a network outage exists, Communication Manager initiates an automatic trace-route command when the connectivity between a server and its port networks, media gateways, or IP trunks is lost.

**Note:**

If disabled, any automatic trace-route currently in progress finishes, and no subsequent trace-route commands are launched or logged. In other words, the link failure buffer is cleared.

**IP options system parameters: page 2*****Prefer use of G.711 by Music Sources***

Enables or disables using G.711 for intra-switch Music-On-Hold. The default value is n.

***Force Phones and Gateways to Active LSPs***

Enables or disables forcing telephones and media gateways to active LSPs. The default is disabled.

***HYPERACTIVE MEDIA GATEWAY REGISTRATIONS*****Enable Detection and Alarms**

Enables or disables the hyperactive media gateway registration feature. Default is disabled.

**Number of Registrations within the Window**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 19     | The number of registrations that occur within the hyperactivity window for generating a Gateway alarm. Default is 3. Available only if detection and alarming is enabled . |

**Related topics:**

[Enable Detection and Alarms](#) on page 705

**Parameters for Media Gateway Alarms: Hyperactive Registration Window (minutes)**

Available only if detection and alarming is enabled.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 15     | The time in minutes for checking hyperactive media gateway registrations. Default is 4 minutes. |

**Related topics:**

[Enable Detection and Alarms](#) on page 705

**Parameters for Network Region Registration (NR-REG) Alarms: % of Gateways in Network Region with Hyperactive Registration Alarms**

Available only if detection and alarming is enabled.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 99     | The percent of Gateways within an ip-network region that should be alarmed before an IP-Registration alarm is generated. Default is 80%. |

**Related topics:**

[Enable Detection and Alarms](#) on page 705

**IP DTMF TRANSMISSION MODE**

**Inter-System IP DTMF Transmission Mode**

Specifies the touchtone signals that are used for dual-tone multifrequency (DTMF) telephone signaling.

| Valid Entry  | Usage   |
|--------------|---|
| in-band      | All G711 and G729 calls pass DTMF in-band. DTMF digits encoded within existing RTP media stream for G.711/G.729 calls. G.723 is sent out-of-band.   |
| in-band-g711 | Only G711 calls pass DTMF in-band.  |
| out-of-band  | All IP calls pass DTMF out-of-band. For IP trunks, the digits are done with either Keypad IEs or H245 indications. This value is not supported for SIP signaling. This is the default for newly added H.323 signaling groups. |
| rtp-payload  | This is the method specified by RFC1533. This is the default for newly added SIP signaling groups. Support for SIP Enablement Services (SES) trunks requires the default entry of rtp-payload.                                |

**Intra-System IP DTMF Transmission Mode**

The IP transmission mode.

| Valid Entry | Usage  |
|-------------|--|
| in-band     | DTMF digits encoded within existing RTP media stream for G.711/G.729 calls. G.723 is sent out-of-band. |
| rtp-payload | Support for SIP Enablement Services (SES) trunks requires the entry of rtp-payload.                    |

**IP options system parameters: page 3**

This screen is used to administer SNMP station parameters and services dialpad parameters. Applicable terminal types include: 4601, 4602, 4610, 4620, 4621, 4622, 4625, 96xx, or 16xx.

**SERVICES DIALPAD PARAMETERS**

**Download Flag**

Determines whether or not the SNMP parameters and associated IP addresses are downloaded to the terminals. The default is disabled

**Password**

The Craft Procedures password used as part of the Craft Procedures, also called Local Procedures. Accepts up to seven digits. This password allows a technician to go to an IP Terminal and modify individual parameters on that specific Terminal, such as the Terminal's IP address, Ethernet interface speed, and so on. The Craft Procedures Password must be entered on the dial pad in the applicable manner for the technician to have access to the Craft Procedures. Default is 27238 (craft).

**SNMP STATION PARAMETERS****Community String**

A string used by IP endpoints to determine whether the terminal allows receipt of SNMP queries, and if so, with what password. Accepts up to 32 characters. If the SNMP community string is null, the terminal ignores all incoming SNMP messages. Otherwise, the community string must be present in the incoming SNMP message for the Terminal to act on that message (subject to other considerations, such as the SNMP Source Address).

**Download Flag**

Determines whether or not the SNMP parameters and associated IP addresses are downloaded to the terminals. The default is disabled

**SOURCE ADDRESSES**

A valid node name that validates the source of an SNMP message. If the SNMP Source Address list is null, the Terminal responds to any valid SNMP message where “valid” means the appropriate SNMP community string is properly included. Otherwise, the Terminal responds to valid SNMP messages only if the IP Source Address of the query matches an address in the SNMP Source Address list.

Up to six node names are allowed that map to proper IP node name addresses. An IP address of 0.0.0.0 is a valid address.

**Related topics:**

[IP Address](#) on page 700

**IP options system parameters: page 4****Dest # 1, 2, or 3 IP address**

The valid destination IPv4 address. The default destination address is 0.0.0.0.

**Local Facility**

| Valid Entry      | Usage  |
|------------------|--|
| local0 to local7 | Displays the help message upon acceptable values for local use. The default value is local4. |

**Port #**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 65535  | The valid port number associated with the destination IPv4 address. The default port number is 514. |

**Related topics:**

[Dest # 1, 2, or 3 IP address](#) on page 707

**MUSIC/ANNOUNCEMENTS IP-CODEC PREFERENCES**

In general, when operating across the WAN with limited bandwidth facilities, the ip-codec-set is configured only with the compressed voice codecs. Sometimes it is necessary to carry the

voice calls with the normal configured compressed codecs, and the music or announcement sources are received with non-compressed G.711 codecs.

If you administer the following fields, when possible, the system overrides the ip-codec-set preference which can be configured to prefer a compressed codec, with non-compressed G.711. If the device receives the music or announcement source which has signaled support for G.711, the system attempts to use G.711.

**Prefer use of G.711 by Announcement Sources**

Overrides the ip-codec-set preference and establishes inter-PN or inter-gateway connections transmitting announcements with G.711. The default value is n.

**Prefer use of G.711 by IP Endpoints Listening to Announcements**

Overrides the ip-codec-set preference and reconfigures the IP endpoints listening to an announcement source with G.711. The default value is n.

**Prefer use of G.711 by IP Endpoints Listening to Music**

Overrides the ip-codec-set preference and reconfigures the IP endpoints listening to a music source with G.711. The default value is n.

**Prefer use of G.711 by Music Sources**

Overrides the ip-codec-set preference and establishes inter-PN or inter-gateway connections transmitting music with G.711. The default value is n.

## IP Routing

There is one-to-one mapping between the **Network Bits** and the **Subnet Mask** fields; entering a value in one field uniquely determines the other field. A list of Subnet Mask addresses and their corresponding Network Bits are shown in Table below.

| Network Bits | Subnet Mask | Number of Hosts | Network Type |
|--------------|-------------|-----------------|--------------|
| 0            | 0.0.0.0     | 4,294,967,294   | / 0          |
| 1            | 128.0.0.0   | 2,147,483,646   | / 1          |
| 2            | 192.0.0.0   | 1,073,741,822   | / 2          |
| 3            | 224.0.0.0   | 536,870,910     | / 3          |
| 4            | 240.0.0.0   | 268,435,454     | / 4          |
| 5            | 248.0.0.0   | 134,217,726     | / 5          |
| 6            | 252.0.0.0   | 67,108,862      | / 6          |
| 7            | 254.0.0.0   | 33,554,430      | / 7          |
| 8            | 255.0.0.0   | 16,777,214      | / 8          |
| 9            | 255.128.0.0 | 8,388,606       | / 9          |
| 10           | 255.192.0.0 | 4,194,302       | / 10         |

| Network Bits | Subnet Mask     | Number of Hosts | Network Type |
|--------------|-----------------|-----------------|--------------|
| 11           | 255.224.0.0     | 2,097,150       | / 11         |
| 12           | 255.240.0.0     | 1,048,574       | / 12         |
| 13           | 255.248.0.0     | 524,286         | / 13         |
| 14           | 255.252.0.0     | 262,142         | / 14         |
| 15           | 255.254.0.0     | 131,070         | / 15         |
| 16           | 255.255.0.0     | 65,534          | / 16         |
| 17           | 255.255.128.0   | 32,766          | / 17         |
| 18           | 255.255.192.0   | 16,382          | / 18         |
| 19           | 255.255.224.0   | 8,190           | / 19         |
| 20           | 255.255.240.0   | 4,094           | / 20         |
| 21           | 255.255.248.0   | 2,046           | / 21         |
| 22           | 255.255.252.0   | 1,022           | / 22         |
| 23           | 255.255.254.0   | 510             | / 23         |
| 24           | 255.255.255.0   | 254             | / 24         |
| 25           | 255.255.255.128 | 126             | / 25         |
| 26           | 255.255.255.192 | 62              | / 26         |
| 27           | 255.255.255.224 | 30              | / 27         |
| 28           | 255.255.255.240 | 14              | / 28         |
| 29           | 255.255.255.248 | 6               | / 29         |
| 30           | 255.255.255.252 | 2               | / 30         |
| 31           | 255.255.255.254 | 1               | /31          |
|              | 255.255.255.255 | 0               | /32          |

## Board

| Valid Entry                           | Usage  |
|---------------------------------------|--|
| 1 to 64                               | First and second characters are the cabinet number |
| A to E                                | Third character is the carrier                     |
| 0 to 20                               | Fourth and fifth character are the slot number     |
| 01 to 04 (Analog TIE trunks)<br>01–31 | Six and seventh characters are the circuit number  |
| 1 to 250                              | Gateway  |

| Valid Entry | Usage  |
|-------------|--------|
| V1 to V9    | Module |

**Destination Node**

The name of the final destination node of the IP route for this connection.

**Related topics:**

[IP Node Names](#) on page 700

**Gateway**

The node name of the first intermediate node consisting of a port on the CLAN circuit pack or a Destination Node on another IP route. If there are one or more intermediate nodes, the first intermediate node is the Gateway. If there are no intermediate nodes between the local and remote CLAN ports for this connection, the Gateway is the local CLAN port.

**Related topics:**

[IP Node Names](#) on page 700

**Metric**

| Valid Entry | Usage  |
|-------------|--|
| 0           | A server that has only one CLAN circuit pack installed.      |
| 1           | A server that has more than one CLAN circuit pack installed. |

**Network Bits**

A 32-bit binary number that divides the network ID and the host ID in an IP address.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 32     | The number of Network Bits associated with this IP route. |

**Route Number**

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 400    | The number of the IP router. |

**IP Server Interface (IPSI) Administration**

Adds a TN2312 IPSI (IP Server Interface) circuit pack. Uses the IP Server Interface (IPSI) to control port networks and provide tone, clock, and call classification services. The IPSI board connects to the control network by way of Ethernet.

In Communication Manager Release 5.2, the IP server interface administration for the TN2312 IPSI or the TN8412 SIPI provides support for Communication Manager—based SAT administration of IPSI Quality of Service (QoS) and Ethernet interface settings parameters. All further references to IPSI also apply to the TN8412 SIPI.

**Note:**

Initial IPSI settings must be done using the IPSI CLI interface.

Example command: `change ipserver-interface n`, where *n* is the assigned IPSI board location.

**IP Server Interface (IPSI) Administration: page 1*****Administer secondary ip server interface board***

If enabled, assigns a secondary IPSI board.

***Enable QoS***

If enabled, turns on quality of service (QoS) from the server to the IPSI link. If you enable QoS for the control network, also enable it from the Web interface.

***Encryption***

Enables socket encryption for the server and IPSI link.

***Ignore Connectivity in Server Arbitration***

If enabled, does *not* test the integrity of the IPSI when checking the health of the server pair.

***IP Control***

Administers IP control of port networks.

| Valid Entry | Usage   |
|-------------|---|
| y           | All port networks have an IPSI that provides control. A DS1 Converter (DS1C) circuit pack cannot be added to a port network when this value is y. |
| n           | This IPSI is used only for Tone Clock/Tone Detector functions. Use when the port network contains a DS1 Converter (DS1C) circuit pack.            |

***PRIMARY IPSI*****DHCP**

Displays whether IPSI is currently set up for DHCP addressing, or static addressing.

If DHCP is not enabled for the System Management Interface, this field is set to disabled (read-only).

- If DHCP is disabled for the IP Server Interface, the following event occurs:
  - If IPSI is in-service, it disallows the service and displays the `ipserver must be busied out` message.
  - If IPSI is busied out, the static equivalent to the DHCP address automatically populates the **Host**. The **Subnet Mask** and **Gateway** values must be populated manually. The pre-populated values can be optionally overwritten.
- If DHCP is enabled for IP Server Interface, the following event occurs:
  - If IPSI is in-service, it disallows the service and displays the `ipserver must be busied out` message.

## Managing inventory

- If the If the IPSI is busied out, it accepts the changes and re-populates this field.

### Gateway

The valid gateway IPv4 address.

- If DHCP is enabled for the IP Server Interface, the value of this field is read-only. View the value of this field based on the access.
- If DHCP is disabled for the IP Server Interface and this field is changed, after screen validation, the system checks if IPSI is busied out. If not, the IPSI does not accept the change, and displays the `ipserver must be busiedout` message.

### Host

The name of the DHCP client identifier. If DHCP is enabled for the System Management Interface, the **Host** value is displayed for the IP Server Interface. If DHCP is not enabled, the **Host** value is not displayed.

### IP Address

The valid IPv4 IP address.

- If DHCP is enabled for the IP Server Interface, the value of this field is read-only. View the value of this field based on the access.
- If DHCP is disabled for the IP Server Interface and this field is changed, after screen validation, the system checks if IPSI is busied out. If not, the IPSI does not accept the change, and displays the `ipserver must be busiedout` message.

### Location

The primary IPSI board location.

| Valid Entry | Usage   |
|-------------|---|
| 01 to 64    | First and second numbers are the cabinet number |
| A to E      | Third character is the carrier                  |
| 01 to 20    | Fourth and fifth characters are the slot number |
| 01 to 250   | Gateway   |
| V1 to V9    | Module  |

### Subnet Mask

| Valid Entry | Usage   |
|-------------|---|
| /xx         | Represented as subnet bits. <ul style="list-style-type: none"><li>• If DHCP is enabled for the IP Server Interface, the value of this field is read-only. View the value of this field based on the access.</li><li>• If DHCP is disabled for the IP Server Interface and this field is changed, after screen validation, the system checks if IPSI is busied out. If not, the IPSI does not accept the change, and displays the <code>ipserver must be busiedout</code> message.</li></ul> |

**QoS AND ETHERNET SETTINGS**

## 802.1p

| Valid Entry | Usage   |
|-------------|---|
| 0 to 7      | Displays the 802.1p value. This value can be changed only if the System Level Parameter Values is disabled for the IP Server interface. This value takes effect when the IPSI is busied out or released. Accepts only whole numbers.<br>The default value is 6. |

**Related topics:**

[Use System Level Parameter Values](#) on page 713

## Auto

If the IPSI is busied out, you can change this value from disabled to enabled and vice versa.

## DiffServ

| Valid Entry | Usage  |
|-------------|--|
| 0 to 63     | Displays the DiffServ code point (DSCP). This value can be changed only if the System Level Parameters Values is disabled for the IP Server interface. This value takes effect when the IPSI is busied out or released. Default is 46. Accepts only whole numbers. |

**Related topics:**

[Use System Level Parameter Values](#) on page 713

## Duplex

| Valid Entry  | Usage  |
|--------------|--|
| Half<br>Full | Displays the duplex settings for this IP board. This value can be changed only if the IPSI is busied out. The default is Full. |

## Speed

| Valid Entry       | Usage   |
|-------------------|---|
| 10Mbps<br>100Mbps | Displays the speed of the Ethernet connection. This value can be changed only if the IPSI is busied out. The default value is 100 Mbps. |

## Use System Level Parameter Values

Enables or disables system level parameter values.

## **SECONDARY IPSI**

### DHCP

Displays whether IPSI is currently set up for DHCP addressing, or static addressing.

If DHCP is not enabled for the System Management Interface, this field is set to disabled (read-only).

- If DHCP is disabled for the IP Server Interface, the following event occurs:
  - If IPSI is in-service, it disallows the service and displays the `ipserver must be busied out` message.
  - If IPSI is busied out, the static equivalent to the DHCP address automatically populates the **Host**. The **Subnet Mask** and **Gateway** values must be populated manually. The pre-populated values can be optionally overwritten.
- If DHCP is enabled for IP Server Interface, the following event occurs:
  - If IPSI is in-service, it disallows the service and displays the `ipserver must be busied out` message.
  - If the If the IPSI is busied out, it accepts the changes and re-populates this field.

### Host

The name of the DHCP client identifier. If DHCP is enabled for the System Management Interface, the **Host** value is displayed for the IP Server Interface. If DHCP is not enabled, the **Host** value is not displayed.

### Gateway

The valid gateway IPv4 address.

- If DHCP is enabled for the IP Server Interface, the value of this field is read-only. View the value of this field based on the access.
- If DHCP is disabled for the IP Server Interface and this field is changed, after screen validation, the system checks if IPSI is busied out. If not, the IPSI does not accept the change, and displays the `ipserver must be busiedout` message.

### IP Address

The valid IPv4 IP address.

- If DHCP is enabled for the IP Server Interface, the value of this field is read-only. View the value of this field based on the access.
- If DHCP is disabled for the IP Server Interface and this field is changed, after screen validation, the system checks if IPSI is busied out. If not, the IPSI does not accept the change, and displays the `ipserver must be busiedout` message.

### Location

The secondary IPSI board location.

| Valid Entry | Usage   |
|-------------|---|
| 01 to 64    | First and second numbers are the cabinet number |

| Valid Entry | Usage   |
|-------------|---|
| A to E      | Third character is the carrier                  |
| 01 to 20    | Fourth and fifth characters are the slot number |
| 01 to 250   | Gateway   |
| V1 to V9    | Module  |

### Subnet Mask

| Valid Entry | Usage   |
|-------------|---|
| /xx         | <p>Represented as subnet bits.</p> <ul style="list-style-type: none"> <li>If DHCP is enabled for the IP Server Interface, the value of this field is read-only. View the value of this field based on the access.</li> <li>If DHCP is disabled for the IP Server Interface and this field is changed, after screen validation, the system checks if IPSI is busied out. If not, the IPSI does not accept the change, and displays the <code>ipserver must be busiedout</code> message.</li> </ul> |

### IP Server Interface (IPSI) Administration: page 2

#### **Dest # 1, 2, or 3 IP Address**

The valid destination IPv4 IP address format. Provides support for future IPv6 address format.

Default destination address is unspecified.

#### **Enable Syslog**

Enabled only for init and inads login access. For duplicated TN2602 boards, this field is displayed for each board.

| Valid Entry | Usage  |
|-------------|--|
| y           | The system checks the firmware support syslog by capabilities exchange information. If it does not get the support, the system displays the <code>unsupported board code or vintage error message</code> and does not enable syslog. |
| n           | The system does not display the rest of the syslog fields. This is the default.  |

#### **Local Facility #**

| Valid Entry                         | Usage  |
|-------------------------------------|--|
| local0 to local7<br>(for local use) | Displays the help message on acceptable values. Default value is local4. |

**Port #**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 65535  | The valid port number associated with the <b>Dest # 1, 2 or 3 IP address</b> value. Default port number is 514. |

**Related topics:**

[Dest # 1, 2, or 3 IP Address](#) on page 715

**Use System Syslog Values**

If enabled, populates the address, port, and facility information as read-only.

**DEBUG FILTER VALUES**

Object

| Valid Entry | Usage  |
|-------------|--|
| 0 to 255    | The category of a log event. For example, angel and archangel.<br><br> <b>Note:</b><br>Maximum value of 255 triggers a file dump. |

Level

| Valid Entry | Usage  |
|-------------|--|
| 0 to 65535  | The level of logging for the given object.<br><br> <b>Note:</b><br>Maximum value of 65535 triggers a file dump. |

**IP Services**

Administers the connectivity for various adjuncts.

 **Note:**

You cannot remove a service from this screen if that service has overrides defined on the Survivable Processor screen.

Example command: `change ip-services`

**IP Services: page 1**

**Enabled**

Enables or disables this IP service. Available only with an IP **Service Type** of AESVCS orSAT.

**Related topics:**

[Service Type](#) on page 717

**Local Node**

| Valid Entry         | Usage   |
|---------------------|---|
| <i>IP node name</i> | A previously-administered node name for the link administered for services over the Control Lan (C-LAN) circuit pack. |
| procr               | The Communication Manager's Processor Ethernet interface for adjunct connectivity.                                    |

**Related topics:**

[Name](#) on page 700

**Local Port**

The originating port number.

| Valid Entry  | Usage  |
|--------------|--|
| 5000 to 9999 | 5111 to 5117 for SAT applications<br>5678 for ASAI |
| 0            | For client applications, defaults to 0.            |

**Remote Node**

The server or switch at the far end of the link for SAT.

| Valid Entry         | Usage   |
|---------------------|---|
| <i>IP node name</i> | A previously-administered node name used to provide added security for SAT. |
| any                 | Any available node.   |

**Remote Port**

The port number of the destination.

| Valid Entry   | Usage   |
|---------------|---|
| 5000 to 64500 | If this service is a client application, such as CDR or PMS. This value must match the port administered on the adjunct, PC, or terminal server that is at the remote end of this connection. |
| 0             | Default for System Management applications.   |

**Service Type**

The service provided.

| Valid Entry | Usage  |
|-------------|--|
| AESVCS      | AE Services.   |
| CBC         | The trunk is reserved for outgoing use only to enhance Network Call Redirection. |

| Valid Entry | Usage   |
|-------------|---|
| CDR1, CDR2  | Either the primary or secondary CDR device connects over a TCP/IP link. |
| PMS         | Property Management System.   |
| PMS_JOURNAL | The PMS journal printer connects over a TCP/IP link.                    |
| PMS_LOG     | The PMS log printer connects over a TCP/IP link.                        |
| SAT         | System administration terminal.   |
| SYS_PRINT   | The system printer connects over a TCP/IP link.                         |

**IP Services: page 3**

Enables reliable protocol for TCP/IP links, and establishes other session-layer parameters. Available only if CDR1, CDR2, PMS\_JOURNAL, or PMS\_LOG is administered for the **Service Type**.

**Connectivity Timer**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 255    | The amount of time in seconds that the link can be idle before Communication Manager sends a connectivity message to ensure the link is still up. |

**Packet Resp Timer**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 255    | The number of seconds to wait from the time a packet is sent until a response (acknowledgement) is received from the far-end, before trying to resend the packet. |

**Reliable Protocol**

Enables or disables reliable protocol over this link. If enabled, uses reliable protocol if the adjunct on the far end of the link supports it.

**Service Type**

The service type for establishing parameters.

| Valid Entry | Usage  |
|-------------|--|
| CDR1, CDR2  | Connects either the primary or secondary CDR device over a TCP/ IP link. |
| PMS_JOURNAL | Connects the PMS journal printer over a TCP/IP link.                     |
| PMS_LOG     | Connects the PMS log printer over a TCP/IP link.                         |

**Session Connect Message Cntr**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 5      | The number of times Communication Manager tries to establish a connection with the far-end adjunct. |

**SPDU Cntr**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 5      | The number of times Communication Manager transmits a unit of protocol data before generating an error. |

**IP Services: page 4**

Creates symbolic name and password pairs for all AE Services servers that are allowed to connect to Communication Manager. Available only if the **Service Type** is AESVCS.

**Enabled**

Enables or disables the AE Services server.

**Password**

A password for future access. Accepts 12 to 16 alphanumeric characters and must contain at least one alpha character and one numeric character.

**AE Services Server**

A valid AE Services Server name. The name must match the AE Services server machine name. Each name must be unique.

**Server ID**

| Valid Entry | Usage                               |
|-------------|-------------------------------------|
| 1 to 16     | The number assigned to this server. |

**Status**

| Valid Entry | Usage   |
|-------------|---|
| idle        | The AE Services server is connected to Communication Manager.     |
| in-use      | The AE Services server is not connected to Communication Manager. |
| blank       | No AE Server is administered.                                     |

**ISDN Numbering Calling Party Number Conversion for Tandem Calls**

This screen administers calling party number formats for tandem calls.

Tandem calls that route to the public network cannot always provide the correct calling party information, resulting in loss of caller ID information. Communication Manager provides a way of modifying the calling party number on a tandem call that lands in the public network.

To generate a calling party number for the public network, the system compares the incoming calling party number to the sets of calling party lengths, calling party prefixes, and trunk groups. When a match is found, the calling party number is constructed by deleting digits identified in the **Delete** field on this screen, and then inserting the digits specified in the **Insert** field. The numbering format specified in the **Format** field is used to determine the encoding of the **NPI** and **TON** fields for the calling party number.

The fields on this screen are available only if **Modify Tandem Calling Number** for the ISDN trunk group is enabled.

 **Note:**

The Calling Party Number Conversion for Tandem Calls screen does not update the Calling Party Number in an NCA-TSC SETUP message. Such updates might come in a QSIG Message Waiting Indication message from a Voice Mail adjunct.

Example command: `change tandem-calling-party-num`

**Related topics:**

[Delete](#) on page 720

[Insert](#) on page 720

[Number Format](#) on page 721

[Modify Tandem Calling Number](#) on page 742

**CPN Len**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 15     | The total number of digits in the calling party number. |
| blank       | Left blank when deleting an entry. This is the default. |

**CPN Prefix**

The prefix of the tandem calling party number. Accepts up to 15 digits.

If left blank, a specific calling party number digit string match is not required, provided other matching criteria for tandem calling party number modification are met. This is the default.

**Delete**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 15     | The digits deleted when modifying the tandem calling party number.                 |
| all         | All digits are deleted.  |
| blank       | No digits are deleted from the received calling party number. This is the default. |

**Insert**

The digits inserted when modifying the tandem calling party number. Accepts up to 15 digits.

If left blank, the received calling party number is not prefixed with any digits. This is the default.

## Number Format

| Valid Entry   | Usage   |
|---|---|
| intl-pub,<br>lev0-pvt,<br>lev1-pvt,<br>lev2-pvt,<br>locl-pub,<br>natl-pub,<br>pub-unk,<br>unk-unk | The numbering format to use in modifying the tandem calling party number. |
| blank   | The numbering format information is not modified.                         |

### Trk Grp(s)

An ISDN trunk group number, or a range (x to y) of group numbers.

If blank, all trunk groups are valid provided **Modify Tandem Calling Number** is enabled for the ISDN Trunk Group. This is the default.

#### Related topics:

[Modify Tandem Calling Number](#) on page 742

## ISDN Trunk Group

Assigns an Integrated Services Digital Network (ISDN) trunk group that supports the ISDN and Call-by-Call Service Selection service selection features. The trunk group provides end-to-end digital connectivity and supports a wide range of services including voice and non-voice services, to which users have access by a limited set of CCITT-defined, standard multipurpose interfaces.

The ISDN trunk group can contain ISDN-PRI or ISDN-BRI interfaces. However, it is not possible to use the two types of interfaces in the same trunk groups. The type of interface is chosen when the trunk members are assigned to the trunk group.

When ISDN-PRI interfaces are used on ISDN trunk groups, they can also be used to support the Wideband Switching feature. This is intended to work with the H0 (384 Kbps), H11 (1536 Kbps), H12 (1920 Kbps), and NXDS0 (128 to 1984 Kbps) data services, and to support high-speed video conferencing and data applications.

Example command: `add trunk-group n`, where *n* is the trunk group number.

### ISDN Trunk Group: page 1

#### **Auth Code**

If enabled, users are required to tandem a call through an AAR or ARS route pattern. The code will be required even if the facility restriction level of the incoming trunk group is normally sufficient to send the call out over the route pattern. This field affects the level of security for tandemed outgoing calls.

Available only for incoming or two-way trunk groups and if **Authorization Codes** are enabled for the system.

**Related topics:**

[Direction](#) on page 724

[Authorization Codes](#) on page 944

**Busy Threshold**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 255    | The number of trunks that must be busy to alert attendants to control access to outgoing and two-way trunk groups during periods of high use. When the threshold is reached and the warning lamp for that trunk group lights, the attendant can activate trunk group control: internal callers who dial out using a trunk access code are connected to the attendant. Calls handled by AAR and ARS route patterns go out normally. |

**Carrier Medium**

The type of transport medium interface used for the ISDN trunk group.

| Valid Entry | Usage  |
|-------------|--|
| ATM         | The trunk is implemented via the ATM Interface circuit pack. Available only if ATM trunking is enabled for the system. |
| H.323       | The trunk is implemented as an H.323 trunk group.  |
| PRI/BRI     | The trunk is implemented as a standard DS1 or BRI interface.   |

**Related topics:**

[Local Country Code](#) on page 605

[International Access Code](#) on page 605

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

[SBS](#) on page 744

[Asynch. Transfer Mode \(ATM\) Trunking](#) on page 943

**CDR Reports**

| Valid Entry | Usage  |
|-------------|--|
| y           | All outgoing calls on this trunk group generate call detail records. If <b>Record Outgoing Calls Only</b> is disabled for CDR, incoming calls on this trunk group also generate call detail records. |
| n           | Calls over this trunk group do not generate call detail records.   |

| Valid Entry    | Usage   |
|----------------|---|
| r (ring-intvl) | <p>CDR records are generated for both incoming and outgoing calls. In addition, the following ringing interval CDR records are generated:</p> <ul style="list-style-type: none"> <li>• <b>Abandoned calls:</b> The system creates a record with a condition code of “H” indicating the time until the call was abandoned.</li> <li>• <b>Answered calls:</b> The system creates a record with a condition code of “G” indicating the interval from start of ring to answer.</li> <li>• <b>Calls to busy stations:</b> The system creates a record with a condition code of “ I ” indicating a recorded interval of 0.</li> </ul> |

**Related topics:**

[Record Outgoing Calls Only](#) on page 474

**Charge Advice**

Determines how to accumulate and access charge information about a call. Requires that **CDR Reports** be enabled before changing this field from its default of none. Receiving Advice of Charge during the call affects system performance because of the increased ISDN message activity on the signaling channel, which might reduce the maximum call capacity.

| Valid Entry       | Usage  |
|-------------------|--|
| none              | The system does not to collect Advice of Charge information for this trunk group.                                      |
| automatic         | The public network sends Advice of Charge information automatically.   |
| end-on-request    | Communication Manager requests charge information with each call, and you receive only the final call charge.          |
| during-on-request | Communication Manager requests charge information with each call, and charges display during and at the end of a call. |

**COR**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 995    | The Class of Restriction (COR) for the trunk group. Classes of restriction control access to trunk groups, including trunk-to-trunk transfers. Decisions regarding the use of Class of Restriction (COR) and Facility Restriction Levels (FRLs) should be made with an understanding of their implications for allowing or denying calls when AAR/ARS/WCR route patterns are accessed. |

 **Tip:**

Remember that FRLs are assigned to classes of restriction. Even if two trunk groups have classes of restriction that allow a connection, different facility restriction levels might prevent operations such as off-net call forwarding or outgoing calls by remote access users.

**Dial Access**

Controls whether users can route outgoing calls through an outgoing or two-way trunk group by dialing its trunk access code. Allowing dial access does not interfere with the operation of AAR/ARS.



**Security alert:**

Calls dialed with a trunk access code over WATS trunks bypass AAR/ARS and are not restricted by facility restriction levels. For security, leave this field disabled unless dial access is needed to test the trunk group.

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows users to access the trunk group by dialing its access code.   |
| n           | Does not allow users to access the trunk group by dialing its access code. Attendants can still select this trunk group with a <b>Trunk Group Select</b> button. |

**Direction**

The direction of the traffic on this trunk group.

Available for all trunk groups except DID and CPE.

| Valid Entry | Usage  |
|-------------|--|
| incoming    | Traffic on this trunk group is incoming.   |
| outgoing    | Traffic on this trunk group is outgoing  |
| two-way     | Traffic on this trunk group is incoming and outgoing. Required for <b>Network Call Redirection</b> . |

**Related topics:**

- [Answer Supervision Timeout](#) on page 733
- [Disconnect Supervision-Out](#) on page 735
- [Receive Answer Supervision](#) on page 825

**Far End Test Line No.**

The number sent to the far-end’s ISDN test line extension. When the **test trunk long** command is issued, this exact number is sent to the far-end to establish a call that tests the integrity of the trunk member under test. The number does not pass through routing or undergo digit manipulation. The digits entered must be what the far-end expects. Accepts up to 15 digits.

**Example**

For an ISDN tandem trunk, the far-end test number should be a seven-digit ETN (Electronic Tandem Network) number.

**Group Name**

A unique name that provides information about the trunk group. Accepts up to 27 characters.

This field should contain names that identify the vendor and function of the trunk group rather than the group type (DID, WATS).

 **Note:**

Supported by Unicode language display for the 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones. Unicode is also an option for the 2420J telephone when the **Display Character Set** is katakana. For more information on the 2420J, see *2420 Digital Telephone User's Guide*.

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Related topics:**

[Display Character Set](#) on page 938

**Group Number**

The trunk group number.

 **Note:**

For trunk groups connecting two servers in Distributed Communication System networks, assign the same group number on both servers.

**Group Type**

The type of trunk group. The fields that are displayed and available might change according to the trunk group type selected.

| Valid Entry | Usage  |
|-------------|--|
| Access      | Used to connect satellite servers to the main switch in Electronic Tandem Networks (ETN). Access trunks do not carry traveling class marks (TCM) and thus allow satellite callers unrestricted access to out-dial trunks on the main server. This entry allows Inband ANI. |
| APLT        | Advanced Private Line Termination (APLT) trunks. Used in private networks. This entry allows Inband ANI.   |
| CAMA        | Used to route emergency calls to the local community's Enhanced 911 systems.   |
| CO          | Typically used to connect Communication Manager to the local telephone company central office, but can also connect adjuncts such as external paging systems and data modules.   |
| CPE         | Used to connect adjuncts, such as paging systems and announcement or music sources, to the server running Communication Manager.   |
| DID         | Used to direct callers directly to individuals within an organization without going through an attendant or some other central point. This entry allows Inband ANI.  |

| Valid Entry | Usage   |
|-------------|---|
| DIOD        | Two-way trunks that are used to transmit dialed digits in both directions. In North America, tie trunks are used for applications that require two-way transmission of dialed digits. This entry allows Inband ANI.   |
| DMI-BOS     | Digital Multiplexed Interface - Bit-Oriented Signaling (DMI-BOS) trunks allow communication with systems using DMI-BOS protocol. This entry also allows Inband ANI.   |
| FX          | A local telephone company central office (CO) trunk that connects the server running Communication Manager directly to a CO outside the local exchange area. Used to reduce long-distance charges if the organization averages a high volume of long-distance calls to a specific area code.  |
| ISDN        | <p>Used when digital trunks are needed that can integrate voice, data, and video signals and provide the bandwidth needed for applications such as high-speed data transfer and video conferencing. ISDN trunks can also efficiently combine multiple services on one trunk group.</p> <p>Also used for <b>Network Call Transfer</b>.</p> <p> <b>Note:</b><br/>Available only if <b>ISDN-PRI, ISDN-BRI Trunks</b>, or both have been enabled for the system.</p> |
| RLT         | Used with Centralized Attendant Service in a private network.   |
| SIP         | <p>Used to connect a server running Communication Manager to a SIP Enablement Services (SES) home server, or to connect two Communication Manager servers.</p> <p> <b>Note:</b><br/>The Automatic CallBack, Priority Calling, and Whisper Page features do not work correctly if each of the call's parties is using a SIP endpoint administered on and managed by a different instance of Communication Manager.</p>  |
| Tandem      | Used to connect tandem nodes in a private network. This entry allows Inband ANI.  |
| Tie         | Used to connect a server running Communication Manager to a local telephone company central office or to another server or switch in a private network. Tie trunks transmit dialed digits with both outgoing and incoming calls. This entry also allows Inband ANI.   |
| WATS        | Used to reduce long-distance bills when your organization regularly places many calls to a specific geographical area in North America. Outgoing WATS service allows calls to certain areas ("WATS band") for a flat monthly charge. Incoming WATS trunks allow toll-free calling to customers and employees.   |

**Related topics:**

[Local Country Code](#) on page 605

[International Access Code](#) on page 605

[Carrier Medium](#) on page 722  
[Supplementary Service Protocol](#) on page 737  
[SBS](#) on page 744  
[Path Replacement](#) on page 750  
[Call Still Held](#) on page 821  
[ISDN-BRI Trunks](#) on page 947  
[ISDN-PRI](#) on page 947

### ***Incoming Calling Number - Format***

The TON/NPI encoding applied to CPN information modified by the CLI Prefix feature. This encoding does not apply to calls originating locally.

If this field is blank, Communication Manager passes on the encoding received in the incoming setup message. If the incoming setup message did not contain CPN information and digits are added, the outgoing message will contain these digits. If a numbering format is not administered in this case, the value defaults to pub-unk. If the numbering format is administered as unknown, the trunk group is modified to unk-unk encoding of the TON/NPI. Therefore, this field also must contain a value other than unknown.

The values for this field map to the Type of Numbering (TON) and Numbering Plan Identifier (NPI) values shown below.

| Valid Entry | Type of Numbering (TON) | Numbering Plan Identifier (NPI) |
|-------------|-------------------------|---------------------------------|
| blank       | incoming TON unmodified | incoming NPI unmodified         |
| natl-pub    | national(2)             | E.164(1)                        |
| intl-pub    | international(1)        | E.164(1)                        |
| locl-pub    | local/subscriber(4)     | E.164(1)                        |
| pub-unk     | unknown(0)              | E.164(1)                        |
| lev0-pvt    | local(4)                | Private Numbering Plan - PNP(9) |
| lev1-pvt    | Regional Level 1(2)     | Private Numbering Plan - PNP(9) |
| lev2-pvt    | Regional Level 2(1)     | Private Numbering Plan - PNP(9) |
| unk-unk     | unknown(0)              | unknown(0)                      |

### **Related topics:**

[Numbering Format](#) on page 742  
[Format](#) on page 999

**Incoming Calling Number Insert**

| Valid Entry            | Usage  |
|------------------------|--|
| 0 to 9<br>all<br>blank | The number of digits inserted in the calling party number for all incoming calls on this trunk group. Accepts up to 15 characters. |

**Member Assignment Method**

Available only if the **Carrier Medium** is H.323.

| Valid Entry | Usage  |
|-------------|--|
| manual      | Users manually assign trunk members to a signaling group. This is the default. |
| auto        | The system automatically generates members to a specific signaling group.      |

**Related topics:**

[Carrier Medium](#) on page 722

**Number of Members**

Available only if the **Carrier Medium** is H.323 and the **Member Assignment Method** is auto.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 255    | The number of virtual trunk members automatically assigned to the signaling group. Default is 0. |

**Related topics:**

[Carrier Medium](#) on page 722

[Member Assignment Method](#) on page 728

[Signaling Group](#) on page 730

**Outgoing Display**

Allows display telephones to show the name and number of the trunk group used for an outgoing call before the call is connected.

| Valid Entry | Usage                                     |
|-------------|---|
| y           | Displays the trunk group name and number. |
| n           | Displays the digits the caller dials.     |

**Queue Length**

Available only for outgoing or two-way trunk groups.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 100    | The number of outgoing calls that can wait in queue when all trunks in a trunk group are busy. Calls wait in queue in the order in which they were |

| Valid Entry | Usage  |
|-------------|--|
|             | made. If a queue is administered, a caller hears a confirmation tone when no trunk is available for the outgoing call. The caller can then hang up and wait; when a trunk becomes available, Communication Manager calls the extension that placed the original call. Communication Manager remembers the number the caller dialed and automatically completes the call. |
| 0           | Callers receive a busy signal when no trunks are available. Use for DCS trunks.  |

**Related topics:**

[Direction](#) on page 724

**Service Type**

The service for which this trunk group is dedicated. In addition to the predefined services or features listed as valid entries, any previously administered user-defined Network Facility **Facility Type** of 0 (feature) or 1 (service) is allowed.

| Valid Entry | Usage  |
|-------------|--|
| access      | A tie trunk giving access to an Electronic Tandem Network.   |
| accunet     | ACCUNET Switched Digital Service — part of ACI (AT&T Communications ISDN) phase 2.   |
| cbc         | Call-by-Call service — provides different dial plans for different services on an ISDN trunk group. Indicates this trunk group is used by the Call-By-Call Service Selection feature.  |
| dmi-mos     | Digital multiplexed interface — message-oriented signaling.  |
| i800        | International 800 Service — allows a subscriber to receive international calls without a charge to the call originating party.   |
| inwats      | INWATS — provides OUTWATS-like pricing and service for incoming calls.   |
| lds         | Long-Distance Service — part of ACI (AT&T Communications ISDN) phase 2.  |
| megacom     | MEGACOM Service — an AT&T communications service that provides unbanded long-distance services using special access (switch to 4ESS switch) from an AT&T communications node.  |
| mega800     | MEGACOM 800 Service — an AT&T communications service that provides unbanded 800 service using special access (4ESS switch to switch) from an AT&T communications node.   |
| multiquest  | AT&T MULTIQUEST Telecommunications Service — dial 700 service. A terminating-user's service that supports interactive voice service between callers at switched-access locations and service provides directly connected to the AT&T Switched Network (ASN). |
| operator    | Network Operator — provides access to the network operator.  |

| Valid Entry  | Usage   |
|--------------|---|
| outwats-bnd  | OUTWATS Band — WATS is a voice-grade service providing both voice and low speed data transmission capabilities from the user location to defined service areas referred to as bands; the widest band is 5.  |
| public-ntwrk | Public network calls — It is the equivalent of CO (outgoing), DID, or DIOD trunk groups. If Service Type is public-ntwrk, <b>Dial Access</b> can be enabled.  |
| sddn         | Software Defined Data Network — provides a virtual private line connectivity via the AT&T switched network (4ESS switches). Services include voice, data, and video applications. These services complement the SDN service. Do not use for DCS with Rerouting. |
| sdn          | Software Defined Network (SDN) — an AT&T communications offering that provides a virtual private network using the public switched network. SDN can carry voice and data between customer locations as well as off-net locations.                               |
| sub-operator | Presubscribed Common Carrier Operator — provides access to the presubscribed common carrier operator.   |
| tandem       | Tandem tie trunks integral to an ET.  |
| tie          | Tie trunks — general purpose.   |
| wats-max-bnd | Maximum Banded Wats — a WATS-like offering for which a user's calls are billed at the highest WATS band subscribed to by users.   |

**Related topics:**

[Facility Type](#) on page 812

**Signaling Group**

Available only if the **Carrier Medium** is H.323 and the **Member Assignment Method** is auto.

| Valid Entry       | Usage   |
|-------------------|---|
| 1 to 650<br>blank | Assigned H.323 or SIP Enablement Services (SES) signaling group number. |

**Related topics:**

[Carrier Medium](#) on page 722

[Member Assignment Method](#) on page 728

**TAC**

The trunk access code (TAC) that must be dialed to access the trunk group. A different TAC must be assigned to each trunk group. CDR reports use the TAC to identify each trunk group. The characters “\*” and “#” can be used as the first character in a TAC. Accepts a one- to four-digit number.

**TestCall BCC**

The Bearer Capability Code (BCC) used for the ISDN test call.

| Valid Entry | Usage               |
|-------------|---------------------|
| 0           | Voice               |
| 1           | Mode 1              |
| 2           | Mode 2 Asynchronous |
| 4           | Mode 0              |

### Testcall ITC

Controls the encoding of the Information Transfer Capability (ITC) codepoint of the bearer capability Information Element (IE) in the `SETUP` message when generating an ISDN test call.

 **Note:**

The ISDN Testcall feature has no routing, so a testcall is never blocked due to an incompatible ITC.

| Valid Entry | Usage        |
|-------------|--------------|
| rest        | Restricted   |
| unre        | Unrestricted |

### Testcall Service

The call-by-call selection for an ISDN test call. Available only if the **Service Type** is cbc. Not available for **Facility Type** 0 (feature), 1 (service), or 3 (outgoing) that is defined by users.

| Valid Entry | Usage   |
|-------------|---|
| access      | A tie trunk giving access to an Electronic Tandem Network.  |
| accunet     | ACCUNET Switched Digital Service — part of ACI (AT&T Communications ISDN) phase 2.  |
| cbc         | Call-by-Call service — provides different dial plans for different services on an ISDN trunk group. Indicates this trunk group is used by the Call-By-Call Service Selection feature. |
| dmi-mos     | Digital multiplexed interface — message-oriented signaling.   |
| i800        | International 800 Service — allows a subscriber to receive international calls without a charge to the call originating party.  |
| inwats      | INWATS — provides OUTWATS-like pricing and service for incoming calls.  |
| lds         | Long-Distance Service — part of ACI (AT&T Communications ISDN) phase 2.   |
| megacom     | MEGACOM Service — an AT&T communications service that provides unbanded long-distance services using special access (switch to 4ESS switch) from an AT&T communications node.         |

| Valid Entry  | Usage  |
|--------------|--|
| mega800      | MEGACOM 800 Service — an AT&T communications service that provides unbanded 800 service using special access (4ESS switch to switch) from an AT&T communications node.   |
| multiquest   | AT&T MULTIQUEST Telecommunications Service — dial 700 service. A terminating-user's service that supports interactive voice service between callers at switched-access locations and service provides directly connected to the AT&T Switched Network (ASN). |
| operator     | Network Operator — provides access to the network operator.  |
| outwats-bnd  | OUTWATS Band — WATS is a voice-grade service providing both voice and low speed data transmission capabilities from the user location to defined service areas referred to as bands; the widest band is 5.   |
| public-ntwrk | Public network calls — It is the equivalent of CO (outgoing), DID, or DIOD trunk groups. If Service Type is public-ntwrk, <b>Dial Access</b> can be enabled.   |
| sdn          | Software Defined Network (SDN) — an AT&T communications offering that provides a virtual private network using the public switched network. SDN can carry voice and data between customer locations as well as off-net locations.                            |
| sub-operator | Presubscribed Common Carrier Operator — provides access to the presubscribed common carrier operator.  |
| tandem       | Tandem tie trunks integral to an ET.   |
| tie          | Tie trunks — general purpose.  |
| wats-max-bnd | Maximum Banded Wats — a WATS-like offering for which a user's calls are billed at the highest WATS band subscribed to by users.  |

**Related topics:**

[Service Type](#) on page 729

[Facility Type](#) on page 812

**TN**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 100    | <p>A tenant partition number assigned to this trunk group.</p> <p> <b>Tip:</b><br/>If an unassigned tenant partition number is used, the system accepts the entry but calls cannot go to the trunk group.</p> |

**Usage Alloc**

If enabled, allocates service provided by the trunk group and enhances Network Call Redirection. Available only if the ISDN Trunk Group **Service Type** is cbc.

**Related topics:**

[Service Type](#) on page 729

**ISDN Trunk Group: page 2****Administer Timers**

Enables or disables administration of timers on this trunk group. The default for the ISDN trunk group type is disabled. All other trunk group types are enabled by default.

Available for all trunk group types *except* cpe, h.323, and sip.

**Related topics:**

[Group Type](#) on page 725

**Answer Supervision Timeout**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 250    | The number of seconds Communication Manager waits before it acts as though answer supervision has been received from the far-end. During a cut-through operation, timing begins after each outgoing digit is sent and timing ceases after the far-end sends answer supervision. On senderized operation, the timer begins after the last digit collected is sent. |

 **Note:**

This field's setting does not override answer supervision sent from the network or from DS1 port circuit timers.

**Related topics:**

[Administer Timers](#) on page 733

[Receive Answer Supervision](#) on page 825

**Bit Rate**

| Valid Entry                                  | Usage  |
|--|--|
| 300<br>1200<br>2400<br>4600<br>9600<br>19200 | The baud rate used by pooled modems. The speed of the fastest modem that uses this ISDN trunk group. |

**Charge Advice**

Determines how to accumulate and access charge information about a call. Requires that **CDR Reports** be enabled before changing this field from its default of none. Receiving Advice of Charge during the call affects system performance because of the increased ISDN message activity on the signaling channel, which might reduce the maximum call capacity.

| Valid Entry       | Usage  |
|-------------------|--|
| none              | The system does not to collect Advice of Charge information for this trunk group.                                      |
| automatic         | The public network sends Advice of Charge information automatically.   |
| end-on-request    | Communication Manager requests charge information with each call, and you receive only the final call charge.          |
| during-on-request | Communication Manager requests charge information with each call, and charges display during and at the end of a call. |

**Codeset to Send Display**

Defines the codeset for sending the information element for display. The value depends on the type of server or switch used for the connection.

| Valid Entry | Usage   |
|-------------|---|
| 0           | CCITT (non-Communication Manager equipment).  |
| 6           | Any other than CCITT or System 85 R2V4, 4E11. |
| 7           | System 85 R2V4, 4E11.                         |

**Codeset to Send National IEs**

The codeset for sending the information element (IE) for national IEs. National IEs include all IEs previously sent only in code set 6 (such as DCS IE). Now these national IEs, including Traveling Class Marks (TCMs) and Lookahead Interflow (LAI), can be sent in code set 6 or 7. The value depends on the type of server/switch to which the user is connected.

| Valid Entry | Usage  |
|-------------|--|
| 6           | Other types.   |
| 7           | System 85 R2V4, 4E11, or newer Avaya S8XXX Server types. |

 **Note:**

A Traveling Class Mark (that is, the user’s FRL or the user’s trunk group FRL) is passed between tandem nodes in an ETN in the setup message only when the **Service Type** is tandem. It then is used by the distant tandem switch to permit access to facilities consistent with the originating user’s privileges.

**CONNECT Reliable When Call Leaves ISDN**

Available only if **Group Type** is ISDN. The value tells the Communication Manager server whether a CONNECT received on an outgoing call that is not end-to-end ISDN is a reliable indication that the far end has answered the call.

| Valid Entry | Usage                                       |
|-------------|---|
| y           | CONNECT is considered as a reliable answer. |

| Valid Entry | Usage   |
|-------------|---|
| n           | If a call is not end-to-end ISDN, the CONNECT message is considered unreliable. That is, it may be the result of a timer expiring. If the call was originated by a Call Center adjunct, a Call Classifier may be used instead to determine whether the call has been answered. This is the default (works as before). |

### **Digit Handling (in/out)**

| Valid Entry  | Usage  |
|--|--|
| enbloc/enbloc<br>enbloc/overlap<br>overlap/enbloc<br>overlap/overlap | Defines whether overlap receiving and overlap sending features are enabled. enbloc disables overlap receiving and overlap sending. The first field value indicates digit receiving and the second value indicates digit sending. |

### **Digital Loss Group**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 19     | Determines which administered two-party row in the loss plan applies to this trunk group if the call is carried over a digital signaling port in the trunk group. If values other than 18 or between 11 and 15 are administered, a warning message displays stating that the loss group may not be appropriate for this trunk group. |

### **Disconnect Supervision-Out**

Indicates whether Communication Manager receives disconnect supervision for outgoing calls over this trunk group. Available for outgoing or two-way trunk groups.

| Valid Entry | Usage   |
|-------------|---|
| y           | Allows trunk-to-trunk transfers involving trunks in this group. The far-end sends a release signal when the called party releases an outgoing call, and the far-end is responsible for releasing the trunk. Enhances Network Call Redirection. Available only if <b>Answer Supervision Timeout</b> is 0 and <b>Receive Answer Supervision</b> is enabled. |
| n           | The far-end server or switch does not provide a release signal, the hardware cannot recognize a release signal, or timers are preferred for disconnect supervision on outgoing calls. Prevents trunk-to-trunk transfers involving trunks in this group.   |

#### **Caution:**

Verify that the far-end server or switch provides answer supervision and disconnect supervision. Most public networks do not provide disconnect supervision over analog trunks. Check with the network services provider.

#### **Related topics:**

[Direction](#) on page 724

[Answer Supervision Timeout](#) on page 733

[Receive Answer Supervision](#) on page 825

**Duplex**

 **Note:**

Even if the trunk group supports full-duplex transmission, other equipment in a circuit might not.

| Valid Entry | Usage   |
|-------------|---|
| full        | Allows simultaneous two-way transmission, which is most efficient. Recommended in most cases. |
| half        | Supports only one transmission direction at a time.   |

**Group Type**

Displays the type of trunk group.

**Related topics:**

[Group Type](#) on page 725

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

**Max Message Size to Send**

| Valid Entry              | Usage   |
|--------------------------|---|
| 128<br>244<br>256<br>260 | The maximum number of bytes of an ISDN message for Communication Manager. |

The following table indicates the expected ISDN-PRI message size from several Lucent Technologies and Avaya Inc. products.

| Products         | Message Length (octets) Received |
|------------------|----------------------------------|
| 4ESS (4E11)      | 256                              |
| 4ESS (4E13)      | 256                              |
| 4ESS (4E14)      | 256                              |
| 5ESS (5E4)       | 244                              |
| 5ESS (5E5)       | 244                              |
| 5ESS (5E6)       | 244                              |
| System 75 (all)  | 260                              |
| System 85 (R2V4) | 128                              |

| Products         | Message Length (octets) Received |
|------------------|----------------------------------|
| System 85 (R2V5) | 260                              |
| System 85 (R2V6) | 260                              |

### Supplementary Service Protocol

The supplementary service protocol to use for services over this trunk group. Supplementary service protocols are mutually exclusive.

| Valid Entry | Usage   |
|-------------|---|
| a           | National.   |
| b           | ISO/ETSI QSIG Private Network. Also used for SBS signaling trunks.  |
| c           | ETSI public network.  |
| d           | European Computer Manufacturer's Association (ECMA) QSIG private network (supports only Name Identification and Additional Network Feature Transit Counter (ANF-TC)). |
| e           | DCS with Rerouting. Do not use with <b>Service Type</b> of dmi-mos or sddn.   |
| f           | ISDN Feature Plus Public network feature plus signaling.  |
| g           | ANSI.   |

#### Related topics:

[Local Country Code](#) on page 605

[International Access Code](#) on page 605

[Carrier Medium](#) on page 722

[Group Type](#) on page 725

[SBS](#) on page 744

### Synchronization



#### Caution:

Do not change this field without the assistance of Avaya or the network service provider.

| Valid Entry   | Usage   |
|---------------|---|
| async<br>sync | Determines whether the trunk group uses synchronous or asynchronous communications. |

### Trunk Hunt

Defines the trunk hunt search order. Communication Manager performs a trunk hunt when searching for available channels within a facility in an ISDN trunk group. The search can be administered per ISDN-PRI trunk group, but it infers the direction of search within all ISDN-PRI facilities (or portions of those facilities) administered within the trunk group.

| Valid Entry | Usage  |
|-------------|--|
| ascend      | Enables a linear trunk hunt search from the lowest to highest numbered channels. All trunks within an ISDN trunk group are selected without regard to the order in which trunks are administered within the trunk group.   |
| cyclical    | Enables a circular trunk hunt based on the sequence the trunks were administered within the trunk group. When using ISDN-BRI interfaces, only cyclical is allowed. The cyclical option cannot be set if the trunk group using ISDN-PRI interfaces is to be used for Wideband operations. |
| descend     | Enables a linear trunk hunt search from the highest to lowest numbered channels. All trunks within an ISDN trunk group are selected without regard to the order in which trunks are administered within the trunk group.   |

**Related topics:**

[Wideband Support](#) on page 748

**Trunk Type**

The type of trunk.

**Related topics:**

[Trunk Type \(in/out\)](#) on page 991

**ISDN Trunk Group: page 3**

***Abandoned Call Search***

Indicates whether this trunk group conducts an Abandoned Call Search to identify ghost calls. Abandoned Call Search is designed to work with analog ground-start local telephone company central office (CO) trunks that do not provide disconnect supervision. The CO must support Abandoned Call Search for the feature to work properly. If the CO provides disconnect supervision, the Abandoned Call Search feature is not needed.

Available only for ground-start type trunks.

**Related topics:**

[Trunk Type](#) on page 826

***ACA Assignment***

Indicates whether Automatic Circuit Assurance (ACA) measurements are taken for this trunk group.

***Apply Local Ringback***

Enables or disables local ringback tone to the caller. If enabled, local ringback is removed when the call is connected. Available only if the **Carrier Medium** is PRI\_BRI.

**Related topics:**

[Carrier Medium](#) on page 722

**BSR Reply-best DISC Cause Value**

Servers running Communication Manager that are polled as resources in a Best Service Routing application return data to the polling server in the ISDN DISC message. Since some cause values do not work over some networks, this field sets the cause value that the server returns in response to a BSR status poll. If this field is set incorrectly, incoming status poll calls over this trunk group are dropped before any data is returned to the polling server or switch.

Available only if **UUI IE Treatment** is shared.

| Valid Entry | Usage   |
|-------------|---|
| 31          | Normal-unspecified. This value is almost always used. |
| 17          | User-busy   |
| 16          | Normal-call-clearing.                                 |

**Caution:**

In most cases, this field is set to the appropriate value during installation. Do not change this field without the assistance of Avaya or your network service provider.

**Related topics:**

[UUI IE Treatment](#) on page 748

**Charge Conversion**

Available only for outgoing or two-way CO, DIOD, FX, and WATS trunk groups.

| Valid Entry    | Usage  |
|----------------|--|
| 1 to 64<br>500 | Communication Manager multiplies the number of charge units by the value of this field and displays it as a currency amount. Without a value in this field, Communication Manager displays the number of charge units without converting it to currency. |

**Related topics:**

[Direction](#) on page 724

[Trunk Direction](#) on page 825

**Currency Symbol**

The symbol that appears on telephone displays before the charge amount. Accepts from one to three characters. Leading and embedded spaces count as characters.

Available only for outgoing or two-way CO, DIOD, FX, and WATS trunk groups.

**Related topics:**

[Direction](#) on page 724

[Trunk Direction](#) on page 825

**Data Restriction**

Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be

changed by the telephone user. Cannot be assigned if **Auto Answer** is administered as all or acd. If enabled, whisper page to this station is denied.

**Related topics:**

[Auto Answer](#) on page 61

**DCS Signaling**

Available only if the trunk is used for DCS and the **Service Type** is anything except dmi-mos or sddn.

| Valid Entry | Usage   |
|-------------|---|
| d-chan      | The means used to send the DCS message. DCS over D-channel is not supported on trunk groups containing ISDN-BRI interfaces. |

**Related topics:**

[Service Type](#) on page 729

[Used for DCS](#) on page 1023

**Decimal Point**

The appropriate representation for a decimal point as it appears on telephone displays. Available only with outgoing or two-way CO, DIOD, FX, and WATS trunk groups.

 **Note:**

If the received charge contains no decimals, no decimal point is displayed (that is, the administered decimal point is ignored for charge information received with no decimals). On a QSIG trunk group, unlike other trunk groups, the **Decimal Point** field does not drive whether a decimal point appears on the calling display. Instead, it tells what symbol should be displayed if the QSIG AOC received has a 1/10 or 1/100 or 1/1000 Multiplier.

| Valid Entry | Usage   |
|-------------|---|
| comma       | If the received charge contains decimals, the charge is displayed at the calling endpoint's display with a comma as the decimal point. Divides the charge value by 100.                       |
| period      | This is the default. If the received charge contains decimals, the charge is displayed at the calling endpoint's display with a period as the decimal point. Divides the charge value by 100. |
| none        | No decimal point is displayed.  |

**Related topics:**

[Charge Advice](#) on page 723

[Direction](#) on page 724

[Trunk Direction](#) on page 825

**DS1 Echo Cancellation**

Enables or disables echo cancellation on a per port basis. If enabled, reduces voice call echo.

**Note:**

Changes to the DS1 Echo Cancellation field do not take effect until one of the following occurs:

- Port is busied-out or released.
- Trunk group is busied-out or released.
- SAT command test trunk group is performed.
- Periodic maintenance runs.

**DSN Term**

Enables or disables the trunk group as a DSN termination telephone. The default is disabled.

**Maintenance Tests**

Enables or disables hourly maintenance tests on this trunk group.

Available only for aplt, isdn, sip, or tie trunk groups.

**Related topics:**

[Group Type](#) on page 725

**Maximum Size of UI IE Contents**

Available only if the **UI IE Treatment** is shared.

| Valid Entry | Usage  |
|-------------|--|
| 32 to 128   | The maximum number of bytes of user information that the network supports. |

**Related topics:**

[UI IE Treatment](#) on page 748

**Measured**

Indicates if the system transmits data for this trunk group to the Call Management System.

| Valid Entry | Usage   |
|-------------|---|
| internal    | Sends the data to the Basic Call Management System (BCMS), the VuStats data display, or both.<br>Available only if <b>BCMS (Basic)</b> or <b>VuStats</b> is enabled for the system. |
| external    | Sends the data to the CMS.  |
| both        | Collects data internally and sends it to the CMS.<br>Available only if <b>BCMS (Basic)</b> or <b>VuStats</b> is enabled for the system.   |
| none        | Trunk group measurement reports are not required.   |

**Related topics:**

[BCMS \(Basic\)](#) on page 950

[VuStats](#) on page 953

**Modify Tandem Calling Number**

Available with outgoing or two-way trunks when the **Carrier Medium** field is set to PRI/BRI or H.323, and the **Send Calling Number** field is set to enabled or restricted.

| Valid Entry      | Usage   |
|------------------|---|
| natl-intl-prefix | Adds the national or international prefixes from the Feature Related System Parameters screen when the calling party number is appropriate. |
| tandem-cpn-form  | Modifies the calling party number IE in the previously administered format specified for the Tandem Calling Party Number.                   |
| no               | Does not modify the calling party number.   |

**Related topics:**

- [Carrier Medium](#) on page 722
- [Direction](#) on page 724
- [Group Type](#) on page 725
- [Send Calling Number](#) on page 745
- [Modify Tandem Calling Number](#) on page 1014

**NCA-TSC Trunk Member**

The trunk member number whose D-channel is used to route tandem NCA-TSCs or QSIG CISCs.

**Network Call Redirection**

Whenever the **Supplementary Service Protocol** is changed, this field resets to none to prevent an inadvertent incorrect value.

Available only if **ISDN Network Call Redirection** is enabled for the system and the **Supplementary Service Protocol** is a, c, or g.

**Related topics:**

- [Supplementary Service Protocol](#) on page 737
- [ISDN-PRI](#) on page 947
- [ISDN/SIP Network Call Redirection](#) on page 947

**Network (Japan) Needs Connect Before Disconnect**

Sends an ISDN Connect message just prior to the disconnect message.

**Numbering Format**

Specifies the encoding of Numbering Plan Indicator for identification purposes in the Calling Number and/or Connected Number IEs, and in the QSIG Party Number.

Available only if **Send Calling Number** or r or the **Send Connected Number** is enabled or restricted.

| Valid Entry | Usage  |
|-------------|--|
| public      | Indicates that the number plan according to CCITT Recommendation E. 164 is used.                                     |
| unknown     | Indicates the <b>Numbering Plan Indicator</b> is unknown.  |
| private     | Indicates the <b>Numbering Plan Indicator</b> is PNP.  |
| unk-pvt     | Determines the type of number from the private numbering format, but the <b>Numbering Plan Indicator</b> is unknown. |

**Related topics:**

[Send Calling Number](#) on page 745

[Send Connected Number](#) on page 746

[Numbering-Private Format](#) on page 813

**Outgoing ANI**

The digit string sent in place of normal ANI. Overrides the normal ANI if this trunk group is used for an outgoing call with ANI. The ANI is sent exactly as administered, except for the normal truncation to seven digits for Russian ANI. This ANI override works both for calls originated in Communication Manager and calls tandemed through it. Accepts up to 15 digits.

Available only for CO, DIOD, FX, and WATS trunk groups.

**Outgoing Channel ID Encoding**

Determines whether to encode the Channel ID IE as preferred or exclusive. Available only if the **Group Type** is isdn and the **Service Type** is anything except dmi-mos or sddn. Blank is not a valid entry.

| Valid Entry | Usage  |
|-------------|--|
| preferred   | Default if <b>Used for DCS</b> is disabled or unavailable. |
| exclusive   | Default if <b>Used for DCS</b> is enabled.                 |

**Related topics:**

[Group Type](#) on page 725

[Service Type](#) on page 729

**Path Replacement Method**

Available only if **Basic Call Setup** and **Supplementary Services with Rerouting** are enabled for the system and when the **Supplementary Service Protocol** is either b or e and the **Group Type** is isdn.

| Valid Entry  | Usage  |
|--------------|--|
| better-route | Uses the most economical route; for example, the reconfigured call does not use the same trunk group as the original call. |
| always       | Always reconfigures the call regardless of the trunk group used.   |

**Related topics:**

[Group Type](#) on page 725

[Service Type](#) on page 729

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

[Basic Call Setup](#) on page 954

[Supplementary Services with Rerouting](#) on page 955

**Per Call CPN Blocking Code**

**Per Call CPN Unblocking Code**

**Replace Restricted Numbers**

Indicates whether to replace restricted numbers with administrable strings for incoming and outgoing calls assigned to the specified trunk group. If enabled, the display is replaced regardless of the service type of the trunk. Applies to BRI, PRI, H.323, and SIP trunks. Available only if the **Group Type** is isdn.

**Related topics:**

[Group Type](#) on page 725

**Replace Unavailable Numbers**

If enabled, replaces unavailable numbers with administrable strings for incoming and outgoing calls assigned to the specified trunk group. The display is replaced regardless of the service type of the trunk. Applies to BRI/PRI, H.323, and SIP Enablement Services (SES) trunks. Also applies to analog trunks if **Analog Trunk Incoming Call ID** is enabled and **Receive Analog Incoming Call ID** is set to any value except disabled. Available only if the **Group Type** is isdn or sip.

**Related topics:**

[Group Type](#) on page 725

[Analog Trunk Incoming Call ID](#) on page 942

[Receive Analog Incoming Call ID](#) on page 1017

**SBS**

Enables or disables Separation of Bearer and Signaling (SBS) for the trunk group.

Available only if the **Local Country Code** and **International Access Code** are administered for the system and when the **Supplementary Service Protocol** is b, the **Group Type** is isdn, the **Carrier Medium** is H.323, and **Dial Access** is disabled.

**Related topics:**

[Local Country Code](#) on page 605

[International Access Code](#) on page 605

[Carrier Medium](#) on page 722

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

**Send Called/Busy/Connected Number**

Specifies if the dialed number, whether called (ringing), busy (busy tone), or connected (answered) is sent on incoming or tandemed ISDN calls.

Available only if **QSIG Value-Added** is enabled for the trunk group.

| Valid Entry | Usage   |
|-------------|---|
| y           | The dialed number is sent on incoming or tandemed ISDN calls. This field must be enabled in order for the Calling Party Number of an incoming ISDN call to display at the transferred-to station after a QSIG transfer operation. If enabled, the Numbering - Public/Unknown Format is accessed to construct the actual number sent, or the Numbering - Private Format is used. |
| n           | Disables the sending of the dialed number on incoming or tandemed ISDN calls.   |
| r           | Restricted. The connected number is sent "presentation restricted".   |

**Related topics:**

[QSIG Value-Added](#) on page 751

[Numbering-Private Format](#) on page 813

[Numbering — Public/Unknown Format](#) on page 814

**Send Calling Number**

Specifies whether the calling party's number is sent on outgoing or tandemed ISDN calls.

**Note:**

The Numbering - Public/Unknown Format can override the Send Calling Number administration

| Valid Entry | Usage  |
|-------------|--|
| y           | The calling party's number is sent on outgoing or tandemed ISDN calls. If enabled, the Numbering - Public/Unknown Format is accessed to construct the actual number sent, or the Numbering - Private Format is used. |
| n           | Disables the sending of the calling party's number on outgoing or tandemed ISDN calls. If disabled, an incoming number is not tandemed out again. This applies to all Supplementary Service Protocols.               |
| r           | Restricted. The calling number is sent "presentation restricted". If set to restricted, an incoming number is marked restricted when it is tandemed out again. This applies to all Supplementary Service Protocols.  |

**Related topics:**

[Number Format](#) on page 721

[Numbering-Private Format](#) on page 813

[Numbering — Public/Unknown Format](#) on page 814

**Send Codeset 6/7 LAI IE**

If enabled, the ISDN trunk transmits information in Codeset 6/7.

If the **UUI IE Treatment** is shared, then this field should be disabled. Otherwise, the same information will be sent twice and might exceed the message size.

**Related topics:**

[UUI IE Treatment](#) on page 748

**Send Connected Number**

Specifies if the connected party's number is sent on incoming or tandemed ISDN calls.

Available only if **QSIG Value-Added** is disabled for the trunk group.

| Valid Entry | Usage   |
|-------------|---|
| y           | The connected party's number is sent on outgoing or tandemed ISDN calls. If enabled, the Numbering - Public/Unknown Format is accessed to construct the actual number sent, or the Numbering - Private Format is used. This field must be enabled for the Calling Party Number of an incoming ISDN call to display at the transferred-to station after a QSIG transfer operation. |
| n           | Disables the sending of the connected party's number on outgoing or tandemed ISDN calls. If disabled, an incoming number is not tandemed out again. This applies to all Supplementary Service Protocols.  |
| r           | Restricted. The connected number is sent "presentation restricted". If this field is set to r, an incoming number is marked restricted when it is tandemed out again. This applies to all Supplementary Service Protocols.  |

 **Note:**

The AT&T Switched Network Protocol does not support restricted displays of connected numbers. Therefore, if you administer the 1a country-protocol/ protocol-version combination for the DS1 Circuit Pack, you should not administer the Send Connected Number as restricted, as this causes display problems. The Numbering - Public/Unknown Format overrides the Send Connected Number administration for any administrable block of extensions.

**Related topics:**

[QSIG Value-Added](#) on page 751

[Numbering-Private Format](#) on page 813

[Numbering — Public/Unknown Format](#) on page 814

**Send Name**

Specifies whether the calling/connected/called/busy party's administered name, or the name on a redirected call, is sent to the network on outgoing/incoming calls.

 **Note:**

If name information is not administered for the calling station or the connected/called/busy station, the system sends the extension number in place of the name.

| Valid Entry | Usage   |
|-------------|---|
| y           | The calling/connected/called/busy party's administered name and the name on a redirected call are sent on outgoing/incoming calls. An entry of y or n is required if the <b>Supplementary Service Protocol</b> is e (DCS with Rerouting).   |
| n           | Disables the sending of the calling/connected/called/busy party's administered name and the name on a redirected call on outgoing/incoming calls. An entry of y or n is required if the <b>Supplementary Service Protocol</b> is e (DCS with Rerouting). With an entry of n, an incoming name is not tandemed out again if the <b>Supplementary Service Protocol</b> field is any value other than b (QSIG).  |
| r           | Restricted. The calling/connected/called/busy party's administered name is sent "presentation restricted" on outgoing/incoming calls. The name on a redirected call is not sent. This value is valid only if the <b>Supplementary Service Protocol</b> is a (national supplementary service), b (for called/busy only), or d (for the QSIG Global Networking Supplementary Service Protocol). With an entry of r, an incoming name is marked restricted when it is tandemed out again. However, if the <b>Supplementary Service Protocol</b> is b (QSIG), then an incoming name is passed on unchanged and <b>Send Name</b> value is ignored. |

**Related topics:**

[Supplementary Service Protocol](#) on page 737

**Send UCID**

If enabled, the trunk transmits Universal Call IDs.

Available only if **UUU IE Treatment** is set to Shared.

**Send UII IE**

If enabled, sends UII information on a per trunk group basis.

**Show ANSWERED BY on Display**

Available only for isdn pri/bri and sip trunk groups.

| Valid Entry | Usage  |
|-------------|--|
| y           | The words "ANSWERED BY" display in addition to the connected telephone number on calls over this trunk. This is the default.<br><br> <b>Note:</b><br>Based on display language settings for stations, "ANSWERED BY" is translated into and displayed in the appropriate language. |
| n           | Only the connected telephone number displays. This might be preferred when outgoing calls are over a trunk that might be redirected.   |

### **Suppress # Outpulsing**

Indicates whether or not to suppress the final “#” in cases where the system would normally outpulse it. Used if end-to-end signaling begins with (and includes) “#”. This field should be enabled when the local telephone company central office or any other facility treats “#” as an error.

### **US NI Delayed Calling Name Update**

If calling name information is received after the incoming call has been delivered to the terminating telephone, enables or disables a display update.

 **Note:**

BRI trunks do not support display updates.

Available only if the **Carrier Medium** is either PRI/ BRI or ATM, and the **Supplementary Service Protocol** is a.

**Related topics:**

[Carrier Medium](#) on page 722

[Supplementary Service Protocol](#) on page 737

[ISDN-PRI](#) on page 947

### **UUI IE Treatment**

Specifies whether the user Information Element (IE) is shared.

| Valid Entry      | Usage                                      |
|------------------|--|
| shared           | The trunk is connected to the server.      |
| service-provider | Service provider functionality is desired. |

### **Wideband Support**

 **Note:**

This feature is not supported on the DS1 interfaces on H.248 gateways (G700/G350).

Enables or disables wideband switching on this trunk group. Only trunk members from TN464C or later circuit packs can use wideband switching.

Available only if **Wideband Switching** is enabled for the system.

 **Note:**

Wideband trunk calls are treated as a single trunk call when Automatic Circuit Assurance (ACA) measurements are taken. This way, if an ACA referral call is generated (for short or long holding time), the wideband call only triggers a single referral call using the lowest B-channel trunk member associated with the wideband channel.

**Related topics:**

[Wideband Switching](#) on page 950

## QSIG Trunk Group Options

This fields on this screen appear only when **Group Type** is isdn and **Supplementary Service Protocol** is b.

### Related topics:

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

[Trunk Group](#) on page 977

## Character Set for QSIG Name

Sets the character set for transmission of QSIG name data for display.

Available only if the **Group Type** is isdn, the **Supplementary Service Protocol** is b, and the **Display Character Set** is Roman.

| Valid Entry | Usage  |
|-------------|--|
| eurofont    | <p>The Roman Eurofont character set. This is the default.</p> <p> <b>Note:</b><br/>Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.</p>   |
| iso-8859-1  | <p>All data (i.e., characters) in the Name value transmitted over QSIG are converted from Eurofont (Avaya proprietary encoding) to ISO 8859-1.</p> <p> <b>Note:</b><br/>ISO 8859-1, more formally known as ISO/IEC 8859-1, or less formally as Latin-1, is part 1 of ISO/IEC 8859, a standard character encoding defined by ISO. It encodes what it refers to as Latin alphabet no. 1, consisting of 191 characters from the Latin script, each encoded as a single 8-bit code value.</p> |

### Related topics:

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

[Display Character Set](#) on page 938

## Display Forwarding Party Name

Enables or disables displaying the name of the party who is forwarding the call. The default is enabled. Available only if the **Group Type** is isdn and the **Supplementary Service Protocol** is b.

### Related topics:

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

## Diversion by Reroute

Enables or disables the Diversion by Reroute feature. If disabled, Communication Manager does not originate a Diversion/Reroute request over that trunk group, and rejects any

Diversion/Reroute request it receives over that trunk group. The default is enabled. Available only if the **Group Type** is isdn and the **Supplementary Service Protocol** is b.

**Related topics:**

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

**Path Replacement**

Enables or disables the Path Replacement feature. The default is enabled. If disabled, Communication Manager does not originate a Path Replacement request over that trunk group, and rejects any Path Replacement request it receives over that trunk group. Available only if the **Group Type** is isdn and the **Supplementary Service Protocol** is b.

**Related topics:**

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

**Path Replacement Method**

Available only if the **Group Type** is ISDN, the **Supplementary Service Protocol** is b or e, and **Supplementary Services with Rerouting** or **DCS with Rerouting** is enabled for the system. Not available if **Path Replacement with Retention** is enabled.

| Valid Entry       | Usage  |
|-------------------|--|
| always            | Use any QSIG (SSB) trunk group as the replacement trunk group. A new call is always originated, even when the original trunk group is determined to be the replacement trunk group.  |
| BR (better route) | Route pattern preferences help determine trunk group path replacement. The original trunk group is retained if <b>Path Replacement with Retention</b> is enabled. Path replacement fails (and the original trunk group is retained) if <b>Path Replacement with Retention</b> is disabled. |

**Related topics:**

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

[Path Replacement with Retention](#) on page 750

[DCS with Rerouting](#) on page 945

[Supplementary Services with Rerouting](#) on page 955

**Path Replacement with Retention**

Available only if the **Group Type** is ISDN, the **Supplementary Service Protocol** is b or e, and **Supplementary Services with Rerouting** or **DCS with Rerouting** is enabled for the system.

| Valid Entry | Usage                             |
|-------------|-----------------------------------|
| y           | Retains the original trunk group. |

| Valid Entry | Usage  |
|-------------|--|
| n           | Allows path replacement according to settings for the <b>Path Replacement Method</b> . |

**Related topics:**

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

[DCS with Rerouting](#) on page 945

[Supplementary Services with Rerouting](#) on page 955

**QSIG Value-Added**

Enables or disables QSIG-VALU services. Available only if **Value-Added (VALU)** is enabled for the system and **Supplementary Services Protocol** is enabled for the trunk.

**Related topics:**

[Supplementary Service Protocol](#) on page 737

[Value Added \(VALU\)](#) on page 955

**QSIG-Value Coverage Encoding**

The encoding method used to encode DL1, DL2, and DL3 extensions. Available only if the **Group Type** is isdn, **Supplementary Service Protocol** is b, and **QSIG Value-Added** is enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| proprietary | Communication Manager sends extension information in the normal manner. This is the default.                       |
| standard    | In addition to normal extension information, Communication Manager sends the data part (as null) of the extension. |

**Related topics:**

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

[Value Added \(VALU\)](#) on page 955

**SBS**

Enables or disables Separation of Bearer and Signaling (SBS) for the trunk group.

Available only if the **Local Country Code** and **International Access Code** are administered for the system and when the **Supplementary Service Protocol** is b, the **Group Type** is isdn, the **Carrier Medium** is H.323, and **Dial Access** is disabled.

**Related topics:**

[Local Country Code](#) on page 605

[International Access Code](#) on page 605

[Carrier Medium](#) on page 722

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

### **SIP Reference Trunk Group**

Appears only when the **Group Type** field is isdn, the **Carrier Medium** field is H.323, and the **Supplementary Service Protocol** field is b.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 2000   | (For Avaya S8510 Server) Assigns a number for the SIP trunk group. If trunk members are already assigned to this trunk group, you must not change the value of <b>SIP Reference trunk Group</b> field. If you change the value of this field, the system displays an error message and prompts you to remove all assigned members before enabling Q-SIP.  |
| 1 to 99     | (For Avaya S8300D Server) Assigns a number for the SIP trunk group. If trunk members are already assigned to this trunk group, you must not change the value of <b>SIP Reference trunk Group</b> field. If you change the value of this field, the system displays an error message and prompts you to remove all assigned members before enabling Q-SIP. |
| blank       | No SIP trunk group is assigned. By default, the value is blank.   |

### **TSC Method for Auto Callback**

Controls the signaling connection method for the QSIG Temporary Signaling Connections (TSC) when Communication Manager is the terminating or the outgoing gateway PINX.

| Valid Entry      | Usage   |
|------------------|---|
| drop-if-possible | QSIG Temporary Signaling Connections are released.  |
| always-retain    | QSIG Temporary Signaling Connections are always retained for successful call completion activation. |

### **ISDN Trunk Group: Administrable Timers**

This screen displays only when **Administer Timers** is enabled. This screen does not display for trunks of **Group Type** cpe or sip.

 **Note:**

If the ISDN trunk group has a **Carrier Medium** value of H.323, or if the trunk group has BRI members, then this page is not administrable. In these cases, an error message displays when you attempt to submit the screen.

 **Caution:**

Customers: Do not change fields on this page without assistance from Avaya or your network service provider.

**Related topics:**

[Carrier Medium](#) on page 722

[Group Type](#) on page 725

[Administer Timers](#) on page 733

**Programmed Dial Pause (msec)**

| Valid Entry                       | Usage   |
|-----------------------------------|---|
| 100 to 25500 in increments of 100 | The exact duration of the pause used during abbreviated dialing, ARS outpulsing, and terminal dialing operations. This timer is administrable for all outgoing and two-way trunk groups. This timer works with the TN464B (or later), TN767, TN458, TN2140, and TN2242 tie circuit packs. All central office (CO) circuit packs that accept administrable timers accept this timer. |

**END TO END SIGNALING**

Pause (msec)

Available only if the **Trunk Type** is blank.

| Valid Entry                    | Usage   |
|--------------------------------|---|
| 20 to 2550 in increments of 10 | The interval (pause) between DTMF tones sent from a hybrid telephone. All CO, DIOD, and tie circuit packs that accept administrable timers accept this timer. However, this timer is sent only to the following circuit packs: TN464B (or later), TN767, TN436B, TN459B, TN2146, TN2199, and TN2242, and TN429 and TN2184 ports in a DID trunk group. |

**Related topics:**

[Trunk Type](#) on page 826

Tone (msec)

Available only if the **Trunk Type** is blank.

| Valid Entry                    | Usage  |
|--------------------------------|--|
| 20 to 2550 in increments of 10 | The duration of the DTMF tone sent when a button on a hybrid telephone is pressed. All CO, DIOD, and Tie circuit packs that accept administrable timers accept this timer. This timer is also sent to the following circuit packs: TN464B (or later), TN767, TN436B, TN459B, TN2146, TN2199, TN429, TN2184 ports in a DID trunk group. |

**Related topics:**

[Trunk Type](#) on page 826

**Shared UUI Feature Priorities**

The fields in this page show the priorities for each type of information to be forwarded in the Shared UUI. This page appears only on the ISDN trunk group screen when all of the following conditions are met:

- The **UUI IE Treatment** is shared.
- The **Supplementary Service Protocol** is set to anything except b.

Changing the priorities in this screen might affect whether certain information will be sent.

**Related topics:**

[Supplementary Service Protocol](#) on page 737

[UUI IE Treatment](#) on page 748

**ASAI**

User information from Adjunct/Switch Applications Interface (ASAI).

| Valid Entry | Usage   |
|-------------|---|
| 1 to 7      | Level of priority, with 1 being the highest. Default priority is 1. |
| blank       | This field's information is not forwarded.                          |

**Collected Digits**

Digits collected from caller (not including dial-ahead digits).

| Valid Entry | Usage   |
|-------------|---|
| 1 to 7      | Level of priority, with 1 being the highest. Default priority is 5. |
| blank       | This field's information is not forwarded.                          |

**Held Call UCID**

The unique tag for the last call that was put on hold by the Automatic Call Distribution (ACD) agent placing this call to another system. This Universal Call ID (UCID) can be used to identify the original or parent call that may eventually be placed into conference or transferred to the other system. This element is required for cradle-to-grave tracking with Avaya IQ release 5.0 and later.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 7      | Level of priority, with 1 being the highest. The UCID included in the element with default priority 2 is the tag for a new call placed by the agent while the original call is on hold. Default priority is 7. |
| blank       | This field's information is not forwarded.   |

**In-VDN Time**

Number of seconds the call has spent in vector processing.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 7      | Level of priority, with 1 being the highest. Default priority is 3. |
| blank       | This field's information is not forwarded.                          |

### **Other LAI Information**

Includes the time stamp of when the call entered the current queue, the call's priority level in its current queue, and the type of interflow.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 7      | Level of priority, with 1 being the highest. Default priority is 6. |
| blank       | This field's information is not forwarded.                          |

### **Universal Call ID**

A unique tag that identifies the call that this message is being sent for and the other information included in the User-User-Information (UUI).

| Valid Entry | Usage   |
|-------------|---|
| 1 to 7      | Level of priority, with 1 being the highest. Default priority is 2. |
| blank       | This field's information is not forwarded.                          |

### **VDN Name**

Name of the active VDN (also called LAI DNIS).

| Valid Entry | Usage   |
|-------------|---|
| 1 to 7      | Level of priority, with 1 being the highest. Default priority is 4. |
| blank       | This field's information is not forwarded.                          |

### **CBC Service Trunk Group Allocation Plan Assignment Schedule**

This screen administers a fixed schedule or a schedule that can change up to six times a day for each day of the week. This screen determines which CBC Service Trunk Group Allocation Plan will be in use at any given time.

Available only if the ISDN trunk group **Service Type** is cbc and the ISDN trunk group **Usage Alloc** are enabled.

#### **Related topics:**

[Service Type](#) on page 729

[Usage Alloc](#) on page 732

### **Act Time**

The time the usage allocation plan will become effective.

| Valid Entry         | Usage   |
|---------------------|---|
| 00:00 through 23:59 | The time using the 24-hour clock (military time). There must be at least one entry per day. |

**Allocation Plan Number**

| Valid Entry     | Usage  |
|-----------------|--|
| 1 to 3<br>blank | The CBC Trunk Allocation Plan that is in effect if a fixed usage method has been selected. Required if the allocation plan is fixed. |

**Fixed**

Indicates whether the allocation plan will be fixed.

**Plan #**

| Valid Entry     | Usage  |
|-----------------|--|
| 1 to 3<br>blank | The number of the usage allocation plan that will be in effect from the activation time until the activation time of the next scheduled plan change. |

**Scheduled**

Indicates whether or not the allocation plans are implemented according to the administered schedule found on this page. If enabled, then there must be at least one entry in the schedule.

**CBC Trunk Group Usage Allocation**

This screen sets a minimum and maximum number of members for up to ten different Services/Features for up to three different Usage Allocation Plans (1 to 3). Available only if the **Service Type** is cbc and **Usage Alloc** is enabled.

**Related topics:**

[Service Type](#) on page 729

[Usage Alloc](#) on page 732

**Max# Chan**

| Valid Entry      | Usage   |
|------------------|---|
| 0 to 99<br>blank | The maximum number of members of an ISDN trunk group with a <b>Service Type</b> of cbc that a particular service or feature can use at any given time. This field must be administered if a service or feature has been entered in the Incoming Call Handling Treatment Table screen. |

**Min# Chan**

| Valid Entry      | Usage  |
|------------------|--|
| 0 to 99<br>blank | The minimum number of members of an ISDN trunk group with a <b>Service Type</b> of cbc that a particular service or feature can use at any given time. The sum of the minimum number of members for all services or features must not exceed the total number of members of the trunk group. |

### Service/Feature

The ISDN services or features that can be requested at call setup time when using this trunk group. In addition to predefined services or features that can be received on a call by call basis, user-defined service types can be used.

| Valid Entry | Usage  |
|-------------|--|
| 0           | Feature  |
| 1           | Service  |
| 2           | Incoming   |
| 3           | Outgoing   |
| other       | Any services or features that are not explicitly specified |

### Wideband Support Options

#### Note:

All B-channels that comprise the wideband call must reside on the same ISDN-PRI facility. Also, all trunk members in an ISDN trunk group with **Wideband Support** enabled must be from a TN464C (or later) circuit pack.

### Contiguous

Available only if “N by DS-zero” (NXDS0) multi-rate service is enabled.

| Valid Entry | Usage   |
|-------------|---|
| y           | Specifies the “floating” scheme. NXDS0 calls are placed on a contiguous group of B-channels large enough to satisfy the requested bandwidth without constraint on the starting channel (no fixed starting point trunk). Not available with H0 ISDN information transfer rate. |
| n           | Specifies the “flexible” scheme. NXDS0 calls are placed on any set of B-channels on the same facility as long as the requested bandwidth is satisfied. There are no constraints, such as contiguity of B-channels or fixed starting points                                    |

#### Related topics:

[NxDS0](#) on page 758

[NXDS0](#) on page 834

### H0

If enabled, specifies the ISDN information transfer rate for 384-kbps of data that is comprised of six B-channels. When a trunk group is administered to support H0, the trunk or hunt algorithm to satisfy a call requiring 384-kbps of bandwidth uses a fixed allocation scheme.

### H11

If enabled, specifies the ISDN information transfer rate for 1536-kbps of data that is comprised of 24 B-channels. When a trunk group is administered to support H11, the trunk or hunt algorithm to satisfy a call requiring 1536-kbps bandwidth uses a fixed allocation scheme.

## H12

If enabled, specifies the ISDN information transfer rate for 1920-kbps of data that is comprised of 30 B-channels. When a trunk group is administered to support H12, the trunk or /hunt algorithm to satisfy a call requiring 1920-kbps bandwidth uses a fixed allocation scheme.

## NxDS0

Enables or disables the "N by DS-zero" multi-rate service.

### ISDN Trunk Group: Group Member Assignments

 **Note:**

When supporting DCS, Member Number Assignments must be the same between nodes. For example, Member #1 must be Member #1 at the far-end trunk group.

#### **Administered Members (min/max)**

The minimum and maximum member numbers that have been administered for this trunk group.

#### **Code**

The type of circuit pack physically installed or logically administered at the location to which this member is assigned. If no circuit pack is installed or administered at the port address, the field is blank.

#### **Name**

The name of the trunk group member. The name should identify the trunk unambiguously. Accepts up to 10 characters.

#### **Example**

- The telephone number assigned to incoming trunks
- The Trunk Circuit Identification number assigned by the service provider

#### **Night**

The night service destination for this trunk group member if different from the night service destination administered for the trunk group. Incoming calls are routed to this destination when the system is placed in night service mode.

| Valid Entry              | Usage   |
|--------------------------|---|
| <i>A valid extension</i> | The extension of the night destination for the trunk.   |
| attd                     | Calls go to the attendant when night service is active. |
| blank                    | Not administered  |

#### **Related topics:**

[Night Service](#) on page 986

**Port**

When using ISDN-BRI interfaces, B-channel 1 is the port number while B channel 2 is the port number plus 16. For example, if B channel 1's port number is 01A1002, then B channel 2's port number is 01A1018.

When using ISDN-PRI interfaces, the port number will be the one allied with the B-channel. For example, if the DS1 is located in 01A10, then B channel 1 will be 01A1001, B channel 2 will be 01A1002 and so forth.

 **Note:**

When administering analog trunks connected to a TIM518, physical ports 17 to 24 are administered as ports 9 to 16 in Communication Manager.

**Sfx**

The model suffix for the type of circuit pack physically installed at the location to which this member is assigned. If no circuit pack is installed at the port address, the field is blank.

**Sig Grp**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 650    | The signaling group of this trunk group member. Required for IP group members. If you administer a port that resides on a DS1 board and that DS1 board belongs to one and only one signaling group, you can leave the <b>Signaling Group</b> blank. The appropriate default signaling group number is inserted by Communication Manager. If a DS1 board is assigned to more than one signaling group, then you must enter a signaling group number. A trunk group can contain members from different signaling groups. |

**Related topics:**

[Group Type](#) on page 725

[Signaling Group](#) on page 730

**Total Administered Members**

The total number of members administered in the trunk group.

**ISDN-BRI Trunk Circuit Pack**

Administers an ISDN-BRI circuit pack.

Example command: `change bri-trunk-board n`, where *n* is the board location.

**ISDN-BRI Trunk Circuit Pack: page 1, TN2185 circuit pack****Cntry/Peer Protocol**

The ISDN protocol standard that is applied.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 25     | An entry of 10, 12, or 13 is equivalent to a <b>Protocol Version</b> of b administered for the DS1 Circuit Pack. All other administered values are equivalent to a <b>Protocol Version</b> of a administered for the DS1 Circuit Pack. |
| etsi        | Equivalent to a <b>Protocol Version</b> of b administered for the DS1 Circuit Pack.  |
| QSIG        | Required for a peer-slave or peer-master interface. Valid only when the Interface field is peer-slave.   |
| blank       | Cannot be blank if an interface is administered.   |

**Related topics:**

[Protocol Version](#) on page 546

[Interface](#) on page 761

**DCP/Analog Bearer Capability**

| Valid Entry   | Usage   |
|---------------|---|
| 3.1kHz speech | Indicates how to encode the Bearer Capability IE for an outgoing call originated by a DCP or analog endpoint. |

**Detect Slips**

Enables or disables logging of slips reported by the BRI port.

**ETSI CCBS**

Available only if **Group Type** is isdn-pri.

| Valid Entry     | Usage  |
|-----------------|--|
| none            | Interface supports neither incoming nor outgoing ETSI CCBS. This is the default.   |
| inco(ming)      | Interface supports only incoming ETSI CCBS.  |
| outg(oing)      | Interface supports only outgoing ETSI CCBS.  |
| both directions | Interface supports incoming and outgoing ETSI CCBS.<br><br> <b>Note:</b><br>When upgrading from a version of Communication Manager that is earlier than 5.1, this is the default. |

**Related topics:**

[Group Type](#) on page 725

**Interface**

| Valid Entry                                  | Usage  |
|--|--|
| network<br>user<br>peer-master<br>peer-slave | Indicates whether a particular port is connected to a user, network or a peer interface. These entries are valid for the TN2185. Peer-slave is available only if the QSIG Basic Call Setup feature is enabled. |

**Interface Companding**

The companding algorithm expected by the system at the far end.

| Valid Entry | Usage   |
|-------------|---|
| a-law       | Algorithm expected at the far-end for E1 service. |
| mu-law      | Algorithm expected at the far-end for T1 service. |

**Layer 1 Stable**

If enabled, the network drops Layer 1 when the BRI port is idle.

**Location**

Displays the TN2185 circuit pack location (PPCSS).

**Name**

The name used to identify the circuit pack. Accepts up to 15 alphanumeric characters.

 **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Port**

The port number to which administered parameters apply.

**Side**

| Valid Entry | Usage   |
|-------------|---|
| a<br>b      | Determines how glare conditions are handled for a peer-slave interface. |

**Related topics:**

[Interface](#) on page 542

**Synch Source**

Enables or disables a port on the circuit pack for clock synchronization with the far-end network. Allows a TN2185 board to be the primary or secondary synchronization source, if at least one of the ports on that board has this field enabled.



**Note:**

Not available for MM720 and MM722 bri media modules. For the MM720 and MM722, this parameter is configured using the gateway Command Line Interface (CLI).

**T3 Timer Length (sec)**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 127    | Tells the TE side how many seconds to wait for an inactive Layer 1 to become active. |

**TEI**

| Valid Entry | Usage   |
|-------------|---|
| auto        | TEI is assigned automatically by the network. |
| 0           | TEI is fixed.                                 |

**Termination Type**

When a MM720 media module is used as a trunk interface, and the MM720 supports both Line side and Trunk side of BRI, indicates whether the media module is to operate in Terminal or Network termination mode.

| Valid Entry | Usage  |
|-------------|--|
| TE          | Terminal Endpoint termination. The MM720 provides the TE side of the BRI interface. This is the default. |
| NT          | Network Termination. The MM720 provides the NT side of the BRI interface.                                |

**ISDN-BRI Trunk Circuit Pack: page 1, TN556B or TN2198 circuit packs**

The following field descriptions are unique to the ISDN-BRI Circuit Pack screen with a TN556B or TN2198 circuit pack. The following fields do not display with a TN556B or TN2198 circuit pack:

- **T3 Timer Length (sec)**
- **Synch Source**
- **Layer 1 Stable**
- **Detect Slips**

**DCP/Analog Bearer Capability**

| Valid Entry   | Usage   |
|---------------|---|
| 3.1kHz speech | Indicates how to encode the Bearer Capability IE for an outgoing call originated by a DCP or analog endpoint. |

**Cntry/Peer Protocol**

The ISDN protocol standard that is applied.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 25     | An entry of 10, 12, or 13 is equivalent to a <b>Protocol Version</b> of b administered for the DS1 Circuit Pack. All other administered values are equivalent to a <b>Protocol Version</b> of a administered for the DS1 Circuit Pack. |
| etsi        | Equivalent to a <b>Protocol Version</b> of b administered for the DS1 Circuit Pack.  |
| QSIG        | Required for a peer-master interface.  |
| blank       | This field cannot be blank if an interface is administered.  |

**Related topics:**

[Protocol Version](#) on page 546

[Interface](#) on page 763

**Interface**

Indicates whether a particular port is connected to a user/network or a peer interface. These entries are valid for the TN556B.

| Valid Entry | Usage   |
|-------------|---|
| network     | User/network connection.  |
| peer-master | Peer interface connection. Available only if QSIG Basic Call Setup is enabled |

**Side**

| Valid Entry | Usage   |
|-------------|---|
| a<br>b      | Determines how glare conditions are handled for a peer-slave interface. |

**Related topics:**

[Interface](#) on page 542

**ISDN-BRI Trunk Circuit Pack: page 2**

 **Note:**

If administering a TN2185 circuit pack, 8 ports appear; otherwise, 12 ports appear.

 **Note:**

You cannot change the **Endpt Init**, **SPID**, or **Endpt ID** port parameters unless that port is busied out or unadministered. It is possible to change all other fields on this page even if the corresponding port is active.

If the **Interface** field on page 1 contains a valid value when the screen is submitted, the contents of the fields on page 2 for that port are validated. If the **Interface** field is blank when the screen is submitted, the fields on this page for that port reset to their default values.

**Directory Number**

The directory numbers assigned to the interface and allocated to two separate endpoints. This field must be administered in pairs. Accepts up to 10 characters.

**Endpt ID**

| Valid Entry | Usage  |
|-------------|--|
| 00 to 62    | The Endpoint Identifier expected by the far end. Communication Manager prevents changing this field unless the port is busied out or unadministered. Leading zeroes are significant and must not be ignored. |

**Endpt Init**

Indicates whether the far end supports endpoint initialization. Communication Manager blocks you from changing this field unless the port is busied out or unadministered.

| Valid Entry | Usage   |
|-------------|---|
| y           | Requires that an <b>SPID</b> be administered.                         |
| n           | Requires that an <b>SPID</b> and <b>Endpt ID</b> not be administered. |

**Related topics:**

[Endpt ID](#) on page 764

[SPID](#) on page 765

**Interworking Message**

Determines what message Communication Manager sends when an incoming ISDN trunk call is routed over a non-ISDN trunk group.

| Valid Entry | Usage  |
|-------------|--|
| PROGress    | Requests the public network to cut through the B-channel and let the caller hear tones such as ringback or busy tone provided over the non-ISDN trunk. Normally-selected value.  |
| ALERTing    | Causes the public network in many countries to play ringback tone to the caller. This value is used only if the DS1 is connected to the public network, and it is determined that callers hear silence (rather than ringback or busy tone) when a call incoming over the DS1 interworks to a non-ISDN trunk. |

**Max NCA TSC**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 63     | The maximum number of Non-Call-Associated Temporary Signaling Connections allowed on this BRI D-channel. |

**Port**

The port number to which administered parameters apply.

## SPID

The Service Profile Identifier (SPID) expected by the far end. Accepts up to 12 characters. Communication Manager prevents changing this field unless the port is busied out or unadministered. The only protocol supported for SPID initialization is Country Code 1. Trunks are not put in service if SPID installation is not successful. Leading zeroes are significant and must not be ignored.

## XID Test

If enabled, the far end supports the Layer 2 XID test.

## Language translations

Pre-translated messages are available in English, French, Italian, and Spanish to display on system telephones. Translations for many Communication Manager messages can be assigned using the Language Translations screens. As of July 1, 2005, new messages are no longer added to these screens, so these screens might not show all available Communication Manager messages.

On the Language Translations screens, phone messages are provided in the left column or top row, with the translation provided in the right column or bottom row.

As a preferred method for entering translations for user-defined phone messages, Avaya recommends using the Avaya Message Editing Tool (AMET). This tool is available for download from <http://www.avaya.com>.

### Note:

If “user-defined” is entered for the display language on the Station screen or Attendant Console screen, and no messages are defined on these screens, a string of asterisks appears on all display messages.

### Warning:

Do not use the translation pages if you have installed the `avaya_user-defined.text` file.

Example command: `change display-messages ad-programming`

## Automatic Wakeup

Replaces the English text for Automatic Wakeup messages that appear on telephone displays.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

### Related topics:

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

### **Button labels**

Replaces the English text for button labels that appear on telephone displays.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

#### **Related topics:**

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

### **Enhanced Abbreviated Dialing**

Administers the Enhanced Abbreviated Dialing messages that appear on telephone displays in place of the English message.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

#### **Related topics:**

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

### **Leave Word Calling**

Replaces the English text for Leave Word Calling messages that appear on telephone displays.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

#### **Related topics:**

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

### **Malicious Call Trace**

Replaces the English text for Malicious Call Trace messages that appear on telephone displays.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

**Related topics:**

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

**Miscellaneous call identifiers**

Replaces the English text for miscellaneous call identifiers that appear on telephone displays.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

**Related topics:**

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

**Miscellaneous features**

Replaces the English text for miscellaneous feature messages that appear on telephone displays.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

**Related topics:**

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

**Property Management Interface**

Replaces the English text for Property Management Interface messages that appear on telephone displays.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

**Related topics:**

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

## Self Administration

Replaces the English text for any self administered messages that appear on telephone displays.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

### Related topics:

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

## Softkey Labels

Replaces the English text for any softkey labels that appear on telephone displays.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

In order to provide unique labels for abbreviated dialing button types for softkey labels, Communication Manager replaces the last two characters with digits for the 12-key 8400 and 15-key 8434D telephones.

On this screen, the digits following the **AD** are derived from the button position. If the first button is an AD button, then it is AD1 and the 15th button is AD15. All the AD buttons between 1 and 15 have the position number appended to AD.

### Related topics:

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

## Transfer Conference

Replaces the English text for any Transfer Conference messages that appear on telephone displays.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

### Related topics:

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

## View Buttons

Replaces the English text for any buttons that appear on telephone displays.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

### Related topics:

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

## Vustats

Replaces the English text for any Vustats that appear on telephone displays.

This screen contains an English version of the display, an explanation of the English message, and a translation of the English message. A long message can be shortened on telephones that display fewer than 32 characters.

### Related topics:

[Message 4](#) on page 769

[Message 6](#) on page 769

[Message 15, 16, 18](#) on page 769

[Message 12](#) on page 770

## Message 4

The character "^" is a place holder.

| English Text                   | Replacement Info   |
|--------------------------------|--|
| ^-party conference in progress | "^" is replaced with the number of parties currently on the conference call. |

Manually change ~ to ^ in any user-defined language. The software does not update manually.

## Message 6

The character "^" is a place holder.

| English Text                             | Replacement Info  |
|--|---|
| Select line ^ to cancel or another line. | "^" is replaced with the letter of the line that is on soft hold. |

Manually change ~ to ^ in any user-defined language. The software does not update manually.

## Message 15, 16, 18

The character "^" is a place holder.

| English Text                | Replacement Info  |
|-----------------------------|---|
| Select line ^ to add party. | "^" is replaced with the letter of the line that is on soft hold. |

**Message 12**

The character "^" is a place holder.

| English Text                | Replacement Info  |
|-----------------------------|---|
| Select line ^ to add party. | "^" is replaced with the letter of the line that is on soft hold. |

Manually change ~ to ^ in any user-defined language. The software does not update manually.

**Listed Directory Numbers**

Allows Direct Inward Dialing (DID) numbers to be treated as public Listed Directory Numbers (LDNs). When one of these numbers is direct inward dialed, the calling party is routed to the attendant. The attendant display indicates a Listed Directory Number call and the name associated with the dialed extension.

Example command: `change listed-directory-numbers`

**Ext**

Any valid extension number.

**Name**

The name used to identify the Listed Directory Number. Accepts up to 27 alphanumeric characters.

**Night Destination**

A valid assigned extension number that receives calls to these numbers when Night Service is active. Accepts up to eight digits.

**TN**

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

**Locations**

Provides daylight savings time displays to users to set the area code for each location, and to administer different location information for each location. If the Multiple Locations feature is enabled, up to 250 location specifications can be administered, depending on the configuration of the server that is running Communication Manager. Otherwise, information for Location No. 1 applies to all locations.

Example command: `change locations`

## ARS FAC

The Feature Access Code (FAC) for accessing Automatic Route Selection (ARS). Any valid FAC format is acceptable, up to four digits. Characters \* or # are permitted, but only in the first position. Many locations are expected to share the same access code.

### Related topics:

[Feature Access Code \(FAC\)](#) on page 558

## ARS Prefix 1 Required for 10-Digit NANP Calls?

If enabled, a 1 must be dialed before all 10-digit NANP calls.

## Attd FAC

The Feature Access Code (FAC) for connection to the attendant. Accepts up to two digits. Characters \* or # are not permitted. Many locations are expected to share the same access code.

Available only if an Attendant Access Code has first been administered either for the Dial Plan or as a standard FAC.

### Note:

Within a dial plan, FAC/DAC codes and extensions cannot both start with the same first digits. Either the FAC/DAC entries or the block of extensions must be changed to have a different first digit.

### Related topics:

[Call Type](#) on page 530

[Attendant Access Code](#) on page 559

## Disp Parm

The administered display parameters for the location.

### Related topics:

[Display Parameters](#) on page 536

## Loc Parm

Required when administering multiple locations.

| Valid Entry      | Usage   |
|------------------|---|
| 1 to 25<br>blank | The number of the corresponding Location Parameter set for this location. Default is blank. |

## Loc Number

| Valid Entry | Usage                |
|-------------|----------------------|
| 1 to 250    | The location number. |

**Name**

A name you use for the location. Names are easier to remember than location numbers. Accepts up to 15 alphanumeric characters.

**NPA**

The three-digit numbering plan area code for each location.

**Prefix**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 99999  | Location prefix used with the Uniform Dialing Plan to identify the location of an originating call. All or part of the prefix is added to the front of the dialed string. |

**Related topics:**

[Insert Digits](#) on page 1044

**Proxy Sel Rte Pat**

| Valid Entry       | Usage  |
|-------------------|--|
| 1 to 999<br>blank | The routing pattern used to get to the proxy server. |

**Related topics:**

[Route Pattern](#) on page 843

**Rule**

Required for each administered location.

| Valid Entry      | Usage  |
|------------------|--|
| 0                | No Daylight Savings  |
| 1 to 15<br>blank | The number for the Daylight-Savings Rule applied to this location. |

**Timezone Offset**

Specifies how much time each location differs from the system time. Required for each administered location. Use +00:00 for the time zone offset for a single location media server.

| Valid Entry | Usage   |
|-------------|---|
| +           | The time set on this location is a certain amount of time ahead of the system time. |
| -           | The time set on this location is a certain amount of time behind the system time.   |

| Valid Entry | Usage   |
|-------------|---|
| 0 to 23     | The number of hours difference between this location and system time. |

| Valid Entry | Usage   |
|-------------|---|
| 0 to 59     | The number of minutes difference between this location and system time. |

## Location Parameters

Sets or changes certain administrable characteristics that determine part of a location's behavior. These include recall timing intervals and loss plans for two-party and conference calls.

Multiple instances of the Location Parameters screen are accessible if **Multiple Locations** is enabled for the system. If **Multinational Locations** is enabled, Location Parameters 2-25 contain the same fields as for Location Parameters 1. If **Multinational Locations** is disabled, the system does not display the following fields for Location Parameters 1:

- **Tone Generation Plan**
- **DCP Terminal-parameters Plan**
- **Country Code for CDR**

Example command: `change location-parameters`

### Related topics:

[Multinational Locations](#) on page 948

[Multiple Locations](#) on page 948

### Location Parameters: page 1

#### *Analog Ringing Cadence*

The country code identifies the ringing cadence to be used by analog telephones in the system

| Valid Entry | Usage  |
|-------------|--|
| 1 to 25     | <p>The location country code.</p> <p> <b>Note:</b><br/>This field must be set to 1 (US) for the Message Waiting Indicator on the Station to be set to neon.</p> |

### Related topics:

[Message Waiting Indicator](#) on page 896

[Country options table](#) on page 935

#### *Analog Line Transmission*

The country code identifies the transmission and signaling parameters.

| Valid Entry | Usage                      |
|-------------|----------------------------|
| 1 to 25     | The location country code. |

**Related topics:**

[Country options table](#) on page 935

**Companding Mode**

The companding algorithm used by system hardware.

| Valid Entry | Usage                           |
|-------------|---------------------------------|
| A-Law       | Generally used outside the U.S. |
| Mu-law      | Generally used in the U.S.      |

**Country code for CDR**

Available only if the Multinational Locations feature is enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 999    | The country code to be used for Call Detail Recording information for a location. Default is 1. |

**Related topics:**

[Country options table](#) on page 935

[Multinational Locations](#) on page 948

**DCP Terminal-parameters Plan**

Corresponds to the DCP terminal transmission parameters administered for the location. Available only if the Multinational Locations feature is enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 25     | The terminal-parameters plan number. Default is 1. |

**Related topics:**

[Multinational Locations](#) on page 948

[Terminal Parameters](#) on page 965

**End OCM After Answer (msec)**

If the **End OCM After Answer** field contains a non-blank value, Communication Manager starts the End OCM timer when Communication Manager receives an answer signal. The End OCM timer ensures that an outgoing call using OCM call classification is answered by an agent or an announcement within a specified time.

| Valid Entry   | Usage   |
|---------------|---|
| 100 to 25,000 | The timeout value is in milliseconds. If the timer expires, Communication Manager disconnects the call classifier and connects the call to the administered intercept extension. If the call classifier |

| Valid Entry | Usage  |
|-------------|--|
|             | classifies the call before the timer expires, the timer is cancelled and the call routed or treated appropriately. |
| blank       | Indicates that the timer has no limit.   |

### ***End of OCM Intercept Extension***

| Valid Entry | Usage  |
|-------------|--|
| extension   | The extension number Communication Manager connects the call to when the <b>End OCM After Answer</b> field expires. The extension number can be a recorded announcement, a vector directory number, or a hunt group extension. |
| blank       | Indicates that the extension number is empty. If the <b>End OCM After Answer</b> field is set to a non-blank value, the <b>End of OCM Intercept Extension</b> field cannot be left blank.                                      |

### ***International Access Code***

An up to five-digit International Access Code. Default is blank.

### ***Local E.164 Country Code***

An up to three-digit E.164 Country Code. Default is blank.

For a list of country codes, see the *International Telecommunications Union List of ITU-T Recommendation E.164 Assigned Country Codes* .

### ***Long Distance Access Code***

| Valid Entry | Usage   |
|-------------|---|
| 0 to 9      | The long distance access code you want the system to prefix to the telephone number. Accepts up to five digits. |
| blank       | Not administered. This is the default.  |

### ***Off-PBX Feature Name Extension Set***

| Valid Entry   | Usage   |
|---|---|
| 0 to 10 for a medium configuration<br>1 to 99 for a large configuration | Feature Name Extension (FNE) set that should be used for location based call routing. |
| blank   | Default FNE set is used. This is the default.   |

### ***Tone Generation Plan***

Available only if the Multinational Locations feature is enabled for the system. The value in this field corresponds to the tone generation characteristics administered for this location.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 25     | The tone-generation plan number. Default is 1. |

**Related topics:**

[Tone Generation](#) on page 975

**RECALL TIMING**

Disconnect Timing (msec)

Available only if a Flashhook Interval is not required.

| Valid Entry                      | Usage   |
|----------------------------------|---|
| 80 to 1250 (in increments of 10) | An on-hook that lasts for a period of time less than this value will be ignored; greater than or equal to this value is regarded as a disconnect. |

**Related topics:**

[Flashhook Interval](#) on page 776

Flashhook Interval

Enables or disables requiring a flashhook interval (recall window).

**Related topics:**

[Disconnect Timing \(msec\)](#) on page 776

Forward Disconnect Timer (msec)

| Valid Entry                      | Usage   |
|----------------------------------|---|
| 25 to 1500 (in increments of 25) | Specifies the duration of a momentary disconnect sent by the server/switch to an analog station user when that user is the last party still off-hook on a call. |

Lower Bound (msec)

Available only if a flashhook interval is required.

| Valid Entry                      | Usage  |
|----------------------------------|--|
| 80 to 1250 (in increments of 10) | The lower bound of the station-to-switch recall signal timing interval in milliseconds. Specifies the lower bound of the flashhook interval. |

**Related topics:**

[Flashhook Interval](#) on page 776

## MF Interdigit Timer (sec)

| Valid Entry | Usage  |
|-------------|--|
| 1 to 255    | The maximum number of seconds Communication Manager waits for the first forward signal (digit) to arrive, and for subsequent digits to arrive. Intercept returns to the calling party if this timer expires. This number must be less than the number of seconds administered for the short interdigit timer. Applies only to multifrequency signaling trunks. |

## Outgoing Shuttle Exchange Cycle Timer (sec)

Available only if the **Incoming Call Type** is group-ii-mfc or non-group-ii-mfc and the **Outgoing Call Type** is group-ii-mfc or none for the Multifrequency Signaling-Related System Parameters. This field applies only to multifrequency signaling calls made from Avaya Communication Manager.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 25     | The number of seconds to time an exchange cycle (starts when the far end requests a digit until Avaya Communication Manager sends the requested digit0). |

**Related topics:**

[Incoming Call Type](#) on page 792

[Outgoing Call Type](#) on page 794

## Upper Bound (msec)

Available only if the flashhook interval is required.

| Valid Entry                      | Usage  |
|----------------------------------|--|
| 80 to 1250 (in increments of 10) | The upper bound of the flashhook interval. Specifies the upper bound of the station-to-switch recall signal timing interval in milliseconds. A flash of 50 msec to 130 msec is always acceptable from a 2500-type set regardless of the setting of the Upper and Lower bounds and is treated as the digit one. |

**Related topics:**

[Flashhook Interval](#) on page 776

**Location Parameters: page 2****LOSS PLANS**

## 2-Party Loss Plan/Tone Loss Plan

Provides the default values for digital loss plan and for *n*-party conference loss.

| Valid Entry | Usage                            |
|-------------|----------------------------------|
| 1 to 25     | A country code for the location. |

**Related topics:**

[Country options table](#) on page 935

Customize

Enables customization on the corresponding loss plan table. When **Customize** is enabled for the End-to-End total loss (dB) in a n-party conference, values can be changed by the administrator. When **Customize** is disabled, the End-to-End total loss (dB) in a n-party conference values are reset to the values that they would have had under the 2 Party Loss Plan. Available only if Digital Loss Plan Modification is enabled for the system.

**Related topics:**

[End-to-End total loss \(dB\) in a n-party conference](#) on page 778

[Digital Loss Plan Modification](#) on page 945

End-to-End total loss (dB) in a n-party conference

| Valid Entry | Usage   |
|-------------|---|
| 0 to 99     | Provides total loss for a conference call with the designated number of parties.<br>The higher the number listed for a call with a fixed display number of parties, the more loss Communication Manager adds into a conference call with that number of parties; therefore, the conference call is quieter. |

 **Note:**

The End-to-End total loss for multi-party conference calls that is administered for this field is not always applied to a specific call.

Inter-location Loss Group

When inserting loss for a call, the server treats parties on the call who are in separate locations as if the location with the most parties were connected by an equal number of IP tie trunks as there are parties at other locations. The field specifies the digital loss group number that is used by these virtual IP tie trunks. Available only if the Multinational Locations feature is enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 19     | The digital loss group number to use on inter-location calls involving this location. Default is 18. |

**Related topics:**

[Multinational Locations](#) on page 948

**Location Parameters: page 3****FROM / TO**

| Valid Entry | Usage   |
|-------------|---|
| -3 to 15    | Identifies the variable digital loss values. An unsigned number is a decibel loss, while a number preceded with a minus sign is a decibel gain. |

**Login Administration**

Beginning with Communication Manager 4.0, there is no longer a Login Administration screen. For details on screens used for login administration, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431, and “AAA Services” in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

**Logging levels**

Administers logging of SAT activities. Specifies that commands associated with specific actions shown on this screen are logged by the system. The amount of detail to be logged is the same for all enabled actions and is specified by the **Log Data Values** field.

 **Note:**

The defaults on this screen provide the same amount and type of logging as in Communication Manager releases prior to 4.0.

Example command: `change logging-levels`

**Related topics:**

[Log Data Values](#) on page 779

**Logging Levels: page 1****Enable Command Logging**

If enabled, SAT activity is logged for selected commands.

**Log Data Values**

| Valid Entry | Usage   |
|-------------|---|
| none        | Only the object, the qualifier, and the command action are logged.          |
| new         | The new value of any field is logged. The old value is not logged.          |
| both        | Both the prior field value and the field value after the change are logged. |

## Logging Levels: page 2

### **Log All Submission Failures**

Form submission failures due to a security violation are always logged and are not affected by this field.

| Valid Entry | Usage  |
|-------------|--|
| y           | Record submission failures on the history log. An event is logged when Avaya Communication Manager rejects a form submission for any reason, such as an invalid entry in a field or a missing value. |
| n           | Submission failures are not recorded on the history log.   |

### **Log CTA/PSA/TTI Transactions in History Log**

Enables or disables logging transactions when extensions and physical telephones move between ports without additional administration from the administrator of Communication Manager.

If enabled, the system records Customer Telephone Activation (CTA), Personal Station Activation (PSA), and TTI transactions in the system history log.

Available only if Terminal Translation Initialization (TTI) is enabled for the system.

#### **Related topics:**

[Terminal Trans. Init. \(TTI\)](#) on page 950

### **Log IP Registrations and Events**

If enabled, allows the logging of IP registrations in the history log.

### **Log PMS/AD Transactions**

If enabled, the system records Property Management System (PMS) and Abbreviated Dialing (AD) events to the log.

## **Loudspeaker Paging**

The Loudspeaker Paging screen administers voice paging, deluxe voice paging, and chime paging.

#### **Note:**

To set up paging on an H.248 gateway, connect the paging system to a port on an MM711 and administer the port as an analog station on the Station screen. No entries on the Loudspeaker Paging screen are required.

Example command: `change paging loudspeaker`

## **CDR**

If enabled, Communication Manager collects CDR data on the paging ports.

**Code Calling — COR**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 995    | Assigns a Class of Restriction to a paging zone for chime paging. |
| blank       | An unused paging zone.  |

**Code Calling Playing Cycles**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 3      | The number of times a chime code plays when a user makes a chime page. |
| blank       | Cannot be blank when administering chime paging (code calling).        |

**Code Calling — TAC**

Assigns a Trunk Access Code (TAC) to a paging zone for chime paging. Users dial this code to make a page to a specific zone. One TAC must be assigned to each zone used. Two zones cannot have the same TAC. A TAC in the zone designated ALL means that users can activate speakers in all the zones by dialing that code.

| Valid Entry   | Usage   |
|---------------|---|
| 1 to 4 digits | A Trunk Access Code (TAC) allowed by the dial plan. |
| *             | Can be used as first digit.                         |
| #             | Can be used as first digit.                         |
| blank         | An unused paging zone.                              |

**Code Calling — TN**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 100    | Assigns a paging zone to a tenant partition for chime paging when Tenant Partitioning is in use. |

**Related topics:**

[Tenant Partitioning](#) on page 949

**Location**

Assigns a descriptive name for the physical location corresponding to each zone when Tenant Partitioning is in use. Accepts up to 27 characters.

**Example**

Typical entries might be “conference room A”, “warehouse”, or “storeroom”.

**Port**

Assigns a port on an auxiliary trunk circuit pack to a paging zone.

| Valid Entry                        | Usage  |
|------------------------------------|--|
| 1 to 64                            | First and second characters are the cabinet number |
| A to E                             | Third character is the carrier                     |
| 0 to 20                            | Fourth and fifth character are the slot number     |
| 01–04 (Analog TIE trunks)<br>01–31 | Six and seventh characters are the circuit number  |
| 1 to 250                           | Gateway  |
| VI to V9                           | Module   |
| 01 to 31                           | Circuit  |
| blank                              | An unused paging zone                              |

### Voice Paging — COR

| Valid Entry | Usage   |
|-------------|---|
| 0 to 995    | Assigns a Class of Restriction to a paging zone for voice paging. |
| blank       | An unused paging zone.  |

### Voice Paging — TAC

Assigns a Trunk Access Code (TAC) to a paging zone for voice paging. Users dial this code to make a page to a specific zone. One TAC must be assigned to each zone you want to use. Two zones cannot have the same TAC. A TAC entered in the zone designated ALL means that users can activate speakers in all the zones by dialing that code.

| Valid Entry   | Usage  |
|---------------|--|
| 1 to 4 digits | A Trunk Access Code (TAC) allowed by your dial plan. |
| *             | Can be used as first digit.                          |
| #             | Can be used as first digit.                          |
| blank         | An unused paging zone                                |

### Voice Paging Timeout (sec)

Limits the duration of voice pages. When this interval ends, calls are disconnected. To determine the best setting, time the typical pages that are expected to broadcast and then add another 4 to 5 seconds.

| Valid Entry      | Usage  |
|------------------|--|
| 10 to 60 seconds | The maximum number of seconds any page lasts.                |
| blank            | The field cannot be blank when voice paging is administered. |

## Voice Paging — TN

| Valid Entry | Usage  |
|-------------|--|
| 1 to 100    | Assigns a paging zone to a tenant partition for voice paging if Tenant Partitioning is in use. |

### Related topics:

[Tenant Partitioning](#) on page 949

## Maintenance-related system parameters

This screen is described in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

## Media-Gateway

This screen is described in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

## Mode Code Related System Parameters

Establishes parameters associated with the Mode Code Voice Mail System Interface. Available only if the **Mode Code Interface** feature is enabled.

Example command: `change system-parameters mode-code`

### Related topics:

[Mode Code Interface](#) on page 593

## MODE CODES (FROM SWITCH TO VMS)

### **Direct Dial Access-Trunk**

The mode code that the media server or switch sends when an external caller dials the Voice Mail System (VMS) access number. Accepts up to six digits. Also accepts #, \*, and #00.

### **Direct Inside Access**

The mode code that the media server or switch sends when a caller at an internal extension dials the Voice Mail System (VMS) access number. Accepts up to six digits. Also accepts #, \*, and #00.

### **External Coverage**

The mode code that the media server or switch sends when an external caller tries to reach a user at another extension and the call goes to the user's voice-mail coverage. Accepts up to six digits. Also accepts #, \*, and #00.

**Internal Coverage**

The mode code that Communication Manager sends when an internal caller tries to reach a user at another extension and the call goes to the user’s voice mail coverage. Accepts up to six digits. Also accepts #, \*, and #00.

**Refresh MW Lamp**

The mode code that Communication Manager sends during a system level 3 or higher reset that requests the VMS to refresh the Message Waiting (MW) lamps. Accepts up to six digits. Also accepts #, \*, and #00.

**System In Day Service**

This value is used by the Voice Mail System (VMS) to indicate that Communication Manager has changed from Night to Day Service. Accepts up to six digits. Also accepts #, \*, and #11.

**System In Night Service**

This value is used by the Voice Mail System (VMS) to indicate that Communication Manager has changed from Day to Night Service. Accepts up to six digits. Also accepts #, \*, and #12.

**OTHER RELATED PARAMETERS**

**DTMF Duration On**

| Valid Entry                    | Usage   |
|--------------------------------|---|
| 75 to 500 — in multiples of 25 | The duration in milliseconds of mode code digits sent to the VMS. This field cannot be blank. |

**Off**

| Valid Entry                             | Usage   |
|---|---|
| Between 75 and 200 — in multiples of 25 | The pause in milliseconds between mode code digits as they are sent to the VMS. This field cannot be blank. |

**Remote VMS Extensions- First**

The first remote UDP VMS hunt group extension. Available only if **Mode Code for Centralized Voice Mail** is enabled for the system.

**Related topics:**

[Mode Code for Centralized Voice Mail](#) on page 948

**Remote VMS Extensions - Second**

The second remote UDP VMS hunt group extension. This extension cannot be the same as the first Remote VMS Extension. Available only if **Mode Code for Centralized Voice Mail** is enabled for the system.

**Related topics:**

[Mode Code for Centralized Voice Mail](#) on page 948

## Sending Delay

| Valid Entry                     | Usage  |
|---------------------------------|--|
| 75 to 1000 — in multiples of 25 | The delay in milliseconds between the time answer supervision is received from the VMS and the time the first mode code digit is sent. This field cannot be blank. |

## VMS Hunt Group Extension

The extension of a hunt group containing VMI extensions. A check is made to verify that a valid hunt group extension is entered, but a check is not made to verify that the hunt group members are VMI extensions.

## Modem Pool Group

There are two types of conversion resources for Modem Pooling. The first type, an integrated conversion resource, is a circuit pack that emulates a Trunk Data Module connected to a 212A-type modem. Two conversion resources are on each circuit pack.

The second type, a combined conversion resource, is a separate Trunk Data Module and modem administered as a unit. The Trunk Data Module component of the conversion resource can be either a Modular Trunk Data Module (MTDM) or 7400A Data Module and connects to a digital port using Digital Communications Protocol (DCP); the modem connects to an analog port.

### Note:

The **Speed**, **Duplex**, and **Synchronization** fields cannot be filled out for the “integrated” pooled modem screens but can be assigned on the “combined” pooled modem screen. The integrated conversion resource automatically will adjust its speed and synchronization to the endpoint it is connected to. In synchronous mode, the integrated modem pool can operate at 1200 baud. In asynchronous mode, it can operate at 300 or 1200 baud. Full-duplex operation is always used.

Example command: `change modem-pool n`, where *n* is the modem pool number.

## Answer Supervision Timeout (sec)

Available only with a combined type modem pool.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 255    | The number of seconds to wait before the far-end answers. |
| 0           | No answer supervision                                     |

### Related topics:

[Group Type](#) on page 786

## CF-CB Common

If enabled, the CF and CB leads on the conversion resource are logically connected. Available only with an integrated type modem pool.

**Related topics:**

[Group Type](#) on page 786

**Direction**

The direction of the call for which the modem pool operates. Available only with a combined type modem pool.

| Valid Entry | Usage  |
|-------------|--|
| incoming    | Converts an analog signal to digital for the data endpoint       |
| outgoing    | Converts analog to digital (or digital to analog) for data calls |
| two-way     | Allows incoming and outgoing data communication                  |

**Related topics:**

[Group Type](#) on page 786

**Duplex**

The duplex mode of the conversion resources in the group. Entry required for a combined type modem pool.

| Valid Entry | Usage                                   |
|-------------|---|
| full        | Can talk and listen at the same time    |
| half        | Cannot talk and listen at the same time |

**Related topics:**

[Group Type](#) on page 786

**Group Number**

The modem pool group number.

**Group Type**

The type of physical model pool.

| Valid Entry | Usage  |
|-------------|--|
| integrated  | Maps to the Pooled Modem circuit pack                                |
| combined    | Maps to an external modem pool when a data module and a modem exists |

**Hold Time (min)**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 99     | The maximum number of minutes that a conversion resource in the group can be held while a call waits in a queue or reserved after Data Call Preindication. |

**Loss of Carrier Disconnect**

If enabled, permits conversion resource to disconnect if it detects a dropped carrier.

Available only with an integrated type modem pool.

**Related topics:**

[Group Type](#) on page 786

**Modem Name**

The name of the modem pool. Accepts from one to six characters. Available only with a combined type modem pool.

**Related topics:**

[Group Type](#) on page 786

**Receive Space Disconnect**

If enabled, allows the conversion resource to disconnect after receiving 1.6 seconds of space.

Available only with an integrated type modem pool.

**Related topics:**

[Group Type](#) on page 786

**Receiver Responds to Remote Loop**

If enabled, allows the far-end modem to put conversion resource into loop back mode.

Available only with an integrated type modem pool.

**Related topics:**

[Group Type](#) on page 786

**Send Space Disconnect**

If enabled, allows the conversion resource to send 4 seconds of space before disconnecting

Available only with an integrated type modem pool.

**Related topics:**

[Group Type](#) on page 786

**Speed**

| Valid Entry   | Usage  |
|---|--|
| LOW (0 to 300<br>blind sampled)<br>300<br>1200<br>2400<br>4800<br>9600<br>19200 | The communication speed in bits per second of the conversion resources in the group. One to three speeds are separated by slashes. For example, 300/1200/2400 indicates a maximum of three running speeds. Entry is required for a combined type modem pool. |

**Related topics:**

[Group Type](#) on page 786

**Synchronization**

The synchronization mode of the conversion resources in the group. Entry required for a combined type modem pool.

| Valid Entry | Usage        |
|-------------|--------------|
| sync        | Synchronous  |
| async       | Asynchronous |

**Related topics:**

[Group Type](#) on page 786

**Time Delay**

Available only with a combined type modem pool.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 255    | The time delay in seconds to insert between sending the ringing to the modem and the off-hook alert to the data module. |

**Related topics:**

[Group Type](#) on page 786

**CIRCUIT PACK ASSIGNMENTS**

***Circuit Pack Location***

The port associated with the conversion resource on the integrated modem pool circuit pack. Available only with an integrated type modem pool.

| Valid Entry                              | Usage  |
|--|--|
| 1 to 64                                  | First and second characters are the cabinet number |
| A to E                                   | Third character is the carrier                     |
| 0 to 20                                  | Fourth and fifth character are the slot number     |
| 01 to 04 (Analog TIE trunks)<br>01 to 31 | Six and seventh characters are the circuit number  |
| 1 to 250                                 | Gateway  |
| V1 to V9                                 | Module   |
| 01 to 31                                 | Circuit  |

**Example**

01A0612 is in cabinet 01, carrier A, slot 06, and circuit number (port) 12.

**Related topics:**

[Group Type](#) on page 786

**PORT PAIR ASSIGNMENTS****Analog Digital**

The port numbers of the modem/TDM pair in a conversion resource. Two port entries are required. Available only with a combined type modem pool.

| Valid Entry                              | Usage  |
|--|--|
| 1 to 64                                  | First and second characters are the cabinet number |
| A to E                                   | Third character is the carrier                     |
| 0 to 20                                  | Fourth and fifth character are the slot number     |
| 01 to 04 (Analog TIE trunks)<br>01 to 31 | Six and seventh characters are the circuit number  |
| 1 to 250                                 | Gateway  |
| V1 to V9                                 | Module   |
| 01 to 31                                 | Circuit  |

**Example**

01A0612 is in cabinet 01, carrier A, slot 06, and circuit number (port) 12.

**Related topics:**

[Group Type](#) on page 786

**MOH Group**

Use the MOH Group screen to define a collection of analog station and/or aux trunk port circuit pack ports that are connected to external audio sources for use with the Music on Hold feature.

Example command: `change moh-analog-group`

**MOH Source Location**

The Music-on-hold analog or aux-trunk port location

| Valid Entry                  | Usage  |
|------------------------------|--|
| 1 to 64                      | First and second characters are the cabinet number |
| A to E                       | Third character is the carrier                     |
| 0 to 20                      | Fourth and fifth character are the slot number     |
| 01 to 04 (Analog TIE trunks) | Six and seventh characters are the circuit number  |

| Valid Entry | Usage   |
|-------------|---------|
| 01 to 31    |         |
| 1 to 250    | Gateway |
| V1 to V9    | Module  |
| 01 to 31    | Circuit |

**Group Name**

The name that identifies the Music-on-hold (MOH) group.

**Multifrequency-Signaling-Related Parameters**

Sets the system or location parameters associated with multifrequency signaling.



**Note:**

With the Multinational Locations feature enabled, you can assign MFC signal sets per trunk group, rather than system-wide.

Example command: `change multifrequency-signaling`

**Related topics:**

[Multinational Locations](#) on page 948

**Multifrequency-Signaling-Related Parameters: page 1**

***ANI Prefix***

The prefix to apply to an extension when ANI is sent to the local telephone company central office. Accepts one to six digits.

Available only if the **Outgoing Call Type** is group-ii-mfc or mfe.

**Related topics:**

[Outgoing Call Type](#) on page 794

***Backward Cycle Timer (sec)***

Available only if the **Incoming Call Type** is mfe.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 255    | The number of seconds the system waits to send the check frequency after receiving an MFE signal. |

**Related topics:**

[Incoming Call Type](#) on page 792

***Collect All Digits Before Seizure***

Available only if the **Outgoing Call Type** is group-ii-mfc or mfe.

| Valid Entry | Usage  |
|-------------|--|
| y           | The system collects all the digits before seizing the trunk. Values administered for <b>ANI Req</b> for AAR and ARS Digit Conversion do not apply. |
| n           | ANI collection is controlled by ARS administration.  |

**Related topics:**

[ANI Req](#)

[Outgoing Call Type](#) on page 794

**Convert First Digit End-of-Dial To**

The digit used when the incoming initial end-of-ani or end-of-dial MF signal is converted on a per-switch basis.

Available only if **Private Group II Permissions and Public Interworking** is enabled.

**Related topics:**

[Private Group II Permissions and Public Interworking](#) on page 795

**Default ANI**

Available only if the **Outgoing Call Type** is group-ii-mfc or mfe.

| Valid Entry | Usage  |
|-------------|--|
| 2 to 15     | The switch or server identification number that is sent to the local telephone company central office (CO) when ANI is requested (by the CO) on a particular call but is not available, such as on tandem tie trunk calls. |
| blank       | Use for tandem switching. If blank, administer a value to send for ANI on outgoing calls when it is not available.   |

**Related topics:**

[Outgoing Call Type](#) on page 794

[ANI Not Available](#) on page 799

**Forward Cycle Timer (sec)**

Available only if the **Incoming Call Type** is mfe.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 255    | The number of seconds the system waits to receive the check frequency after sending an MFE signal. Communication Manager drops the call if the time runs out before it receives check frequency. |

**Related topics:**

[Incoming Call Type](#) on page 792

**Group II Called Party Category**

The type of Group II signals that should be used on the outgoing R2-MFC call. Available only if the **Outgoing Call Type** is group-ii-mfc and **Use COR for All Group II Responses** is disabled.

| Valid Entry | Usage   |
|-------------|---|
| user-type   | The type of telephone making the call determines the type of Group II signal that the switch or server sends (normal = ordinary telephone set, attendant = attendant console, data-call = data modules and similar data endpoints). |
| call-type   | The dialed digits determine the type of Group II signal that the server sends.  |

**Related topics:**

[Outgoing Call Type](#) on page 794

[Use COR for All Group II Responses](#) on page 796

**Incoming Call Type**

| Valid Entry                      | Usage   |
|----------------------------------|---|
| group-ii-mfc<br>non-group-ii-mfc | The signal type that a local telephone company central office uses to place an incoming call to the server. |
| mfe                              | Multi-frequency Espanol used for Spain  |

**Incomplete Dial Timer (sec)**

Available only if the **Incoming Call Type** is mfe.

| Valid Entry | Usage   |
|-------------|---|
| 45 to 255   | The number of seconds Communication Manager waits from the start of a call until the end of the check frequency of the last signal. Communication Manager drops the call if the time runs out before it receives the check frequency. |

**Related topics:**

[Incoming Call Type](#) on page 792

**Maintenance Call Type**

Available only if the **Incoming Call Type** is group-ii-mfc or non-group-ii-mfc.

| Valid Entry | Usage   |
|-------------|---|
| 1           | The Belgium maintenance sequence is indicated when the local telephone company central office (CO) sends an MFC maintenance tone. |
| 2           | The Saudi Arabian sequence is indicated when the CO sends an MFC maintenance tone.  |
| none        | Not administered.   |

**Related topics:**

[Incoming Call Type](#) on page 792

**Maximum Resend Requests**

The threshold number of resend type MFC signals the server running Communication Manager accepts during an outgoing call.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 99     | The number of resend requests.                        |
| 1           | The call is dropped if one resend signal is received. |
| blank       | An unlimited number of resend requests is allowed.    |

**MF Signaling Intercept Treatment - Incoming**

| Valid Entry | Usage  |
|-------------|--|
| y           | Sends the group B signal for the intercept to the local telephone company central office and play intercept tone on the trunk. |
| n           | Uses normal DID/TIE/ISDN intercept treatment.  |

**MF Signaling Intercept Treatment - Outgoing**

Defines the treatment for outgoing calls that cannot be completed as dialed. Available only if **Outgoing Call Type** is group-ii-mfc.

| Valid Entry  | Usage  |
|--------------|--|
| announcement | Plays a recorded announcement for outgoing calls that cannot be completed as dialed. You select and record the message. Requires entry of the extension number for the announcement. |
| tone         | Plays intercept tone for outgoing calls that cannot be completed as dialed.  |

**Related topics:**

[Outgoing Call Type](#) on page 794

**MFE Type**

Available only if the **Incoming Call Type** is mfe.

| Valid Entry | Usage   |
|-------------|---|
| 2/5<br>2/6  | Determines which public signaling Communication Manager uses. |

**Related topics:**

[Incoming Call Type](#) on page 792

**Outgoing Call Type**

| Valid Entry  | Usage   |
|--------------|---|
| group-ii-mfc | The signal type that the switch or server uses to place an outgoing call to a local telephone company central office. |
| mfe          | Multi-frequency Espanol used in Spain.  |
| none         | Not administered.   |

**Outgoing Forward Signal Absent Timer (sec)**

Available only if the **Outgoing Call Type** is group-ii-mfc.

| Valid Entry | Usage  |
|-------------|--|
| 11 to 255   | The maximum time to elapse between forward signals on outgoing calls. The timer starts and restarts when a forward tone is taken off the link, and it stops when the next forward tone is applied to the link. |

**Related topics:**

[Outgoing Call Type](#) on page 794

**Outgoing Forward Signal Present Timer (sec)**

Available only if the **Outgoing Call Type** is group-ii-mfc.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 255    | The maximum time to elapse between signals on a call. This timer runs when MFC tones are being sent or received on an outgoing call. The timer starts (and restarts) when Communication Manager begins sending a forward signal and stops when Communication Manager receives the backward signal. |

**Related topics:**

[Outgoing Call Type](#) on page 794

**Outgoing Start Timer (sec)**

Available only if the **Incoming Call Type** is mfe.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 255    | The number of seconds from seizure until the beginning of the first Group A signal from the receiving end, and from the end of the check frequency until the beginning receipt of the first digit following the Group II signal. |

**Related topics:**

[Incoming Call Type](#) on page 792

**Overlap Sending on Link-to-Link Tandem Calls**

If enabled, and calls are tandemed between servers, then ANI for the switch or server is sent to the terminating switch if that switch requests ANI before Communication Manager receives it from the originating server or switch. The terminating server or switch can request ANI before

the receipt of the last address digit if it is not running Communication Manager, or if Communication Manager is administered to request the call category at the start of the call.

If enabled, Communication Manager sends and receives digits one digit at a time instead of enbloc. With enbloc, digits are not sent until the entire group of digits is received.

Available only if **Collect All Digits Before Seizure** is disabled.

**Related topics:**

[Collect All Digits Before Seizure](#) on page 790

[Request Call Category at Start of Call](#) on page 798

**Private Group II Permissions and Public Interworking**

If enabled, then Communication Manager:

- Sends the category for MFC ANI for the COR of the originating party for non-private-MFC-trunk to MFC-private-trunk calls.
- Sends the Group II category received over the incoming private trunk as the outgoing Group II category on tandem private MFC calls.
- Applies MFC group II-CPC termination restrictions on incoming MFC private trunk calls.
- Checks station permissions for call forward off-net calls.

Available only if the **Incoming Call Type** is group-ii-mfc or non-group-ii-mfc and the **Outgoing Call Type** is group-ii-mfc or none.

**Related topics:**

[Incoming Call Type](#) on page 792

[Outgoing Call Type](#) on page 794

**Received Signal Gain (dB)**

| Valid Entry | Usage  |
|-------------|--|
| -15 to 3    | The number for the loss or gain when the MFC port listens to the trunk port. Communication Manager listens with a range of -5 to -35. This value moves the range (for example, a value of -5 provides a range of -10 to -40). Also applies to Russian MF Shuttle trunks. |

**Request Incoming ANI (non-AAR/ARS)**

If enabled, ANI is requested on incoming R2-MFC calls.

Available only if **Incoming Call Type** is group-ii-mfc or mfe and the **Outgoing Call Type** is group-ii-mfc or mfe. Applies only if the incoming call via the R2-MFC trunk is terminating to a local station on this PBX.

**Related topics:**

[Incoming Call Type](#) on page 792

[Outgoing Call Type](#) on page 794

**Transmitted Signal Gain (dB)**

| Valid Entry | Usage   |
|-------------|---|
| -15 to 3    | The number for the loss or gain when the trunk port listens to the MFC port. The MFC port generates at -5 for MFC and -8 for MFE. This field adds gain or loss to the starting value of -5. Also applies to Russian Shuttle trunks and Russian multi-frequency ANI. |

**Use COR for All Group II Responses**

If enabled, the COR administered category is used for both the calling party and called party categories.

Available only if the **Outgoing Call Type** is group-ii-mfc.

**Related topics:**

[Outgoing Call Type](#) on page 794

**Use COR for Calling Party Category**

Indicates the category to send with ANI if requested on an outgoing R2-MFC call. Available only if the **Outgoing Call Type** is group-ii-mfc and **Use COR for All Group II Responses** is disabled.

| Valid Entry | Usage  |
|-------------|--|
| y           | The calling facility's COR is used to determine category.        |
| n           | The calling party's user-type COR is used to determine category. |

**Related topics:**

[Outgoing Call Type](#) on page 794

[Use COR for All Group II Responses](#) on page 796

**NEXT ANI DIGIT**

**Related topics:**

[Incoming Call Type](#) on page 792

[Outgoing Call Type](#) on page 794

**Incoming**

Available only if the **Incoming Call Type** is group-ii-mfc and the **Outgoing Call Type** is group-ii-mfc or mfe.

| Valid Entry                              | Usage  |
|--|--|
| next-digit<br>next_ani_digit<br>send-ani | Determines whether the Next ANI Digit signal is the same as the send-ani signal, the next-digit signal, or another signal defined as next_ani_digit. |

**Outgoing**

Available only if the **Outgoing Call Type** is group-ii-mfc.

| Valid Entry                              | Usage   |
|--|---|
| next-digit<br>next_ani_digit<br>send-ani | Determines whether the Next ANI Digit signal is the same as the send-ani signal or the next-digit signal or another signal defined as next_ani_digit. |

**Related topics:**

[Outgoing Call Type](#) on page 794

**Multifrequency-Signaling-Related Parameters: page 2**

These fields define call category and ANI information. For India, the ANI can be requested without the call category information.

**Address Digits Include End-of-Digits Signal**

If enabled, indicates that an outgoing forward Group I end-of-digit signal is always sent after completion of address digits upon request from the local telephone company central office for outgoing calls.

**ANI Source for Forwarded & Covered Calls**

| Valid Entry | Usage  |
|-------------|--|
| caller      | Send the calling party's ANI when calls are redirected.    |
| forwarder   | Send the forwarding party's ANI when calls are redirected. |

**Call Category for Vector ii-digits**

If enabled, allows the use of the call category digit, which is part of ANI, as the ii-digits on call vector steps.

**Do Not Send Group B Signals to CO**

Available only if the **Incoming Call Type** is group-ii-mfc.

| Valid Entry | Usage  |
|-------------|--|
| y           | Does <i>not</i> send Group-B signals to complete an incoming call. |
| n           | Sends Group-B signals to complete an incoming call.                |

**Related topics:**

[Incoming Call Type](#) on page 792

**Number of Incoming ANI Digits**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 15     | The number of ANI digits for incoming MFC calls. |

**Number of Outgoing ANI Digits**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 15     | The number of ANI digits for outgoing MFC calls. |

| Valid Entry | Usage   |
|-------------|---|
|             | <p>In India or any country where end-of-ani and end-of-digits are not defined for Tones to CO on Outgoing Forward Calls - Group I, Avaya Communication Manager appends ANI-Not-Available digits to ANI digits if the actual ANI length is less than the number entered in this field. If end-of-ani or end-of-digits are defined, this field is used in conjunction with Truncate Station Number in ANI as a maximum ANI length. For India, even if the length of ANI is defined, if the timeout occurs during the ANI collection, the call is routed with the ANI digits already collected. Applies to Russian shuttle trunks, and MFC and MFE trunks.</p> |

**Outgoing II by COR**

Available only if either **Use COR for Calling Party Category** or **Use COR for All Group II Responses** are enabled.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 10     | <p>The Group II signal sent to the local telephone company central office on outgoing calls can be administered per COR (Class of Restriction) and per trunk group. The Group II signal is administered per COR. That per-COR value in turn can be mapped into a different outgoing signaling parameter set. The values for this field administer that outgoing mapping.</p> |

**Related topics:**

[Use COR for All Group II Responses](#) on page 796

[Use COR for Calling Party Category](#) on page 796

**Request Call Category at Start of Call**

Indicates that the Send-ANI backward signal requesting for the caller-category information is sequenced differently in the MFC signaling flow. The Caller-category Request backward signal is disjointed from the ANI request.

If enabled, the Send-ANI backward signal corresponds exclusively to the caller-category request. In response to this signal, Communication Manager sends a forward signal containing the caller-category information on outgoing calls. On incoming calls, Communication Manager sends the Send-ANI backward signal upon receipt of the first address signal.

**Request CPN at Start of Call**

Allows Communication Manager to collect ANI and call category immediately after receipt of the first address digit.

If enabled, provides ANI Calling Party Number (CPN) and call category immediately after receiving the first address digit.

Available only if the **Incoming Call Type** is group-ii-mfc.

**Related topics:**

[Incoming Call Type](#) on page 792

**Restart ANI from Caller Category**

If enabled, Avaya Communication Manager sends the caller-category signal later again when the signals for Caller-Category and ANI requests are the same and this signal is received after the Next-Digit forward signals have been received.

**Truncate Station Number in ANI**

Applies to Russian shuttle trunks, and MFC and MFE trunks.

| Valid Entry               | Usage  |
|---------------------------|--|
| beginning<br>ending<br>no | Defines the side of the extension number from which to truncate when station ANI is sent to the local telephone company central office and the combined length of the ANI prefix and extension number is greater than the administered Number of Outgoing ANI Digits. The ANI prefix (either MFC or COR) is not truncated. There is no effect if ANI for switch or server is sent. |

**Related topics:**

[Number of Outgoing ANI Digits](#) on page 797

**INCOMING / OUTGOING****ANI Available**

| Valid Entry      | Usage  |
|------------------|--|
| 1 to 15<br>blank | The signal number used for incoming ANI-Available. |

**ANI Not Available**

Required if the **Default ANI** is not administered.

| Valid Entry      | Usage   |
|------------------|---|
| 1 to 15<br>blank | The signal number used for outgoing ANI-Available. Communication Manager outpulses the End-of-Dial backward signal when the ANI-Not-Available forward signal is received on incoming calls. Communication Manager outpulses the ANI-Not-Available forward signal to the local telephone company central office on outgoing calls where ANI is not possible. |

**Multifrequency-Signaling-Related Parameters: page 3**

These fields define the meaning of MFC tones for calls originated at the local telephone company central office.

When the screen initially appears, either of two sets of default values is possible. One set is for the Group II call type; the other set is for non-Group II call type. In each set, the default value for each field is set to the most common value.

Available only if the **Incoming Call Type** is group-ii-mfc or non-group-ii-mfc.

**Related topics:**

[Incoming Call Type](#) on page 792

**INCOMING FORWARD SIGNAL TYPES (Tones from CO)**

Group I

Displays message codes 11 to 15. (Numbers 1 through 10 are assigned to the digits of the destination telephone number.) A Group I signal type can be administered for each code.

Group I signals are a set of forward signals generated by the originating server.

| Valid Entry   | Usage  |
|---------------|--|
| ani-avail     | Used in Hungary. If this signal is defined and Automatic Number Identification (ANI) is requested on outgoing R2-MFC calls, ANI is sent to the local telephone central office before ANI caller digits are sent. This signal is sent after the ANI caller category signal.<br>Available if <b>Incoming Call Type</b> is group-ii-mfc.                |
| ani-not-avail | Used on Direct Outward Dialing calls in Brazil and Columbia. Communication Manager sends this signal to the local telephone company central office when it receives an Automatic Number Identification (ANI) request and the caller's number is not available.<br>Available if <b>Incoming Call Type</b> is group-ii-mfc.                            |
| drop          | When this signal is received from the local telephone company central office, Avaya Communication Manager starts the disconnect sequence and drops the call.<br>Available if <b>Incoming Call Type</b> is group-ii-mfc or non-group-ii-mfc.  |
| end-of-ani    | This signal is used on Direct Outward Dialing and Direct Inward Dialing calls. Communication Manager sends this signal to indicate the end-of-ANI digits when Automatic Number Identification (ANI) digits are sent to the local telephone company central office.<br>Available if <b>Incoming Call Type</b> is group-ii-mfc.                        |
| end-of-dial   | This signal is used when open numbering is used on Direct Inward Dialing calls. The local telephone company central office sends this signal to indicate the end-of-dial digits and Communication Manager responds with a request for a Group II signal.<br>Available if <b>Incoming Call Type</b> is group-ii-mfc.                                  |
| ignored       | If this signal is received from the local telephone company central office, Communication Manager sends a corresponding signal (A.1, and so on) but no action is taken in the response and it is not counted as a digit. In Belgium, this signal is not acknowledged.<br>Available if <b>Incoming Call Type</b> is group-ii-mfc or non-group-ii-mfc. |
| maint-call    | The local telephone company central office (CO) sends a signal to indicate that a call is a maintenance call and Communication Manager prepares the special maintenance call sequences for the CO. This signal can be used on Direct Inward Dialing calls in Saudi Arabia.<br>Available if <b>Incoming Call Type</b> is group-ii-mfc.                |
| send-congest  | When Communication Manager receives this signal from the local telephone company central office (CO) on a Direct Inward Dialing call, it returns a congestion signal (Group A), in compel (not pulse) mode, to the CO.   |

| Valid Entry | Usage   |
|-------------|---|
|             | Available if <b>Incoming Call Type</b> is group-ii-mfc. |

## Group II

Displays message codes 1 to 15. A Group II signal type can be administered for each code. Group II signals are a more elaborate set of forward signals generated by the originating server.

| Valid Entry  | Usage   |
|--------------|---|
| attendant    | If Communication Manager receives this signal on Direct Inward Dialing (DID) calls, the call terminates at an attendant regardless of the extension dialed. On Direct Outward Dialing (DOD) calls, this signal is sent to the local telephone company central office (CO) if the CO requests calling-category information and the originating extension is an attendant. This signal is used on both DID and DOD calls.   |
| busy-rt-attd | If Communication Manager receives this signal on Direct Inward Dialing (DID) calls, the call terminates at an attendant if the called extension is busy or at the called extension if it is not busy. This signal is used on DID calls.   |
| data-call    | If Communication Manager receives this signal on Direct Inward Dialing (DID) calls, it sends intercept treatment. On Direct Outward Dialing (DOD) calls, this signal is sent to the local telephone company central office (CO) if the CO requests calling-category information and the originating extension is a data extension. This signal is used on both DID and DOD calls.   |
| data-verify  | If Communication Manager receives this signal on Direct Inward Dialing (DID) calls and the terminating extension is not a data extension, it sends intercept treatment. On Direct Outward Dialing (DOD) calls, this signal is sent to the local telephone company central office (CO) if the CO requests calling-category information and the originating extension is a data extension. This signal is used on both DID and DOD calls.                                       |
| drop         | When this signal is received from the local telephone company central office (CO), Communication Manager starts the disconnect sequence and drops the call.   |
| maint-call   | The local telephone company central office (CO) sends a signal to indicate that a call is a maintenance call and Avaya Communication Manager prepares the special maintenance call sequences for the CO.  |
| normal       | This signal indicates that the caller is a normal subscriber. If it is received on a Direct Inward Dialing (DID) call, the call is terminated at the called extension. For an outgoing MF signaling call that uses Group II signaling, this signal is sent to the local telephone company central office (CO) when the CO requests calling-category information and the originating extension is a station. This signal is used in both DID and Direct Outward Dialing calls. |

| Valid Entry    | Usage   |
|----------------|---|
| send-intercept | If Communication Manager receives this signal from the local telephone company central office (CO) on a Direct Inward Dialing call, it returns Group B intercept signal to the CO.  |
| toll-auto      | This signal is used in China. This signal indicates that a call is an automatic toll call. When the call terminates at a busy station and a special busy signal is defined, the busy signal is sent to the local telephone company central office. A special busy signal can be defined by choosing the option toll-busy on the incoming Group B signals. |
| toll-operator  | This signal, used in China, is treated as a normal subscriber signal. See the normal definition.  |

**INCOMING BACKWARD SIGNAL TYPES (Tones to CO)**

Group A

Displays message codes 11 to 15. (Numbers 1 through 10 are assigned to the digits of the destination telephone number.) A Group A signal type can be administered for each code.

Group A signals are backward signals generated by the destination server or switch.

| Valid Entry    | Usage  |
|----------------|--|
| congestion     | The local telephone company central office sends this signal to indicate that it is experiencing network congestion. When Communication Manager receives this signal on Direct Outward Dialing (DOD) calls, it drops the trunk and plays reorder tone to the calling party. This signal is used on DOD calls.                                      |
| end-of-dial    | This signal is sent to indicate the end of the address digit string. For MF Group II calls, this signal requests a Group II signal and switches the sender over to the Group B signaling mode. This signal is used on both Direct Inward Dialing and Direct Outward Dialing calls.   |
| intercept      | The local telephone company central office sends this signal to indicate the call has been terminated to an invalid destination. When Communication Manager receives this signal on Direct Outward Dialing (DOD) calls, it drops the trunk and plays intercept tone to the calling party. This signal is used on DOD calls.                        |
| next-ani-digit | Communication Manager sends this signal to request the next ANI digit. This signal is used on Direct Inward Dialing and Direct Outward Dialing calls.  |
| next-digit     | Communication Manager sends this signal to request the next digit. This signal is used on both Direct Inward Dialing and Direct Outward Dialing calls.   |
| send-ani       | The local telephone company central office (CO) sends this signal to request calling-party category and sends additional signals to request ANI digits. This signal is sent to the CO when Avaya Communication Manager requests ANI digits on Direct Inward Dialing (DID) calls. This signal is used on both Direct Outward Dialing and DID calls. |

| Valid Entry  | Usage   |
|--------------|---|
| setup-sppath | The local telephone company central office sends this signal to Communication Manager to set up a speech path. This signal is used on Direct Outward Dialing calls and on Direct Inward Dialing calls in Belgium. |

## Group B

Displays message codes between 1 and 15. A Group B signal type can be administered for each code

Group B signals enhance Group A signals for backward signaling from the destination end by providing the status of the called party. In addition, if the originating server uses Group II signals, the destination end answers with Group B signals.

Not available if **Do Not Send Group B Signals to CO** is enabled.

| Valid Entry | Usage  |
|-------------|--|
| busy        | This signal is sent to indicate that the called party is busy. On Direct Inward Dialing calls, the signal is sent to the local telephone company central office if there is no coverage point to terminate the call. If Communication Manager receives this signal on Direct Outward Dialing calls, it plays busy tone to the calling party and drops the trunk.   |
| congestion  | This signal is sent to indicate that the system is congested and the call cannot be terminated successfully. On Direct Inward Dialing calls, the signal is sent to the local telephone company central office to indicate that a resource is not available. On Direct Outward Dialing calls, if Communication Manager receives this signal, reorder tone is played to the calling party and the trunk is dropped.  |
| free        | This signal indicates that the called party is idle. On Direct Inward Dialing calls, the signal is sent to the local telephone company central office to indicate that the called party is idle and the call is terminated successfully. If Communication Manager receives this signal on Direct Outward Dialing calls, it connects the trunk to the calling party.  |
| intercept   | This signal indicates that the called party number is not in service or is not correct. On Direct Inward Dialing calls, if intercept treatment is set to provide a tone, tone is sent to the local telephone company central office to indicate that the called number is not valid. If Communication Manager receives the signal on Direct Outward Dialing calls, it plays intercept tone to the calling party and drops the trunk.   |
| mct         | This signal identifies the call as one that needs to be traced by the local telephone company central office (CO). Avaya Communication Manager then generates an MFC Call Trace Backward Signal administered for multifrequency signaling during call setup instead of the "free" signal. If the terminating station's Class of Restriction (COR) is enabled, the CO collects trace information before releasing the calling party. If the station's COR has MF Incoming Call Trace enabled and the "mct" signal is not defined, then the "free" signal is sent. |

| Valid Entry | Usage  |
|-------------|--|
| tariff-free | This signal is sent when the trunk group provides an 800 service. Avaya Communication Manager generates an MFC tariff-free backward signal during call setup instead of the "free" signal, facilitating local telephone company central office billing. If the trunk is administered as a tariff-free trunk and the "tariff-free" signal is not defined, then the "free" signal is sent. |
| tie-free    | This signal is used only when an incoming call is received and defined and the incoming facility is a tie trunk. Otherwise, the free signal is used.   |
| toll-busy   | This signal, used in China, is sent to indicate that the called party is busy if the call is an automatic toll call.   |

**Related topics:**

[Do Not Send Group B Signals to CO](#) on page 797

**Multifrequency - Signaling- Related Parameters: page 4**

The fields shown on this page define the meaning of MFC tones for calls originated at the switch or server.

This screen appears only if **Outgoing Call Type** is group-ii-mfc or mfe.

**Related topics:**

[Outgoing Call Type](#) on page 794

**OUTGOING FORWARD SIGNAL TYPES (Tones to CO)**

Group I

Displays message codes 11 to 15. (Numbers 1 through 10 are assigned to the digits of the destination telephone number.) A Group I signal type can be administered for each code.

Group I signals are a set of forward signals generated by the originating server.

| Valid Entry   | Usage  |
|---------------|--|
| ani-avail     | Used in Hungary. If this signal is defined and Automatic Number Identification (ANI) is requested on outgoing R2-MFC calls, ANI is sent to the local telephone central office before ANI caller digits are sent. This signal is sent after the ANI caller category signal. |
| ani-not-avail | Used on Direct Outward Dialing calls in Brazil and Columbia. Communication Manager sends this signal to the local telephone company central office when it receives an Automatic Number Identification (ANI) request and the caller's number is not available.             |
| end-of-ani    | This signal is used on Direct Outward Dialing and Direct Inward Dialing calls. Communication Manager sends this signal to indicate the end-of-ANI digits when Automatic Number Identification (ANI) digits are sent to the local telephone company central office.         |
| end-of-digits | This signal is sent by the originating server that makes outgoing calls, sends digits, and receives a next-digit Group A signal from the destination   |

| Valid Entry | Usage  |
|-------------|--|
|             | server or switch when there are no more digits to be sent. This signal is also sent when Communication Manager does not have end-of-ani assigned, makes an outgoing call, sends ANI, and receives a call-info-ani Group A signal from the destination end when there are no more Automatic Number Identification (ANI) digits to be sent. If both end-of-digits and end-of-ani are assigned, Communication Manager uses end-of-ani after it sends the last ANI digit and end-of-digits after sending the last called-number digit. |

## Group II

Displays message codes between 1 and 15. A Group II signal type can be administered for each code. Each entry can only appear once in the Group II column.

Group II signals are a more elaborate set of forward signals generated by the originating server.

| Valid Entry | Usage   |
|-------------|---|
| attendant   | If Communication Manager receives this signal on Direct Inward Dialing (DID) calls, the call terminates at an attendant regardless of the extension dialed. On Direct Outward Dialing (DOD) calls, this signal is sent to the local telephone company central office (CO) if the CO requests calling-category information and the originating extension is an attendant. This signal is used on both DID and DOD calls.   |
| data-call   | If Communication Manager receives this signal on Direct Inward Dialing (DID) calls, it sends intercept treatment. On Direct Outward Dialing (DOD) calls, this signal is sent to the local telephone company central office (CO) if the CO requests calling-category information and the originating extension is a data extension. This signal is used on both DID and DOD calls.   |
| normal      | This signal indicates that the caller is a normal subscriber. If it is received on a Direct Inward Dialing (DID) call, the call is terminated at the called extension. For an outgoing MF signaling call that uses Group II signaling, this signal is sent to the local telephone company central office (CO) when the CO requests calling-category information and the originating extension is a station. This signal is used in both DID and Direct Outward Dialing calls. |
| toll-auto   | This signal is used in China. This signal indicates that a call is an automatic toll call. When the call terminates at a busy station and a special busy signal is defined, the busy signal is sent to the local telephone company central office. A special busy signal can be defined by choosing the option toll-busy on the incoming Group B signals.   |

## **OUTGOING BACKWARD SIGNAL TYPES (Tones from CO)**

### Group A

Displays message codes between 1 and 15. A Group A signal type can be administered for each code.

Group A signals are backward signals generated by the destination server or switch.

| Valid Entry    | Usage  |
|----------------|--|
| congestion     | The local telephone company central office sends this signal to indicate that it is experiencing network congestion. When Communication Manager receives this signal on Direct Outward Dialing (DOD) calls, it drops the trunk and plays reorder tone to the calling party. This signal is used on DOD calls.                                      |
| drop           | When this signal is sent, the receiving end starts the disconnect sequence.  |
| end-of-dial    | This signal is sent to indicate the end of the address digit string. For MF Group II calls, this signal requests a Group II signal and switches the sender over to the Group B signaling mode. This signal is used on both Direct Inward Dialing and Direct Outward Dialing calls.   |
| intercept      | The local telephone company central office sends this signal to indicate the call has been terminated to an invalid destination. When Communication Manager receives this signal on Direct Outward Dialing (DOD) calls, it drops the trunk and plays intercept tone to the calling party. This signal is used on DOD calls.                        |
| last-2-digits  | Communication Manager sends this signal to adjust the outpulsing pointer so that the last three digits can be resent. This signal is used on Direct Outward Dialing calls.   |
| last-3-digits  | Communication Manager sends this signal to adjust the outpulsing pointer so that the last four digits can be resent. This signal is used on Direct Outward Dialing calls.  |
| last-digit     | Communication Manager sends this signal to adjust the outpulsing pointer so that the last two digits can be resent. This signal is used on Direct Outward Dialing calls.   |
| next-ani-digit | Communication Manager sends this signal to request the next ANI digit. This signal is used on Direct Inward Dialing and Direct Outward Dialing calls.  |
| next-digit     | Communication Manager sends this signal to request the next digit. This signal is used on both Direct Inward Dialing and Direct Outward Dialing calls.   |
| restart        | Communication Manager sends this signal to request the whole digit string again. This signal is used on Direct Outward Dialing calls.  |
| resend-digit   | Communication Manager sends this signal to adjust the outpulsing pointer so that the last digit can be resent again. This signal is used on Direct Outward Dialing calls.  |
| send-ani       | The local telephone company central office (CO) sends this signal to request calling-party category and sends additional signals to request ANI digits. This signal is sent to the CO when Avaya Communication Manager requests ANI digits on Direct Inward Dialing (DID) calls. This signal is used on both Direct Outward Dialing and DID calls. |

| Valid Entry  | Usage   |
|--------------|---|
| setup-sppath | The local telephone company central office sends this signal to Communication Manager to set up a speech path. This signal is used on Direct Outward Dialing calls and on Direct Inward Dialing calls in Belgium. |

## Group B

Displays message codes between 1 and 15. A Group B signal type can be administered for each code.

Group B signals enhance Group A signals for backward signaling from the destination end by providing the status of the called party. In addition, if the originating server uses Group II signals, the destination end answers with Group B signals.

| Valid Entry | Usage  |
|-------------|--|
| busy        | This signal is sent to indicate that the called party is busy. On Direct Inward Dialing calls, the signal is sent to the local telephone company central office if there is no coverage point to terminate the call. If Communication Manager receives this signal on Direct Outward Dialing calls, it plays busy tone to the calling party and drops the trunk.   |
| congestion  | This signal is sent to indicate that the system is congested and the call cannot be terminated successfully. On Direct Inward Dialing calls, the signal is sent to the local telephone company central office to indicate that a resource is not available. On Direct Outward Dialing calls, if Communication Manager receives this signal, reorder tone is played to the calling party and the trunk is dropped.  |
| free        | This signal indicates that the called party is idle. On Direct Inward Dialing calls, the signal is sent to the local telephone company central office to indicate that the called party is idle and the call is terminated successfully. If Communication Manager receives this signal on Direct Outward Dialing calls, it connects the trunk to the calling party.  |
| intercept   | This signal indicates that the called party number is not in service or is not correct. On Direct Inward Dialing calls, if intercept treatment is set to provide a tone, tone is sent to the local telephone company central office to indicate that the called number is not valid. If Communication Manager receives the signal on Direct Outward Dialing calls, it plays intercept tone to the calling party and drops the trunk.   |
| mct         | This signal identifies the call as one that needs to be traced by the local telephone company central office (CO). Avaya Communication Manager then generates an MFC Call Trace Backward Signal administered for multifrequency signaling during call setup instead of the "free" signal. If the terminating station's Class of Restriction (COR) is enabled, the CO collects trace information before releasing the calling party. If the station's COR has MF Incoming Call Trace enabled and the "mct" signal is not defined, then the "free" signal is sent. |
| tariff-free | This signal is sent when the trunk group provides an 800 service. Avaya Communication Manager generates an MFC tariff-free backward signal   |

| Valid Entry | Usage   |
|-------------|---|
|             | during call setup instead of the "free" signal, facilitating local telephone company central office billing. If the trunk is administered as a tariff-free trunk and the "tariff-free" signal is not defined, then the "free" signal is sent. |
| toll-busy   | This signal, used in China, is sent to indicate that the called party is busy if the call is an automatic toll call.  |

## Multiple Level Precedence & Preemption (MLPP) Parameters

Use this screen to set up system parameters for the Multiple Level Precedence & Preemption feature.

Example command: `change system-parameters mlpp`

### ANNOUNCEMENTS

#### ***Blocked Precedence Level***

The extension of the Blocked Precedence Level announcement.

#### ***Busy, Not Equipped***

The extension of the Busy, Not Equipped for Preemption announcement.

#### ***Service Interruption***

The extension of the Service Interruption announcement.

#### ***Unauthorized Precedence Level***

The extension of the Unauthorized Precedence Level announcement.

#### ***Vacant Code***

The extension of the Vacant Code announcement.

### PRECEDENCE CALLING-DIALED DIGIT ASSIGNMENT

#### **Caution:**

Avaya recommends that you do not change the default Precedence Calling dialed digits unless you are coordinating this change with other companion networks in your system. If the Precedence Calling digits do not match across networks, the system does not properly process the calls. Each of the Precedence Calling digits must be different. You cannot use the same digit for two different precedence levels.

#### ***Attendant Diversion Timing (sec)***

| Valid Entry       | Usage   |
|-------------------|---|
| 10 to 99<br>blank | Controls how many seconds this type of call rings before the call is routed to the Remote Attendant Route String that consists of any valid telephone number on the network. Attendant Diversion Timing is usually a backup answering position for the remote attendant console. The Remote Attendant Route String does not raise the precedence level of the call. |

**Default Route Digit**

Available only if Worldwide Numbering Dial Plan is enabled. A valid digit is required in this field.

| Valid Entry | Usage                          |
|-------------|--------------------------------|
| 0           | Voice call (the default value) |
| 1           | Circuit switched data call     |
| 2           | Satellite avoidance call       |
| 3           | (reserved)                     |
| 4           | (reserved)                     |
| 5           | Hotline voice grade call       |
| 6           | Hotline data grade call        |
| 7           | (reserved)                     |
| 8           | (reserved)                     |
| 9           | (reserved)                     |

**Related topics:**

[Worldwide Numbering Dial Plan Active](#) on page 810

**Default Service Domain**

| Valid Entry   | Usage  |
|---------------|--|
| 0 to 16777215 | The system service domain number. This number must be unique within a switching network. The system uses the system service domain to determine eligibility for precedence calling when interswitch precedence calls over non-ISDN trunks occur. |

**Flash**

The digit assignment for Flash precedence level calls. The default is 1.

**Flash Override**

The digit assignment for Flash Override precedence level calls. The default is 0.

**Immediate**

The digit assignment for Immediate precedence level calls. The default is 2.

**ISDN Precedence Call Timeout (sec)**

| Valid Entry | Usage  |
|-------------|--|
| 4 to 30     | The timeout seconds used instead of the Precedence Call Timeout when the call is from a Multiple Level Precedence and Preemption (MLPP) ISDN-PRI trunk. Default is 30 seconds. |

**Line Load Control Restriction Level**

Determines what stations, based on their COR, are restricted from originating calls.

| Valid Entry | Usage  |
|-------------|--|
| 0           | Feature not active (no restrictions). This is the default.       |
| 2           | Restrict stations with a COR assigned to LLC levels 2, 3, and 4. |
| 3           | Restrict stations with a COR assigned to LLC levels 3 and 4.     |
| 4           | Restrict stations with a COR assigned to LLC level 4.            |

**Precedence Call Timeout (sec)**

| Valid Entry | Usage  |
|-------------|--|
| 4 to 30     | The number of seconds a precedence call remains in call waiting status before it is diverted. A busy user receives a precedence call waiting tone only if the incoming call cannot be connected and cannot preempt the user. The called party hears the tone every 10 seconds until answered or the administered time-out occurs. If ignored, the caller is diverted to an attendant or a call-forwarded station. The default is 30 seconds. |

**Preempt Emergency Call**

If enabled, allows preemption of an Emergency 911 call made from a preemptable station by a higher precedence call.

**Priority**

The digit assignment for Priority precedence level calls. The default is 3.

**Remote Attendant Route String**

A user-defined telephone to which a precedence call can be routed when no console or night telephone is administered. Accepts from 1 to 24 digits.

**Routine**

The digit assignment for Routine precedence level calls. The default is 4.

**W NDP Emergency 911 Route String**

This route string is outpulsed when a user dials either 911 and waits for the interdigit timeout, or dials 911 followed by #. This dialing option only works when the W NDP Flash FAC is 91. Use a trunk access code (TAC), the AAR or the ARS access code, a W NDP access code, or an extension. For a W NDP access code, use the access code for the lowest precedence calling level in the system. Accepts from 1 to 24 digits.



**Note:**

An Emergency/911 call is a call that routes using the ARS table with the call type defined as either “alrt” or “emer”.

**Worldwide Numbering Dial Plan Active**

Enables or disables the Worldwide Numbering Dial Plan. Disabled by default.

## Music Sources

Use this screen to define music sources for Tenant Partitions. Each music source defined on this screen can be used by one or more Tenant Partitions. However, a partition can have only one music source.

 **Note:**

If you use equipment that rebroadcasts music or other copyrighted materials, you might be required to obtain a copyright license from, or pay fees to, a third party. You can purchase a Magic Hold system, which does not require such a license, from Avaya Inc. or Avaya's business partners.

Available only if **Tenant Partitioning** is enabled for the system.

Example command: `change music-sources`

**Related topics:**

[Tenant Partitioning](#) on page 949

### Description

A description of the administered music source. Accepts up to 20 alphanumeric characters. Available only if music or tone is administered for treatment for hold.

**Related topics:**

[Type \(Column\)](#) on page 811

### Source

Available only if music is administered for treatment for hold.

| Valid Entry | Usage  |
|-------------|--|
| ext         | Audio source extension for a single or group audio source. |
| group       | A Music-on-Hold analog group number.                       |
| port        | An analog or auxiliary trunk source location.              |

**Related topics:**

[Type \(Column\)](#) on page 811

### Source No

The number assigned to this music source.

### Type (Column)

| Valid Entry           | Usage   |
|-----------------------|---|
| music<br>tone<br>none | The type of treatment to be provided by the music source. Only one music source can use the tone value. |

**Type (field)**

Available only if music is administered for treatment for hold.

| Valid Entry          | Usage   |
|----------------------|---|
| ext<br>group<br>port | <p>The source for the music on hold. The source can be an announcement extension, an audio group, or a port on a VAL board.</p> <p> <b>Note:</b><br/>A source identifier (extension number, audio group number, or port number) must be administered with the source type.</p> |

**Related topics:**

[Type \(Column\)](#) on page 811

**Network Facilities**

Used to administer new network-provided service or feature names and corresponding ISDN PRI (network specific facilities information element) encodings, for call-by-call trunk groups. Values for pre-defined facilities are displayed at the top of the screen and are display-only. User-defined facilities and services can be entered in the fields below.

When **Usage Allocation Enhancements** is enabled for the system, this screen appears, allowing for administration of additional user-defined entries.

Example command: `change isdn network-facilities`

**Facility Coding**

The ISDN-specified value for this service or feature.

**Facility Type**

The facility type. For types 2 and 3, **Usage Allocation Enhancements** must be enabled for the system.

| Valid Entry  | Usage                                |
|--------------|--------------------------------------|
| 0 - feature  | Predefined features.                 |
| 1 - service  | Predefined services.                 |
| 2 - incoming | An incoming-type user-defined entry. |
| 3 - outgoing | An outgoing-type user-defined entry. |

**Related topics:**

[Usage Allocation Enhancements](#) on page 950

**Name**

The name for the feature or service.

## Node Number Routing

Specifies the routing pattern associated with each node in a public or private network. Node Number Routing is a required capability for Extension Number Portability (ENP) and is associated with the Uniform Dial Plan (UDP).

Example command: `change node-routing n`, where *n* is the node number.

### Node Number

The node number.

### Partitioned Group Number

The partitioned group number associated with the node numbers being administered.

### Route Pat

| Valid Entry       | Usage  |
|-------------------|--|
| 1 to 254<br>blank | The routing pattern associated with the corresponding node number. |

## Numbering-Private Format

Supports Private Numbering Plans (PNP). The screen specifies the digits to be put in the Calling Number information element (IE), the Connected Number IE, and the QSIG Party Number for extensions in the Private Numbering Plan.

Communication Manager supports private-network numbers up to 15 digits long. If the total number — including the level 1 and 2 prefixes, the PBX identifier, and the extension — is more than 15 digits long, neither QSIG Party Numbers nor the information elements are created or sent.

Example command: `change private-numbering n`, where *n* is the extension length.

### Ext Code

In the case of a four-digit **Ext Len**, an **Ext Code** of 12 is the equivalent of all extensions of the screen 12xx, excluding any explicitly listed longer codes. If a code of 123 is also listed, the 12 code is equivalent of all extensions of the screen 12xx except extensions of the screen 123x. The coding precludes having to list all the applicable 12xx extensions.

| Valid Entry      | Usage  |
|------------------|--|
| 0 to 13<br>blank | Accepts up to 13 digits depending on the administered extension length. When 0 alone is entered, the administered extension length must be 1 and the DDD number must be 10 digits. |
| attd             | Generates a private calling number for a call from the attendant group.  |

### Related topics:

[Ext Len](#) on page 814

**Ext Len**

| Valid Entry      | Usage  |
|------------------|--|
| 0 to 13<br>blank | The number of digits the extension can have.<br>Corresponds to the extension lengths allowed by the dial plan. |

**Maximum Entries**

The maximum number of private numbering entries that can be administered on the system.

**Private Prefix**

The number that is added to the beginning of the extension to form a Private Identification Number. The length of the prefix and the extension must at least equal the total length.

**Total Administered**

The number of private numbering entries currently administered on the system.

**Total Len**

| Valid Entry | Usage                               |
|-------------|-------------------------------------|
| 0 to 13     | The total number of digits to send. |

**Trk Grp(s)**

Communication Manager generates the station’s identification number if **Ext Code** is administered, and this field is administered with the trunk group number carrying the call. Accepts one to seven digits. If blank, the identification numbers are not dependent on the trunk group carrying the call.

**Related topics:**

[Ext Code](#) on page 813

**Numbering — Public/Unknown Format**

Specifies the desired digits for the Calling Number IE and the Connected Number IE (in addition to the QSIG Party Number) for any extension in the Public and/or Unknown Number Plans.

This screen is used for ARS public trunks as well as SIP Enablement Services (SES) trunks. It supports the ISDN Call Identification Display feature. The feature provides a name/number display for display-equipped stations within an ISDN network. The system uses the caller’s name and number and displays it on the called party’s display. Likewise, the called party’s name and number can be displayed on the caller’s display.

Administer this screen if either **Send Calling Number** or **Send Connected Number** is specified, or **Supplementary Service Protocol** is b on the Trunk Group screen.

 **Note:**

If the table is not properly administered and **Send Calling Number** or **Send Connected Number** is y or r and **Numbering Format** on the ISDN Trunk Group screen is public or unknown, the Calling Number and Connected Number IE are not sent. If the table is not

administered, but the **Send Calling Number** or **Send Connected Number** is public or unknown, the Identification Number (PartyNumber data type) is not sent for QSIG PartyNumbers. In this case, the ASN.1 data type containing the PartyNumber (PresentedAddressScreened, PresentedAddressUnscreened, PresentedNumberScreened, or PresentedNumberUnscreened) will be sent marked as PresentationRestricted with NULL for the associated digits.

Example command: `change public-unknown-numbering n`, where *n* is the extension length.

#### Related topics:

[Numbering Format](#) on page 742

[Send Calling Number](#) on page 745

[Send Connected Number](#) on page 746

[Supplementary Service Protocol](#) on page 1005

#### CPN Prefix

The number that is added to the beginning of the extension to form a Calling or Connected Number.

Only digits are allowed. Leading spaces, or spaces in between the digits, are not allowed. Accepts up to 15 digits.

- If the length of the CPN Prefix matches the Total CPN Length, the extension number is not used to formulate the CPN number.
- If the number of digits in the CPN Prefix plus the extension length exceeds the administered Total CPN Length, excess leading digits of the extension are deleted when formulating the CPN number.
- If the number of CPN Prefix digits plus the extension length is less than the Total CPN Length, the entry is not allowed.
- If the Total CPN Length is 0, no calling party number information is provided to the called party and no connected party number information is provided to the calling party.

If blank, the extension is sent unchanged. This is useful in countries where the public network is able to insert the appropriate CPN Prefix to form an external DID number.

#### Ext Code

In the case of a four-digit **Ext Len**, an **Ext Code** of 12 is the equivalent of all extensions of the screen 12xx, excluding any explicitly listed longer codes. If a code of 123 is also listed, the 12 code is equivalent of all extensions of the screen 12xx except extensions of the screen 123x. The coding precludes having to list all the applicable 12xx extensions.

| Valid Entry      | Usage  |
|------------------|--|
| 0 to 13<br>blank | Accepts up to 13 digits depending on the administered extension length. When 0 alone is entered, the administered extension length must be 1 and the DDD number must be 10 digits. |
| attd             | Generates a private calling number for a call from the attendant group.  |

**Related topics:**

[Ext Len](#) on page 814

**Ext Len**

| Valid Entry      | Usage  |
|------------------|--|
| 0 to 13<br>blank | The number of digits the extension can have.<br>Corresponds to the extension lengths allowed by the dial plan. |

**Total CPN Len**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 15     | The number of digits the extension can have.      |
| blank       | Used when deleting an entry. This is the default. |

**Trk Grp(s)**

Communication Manager generates the station's identification number if **Ext Code** is administered, and this field is administered with the trunk group number carrying the call. Accepts one to seven digits. If blank, the identification numbers are not dependent on the trunk group carrying the call.

**Related topics:**

[Ext Code](#) on page 813

## Off-PBX Telephone Mobile Feature Extensions

Example command: `change off-pbx-telephone mobile-feature-ext`

**Mobile Call (CTI) Extension**

A CTI call to this Mobile Feature Extension (MCE) creates an OPTIM call under CTI influence. A call to the MCE triggers an OPTIM extend-call from a desk phone to its mapped cell phone number and to the destination. All calls made using the MCE appear to the destination as if they were dialed from the desk phone.

## Partition Routing Table

Identifies routing for partition groups associated with an ARS analysis entry.

Example command: `change partition-route-table n`, where *n* is the routing index.

**PGN 1 (through PGN 8)**

The routing for each partition group associated with each route index number.

| Valid Entry | Usage                                     |
|-------------|---|
| 1 to 640    | The route pattern used to route the call. |

| Valid Entry | Usage   |
|-------------|---|
| r1 to r32   | The remote home numbering plan area table used to route the call. |
| node        | Node number routing.  |
| deny        | Blocks the call.  |

## Personal CO Line Group

Sets up a personal central office line trunk group.

Example command: `add personal-co-line n`, where *n* is the personal central office line trunk group number.

### Personal CO Line Group: page 1

#### CDR Reports

| Valid Entry    | Usage  |
|----------------|--|
| y              | All outgoing calls on this trunk group generate call detail records. If <b>Record Outgoing Calls Only</b> is disabled for CDR, incoming calls on this trunk group also generate call detail records.   |
| n              | Calls over this trunk group do not generate call detail records.   |
| r (ring-intvl) | CDR records are generated for both incoming and outgoing calls. In addition, the following ringing interval CDR records are generated: <ul style="list-style-type: none"> <li>• <b>Abandoned calls:</b> The system creates a record with a condition code of "H" indicating the time until the call was abandoned.</li> <li>• <b>Answered calls:</b> The system creates a record with a condition code of "G" indicating the interval from start of ring to answer.</li> <li>• <b>Calls to busy stations:</b> The system creates a record with a condition code of "I" indicating a recorded interval of 0.</li> </ul> |

#### Related topics:

[Record Outgoing Calls Only](#) on page 474

#### Coverage Path

| Valid Entry | Usage  |
|-------------|--|
| 1 to 9999   | The number of the call coverage path to use for incoming calls.      |
| t1 to t999  | The number of a time-of-day coverage table.                          |
| blank       | No coverage path is assigned. Assigning a coverage path is optional. |

#### Data Restriction

Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be

changed by the telephone user. Cannot be assigned if **Auto Answer** is administered as all or acd. If enabled, whisper page to this station is denied.

**Related topics:**

[Auto Answer](#) on page 61

**Group Name**

A unique name that provides information about the trunk group. Accepts up to 27 characters.

This field should contain names that identify the vendor and function of the trunk group rather than the group type (DID, WATS).

 **Note:**

Supported by Unicode language display for the 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones. Unicode is also an option for the 2420J telephone when the **Display Character Set** is katakana. For more information on the 2420J, see *2420 Digital Telephone User's Guide*.

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Related topics:**

[Display Character Set](#) on page 938

**Group Number**

The trunk group number.

 **Note:**

For trunk groups connecting two servers in Distributed Communication System networks, assign the same group number on both servers.

**Group Type**

The type of trunk group. The fields that are displayed and available might change according to the trunk group type selected.

| Valid Entry | Usage  |
|-------------|--|
| Access      | Used to connect satellite servers to the main switch in Electronic Tandem Networks (ETN). Access trunks do not carry traveling class marks (TCM) and thus allow satellite callers unrestricted access to out-dial trunks on the main server. This entry allows Inband ANI. |
| APLT        | Advanced Private Line Termination (APLT) trunks. Used in private networks. This entry allows Inband ANI.   |
| CAMA        | Used to route emergency calls to the local community's Enhanced 911 systems.   |
| CO          | Typically used to connect Communication Manager to the local telephone company central office, but can also connect adjuncts such as external paging systems and data modules.   |

| Valid Entry | Usage  |
|-------------|--|
| CPE         | Used to connect adjuncts, such as paging systems and announcement or music sources, to the server running Communication Manager.   |
| DID         | Used to direct callers directly to individuals within an organization without going through an attendant or some other central point. This entry allows Inband ANI.  |
| DIOD        | Two-way trunks that are used to transmit dialed digits in both directions. In North America, tie trunks are used for applications that require two-way transmission of dialed digits. This entry allows Inband ANI.  |
| DMI-BOS     | Digital Multiplexed Interface - Bit-Oriented Signaling (DMI-BOS) trunks allow communication with systems using DMI-BOS protocol. This entry also allows Inband ANI.  |
| FX          | A local telephone company central office (CO) trunk that connects the server running Communication Manager directly to a CO outside the local exchange area. Used to reduce long-distance charges if the organization averages a high volume of long-distance calls to a specific area code.   |
| ISDN        | Used when digital trunks are needed that can integrate voice, data, and video signals and provide the bandwidth needed for applications such as high-speed data transfer and video conferencing. ISDN trunks can also efficiently combine multiple services on one trunk group.<br>Also used for <b>Network Call Transfer</b> .<br><br> <b>Note:</b><br>Available only if <b>ISDN-PRI</b> , <b>ISDN-BRI Trunks</b> , or both have been enabled for the system. |
| RLT         | Used with Centralized Attendant Service in a private network.  |
| SIP         | Used to connect a server running Communication Manager to a SIP Enablement Services (SES) home server, or to connect two Communication Manager servers.<br><br> <b>Note:</b><br>The Automatic CallBack, Priority Calling, and Whisper Page features do not work correctly if each of the call's parties is using a SIP endpoint administered on and managed by a different instance of Communication Manager.   |
| Tandem      | Used to connect tandem nodes in a private network. This entry allows Inband ANI.   |
| Tie         | Used to connect a server running Communication Manager to a local telephone company central office or to another server or switch in a private network. Tie trunks transmit dialed digits with both outgoing and incoming calls. This entry also allows Inband ANI.  |
| WATS        | Used to reduce long-distance bills when your organization regularly places many calls to a specific geographical area in North America. Outgoing WATS service allows calls to certain areas ("WATS band") for  |

| Valid Entry | Usage   |
|-------------|---|
|             | a flat monthly charge. Incoming WATS trunks allow toll-free calling to customers and employees. |

**Related topics:**

- [Local Country Code](#) on page 605
- [International Access Code](#) on page 605
- [Carrier Medium](#) on page 722
- [Supplementary Service Protocol](#) on page 737
- [SBS](#) on page 744
- [Path Replacement](#) on page 750
- [Call Still Held](#) on page 821
- [ISDN-BRI Trunks](#) on page 947
- [ISDN-PRI](#) on page 947

**Outgoing Display**

Allows display telephones to show the name and number of the trunk group used for an outgoing call before the call is connected.

| Valid Entry | Usage                                     |
|-------------|---|
| y           | Displays the trunk group name and number. |
| n           | Displays the digits the caller dials.     |

**Security Code**

The code users must dial to retrieve voice messages and to use the Demand Print Message feature. Accepts from three to eight digits.

**TAC**

The trunk access code (TAC) that must be dialed to access the trunk group. A different TAC must be assigned to each trunk group. CDR reports use the TAC to identify each trunk group. The characters “\*” and “#” can be used as the first character in a TAC. Accepts a one- to four-digit number.

**TRUNK PARAMETERS**

**Analog Loss Group**

Determines which administered two-party row in the loss plan applies to this trunk group if the call is carried over an analog signaling port in the trunk group.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 17     | The index into the loss plan and tone plan. If values are administered other than in between 6 and 10 or 15 and 17, a warning message displays stating that the loss group may not be appropriate for this trunk group. |

### Answer Supervision Timeout

| Valid Entry | Usage   |
|-------------|---|
| 0 to 250    | The number of seconds Communication Manager waits before it acts as though answer supervision has been received from the far-end. During a cut-through operation, timing begins after each outgoing digit is sent and timing ceases after the far-end sends answer supervision. On senderized operation, the timer begins after the last digit collected is sent. |



**Note:**

This field's setting does not override answer supervision sent from the network or from DS1 port circuit timers.

**Related topics:**

[Administer Timers](#) on page 733

[Receive Answer Supervision](#) on page 825

### Call Still Held

If enabled, the system prevents glare by extending the Incoming Glare Guard timer and delaying an outgoing seizure of a trunk for at least 140 seconds after it is released from an incoming call. This field is used when the receiving end media server or switch initiates the disconnection of incoming calls. This field affects only TN438B, TN465B, and TN2147 ports and is used primarily when the **Country** code is 2.

Available only for co or fx trunk groups.

**Related topics:**

[Group Type](#) on page 725

### Charge Conversion

Available only for outgoing or two-way CO, DIOD, FX, and WATS trunk groups.

| Valid Entry    | Usage  |
|----------------|--|
| 1 to 64<br>500 | Communication Manager multiplies the number of charge units by the value of this field and displays it as a currency amount. Without a value in this field, Communication Manager displays the number of charge units without converting it to currency. |

**Related topics:**

[Direction](#) on page 724

[Trunk Direction](#) on page 825

### Charge Type

Text string used to describe charges related to a telephone call. These words or characters appear on telephone displays after the charge amount. Typically uses either the currency symbol or the charge type, but not both. Accepts up to seven characters. Embedded spaces count as characters.

Available only for outgoing or two-way CO, DIOD, FX, and WATS trunk groups.

**Related topics:**

[Direction](#) on page 724

**Country**

The country code that corresponds to the protocol used by the local telephone company central office (CO) where the trunk group terminates.

Available only for trunk groups that connect Communication Manager to a CO in the public network — CO, DID, DIOD, FX, and WATS trunk groups.

 **Caution:**

Customers should not attempt to administer this field. Please contact your Avaya technical support representative for assistance.

| Valid Entry            | Usage   |
|------------------------|---|
| 1 to 25, except for 19 | For a list of country codes, see the <i>Country code table</i> .  |
| 11                     | Communication Manager is administered for Public Network Call Priority (Call Retention and Re-ring).                              |
| 14                     |   |
| 15                     | Communication Manager is administered for Public Network Call Priority (Intrusion and Re-ring).                                   |
| 18                     | Communication Manager is administered for Public Network Call Priority (Mode of Release Control, Forced Disconnect, and Re-ring). |
| 23                     | If the trunk <b>Group Type</b> is either CO or DID, Communication Manager is administered for Block Collect Calls.                |

**Related topics:**

[Trunk Gain](#) on page 826

[Trunk Termination](#) on page 827

[Country options table](#) on page 935

**Currency Symbol**

The symbol that appears on telephone displays before the charge amount. Accepts from one to three characters. Leading and embedded spaces count as characters.

Available only for outgoing or two-way CO, DIOD, FX, and WATS trunk groups.

**Related topics:**

[Direction](#) on page 724

[Trunk Direction](#) on page 825

**Decimal Point**

The appropriate representation for a decimal point as it appears on telephone displays. Available only with outgoing or two-way CO, DIOD, FX, and WATS trunk groups.

 **Note:**

If the received charge contains no decimals, no decimal point is displayed (that is, the administered decimal point is ignored for charge information received with no decimals). On a QSIG trunk group, unlike other trunk groups, the **Decimal Point** field does not drive whether a decimal point appears on the calling display. Instead, it tells what symbol should be displayed if the QSIG AOC received has a 1/10 or 1/100 or 1/1000 Multiplier.

| Valid Entry | Usage   |
|-------------|---|
| comma       | If the received charge contains decimals, the charge is displayed at the calling endpoint's display with a comma as the decimal point. Divides the charge value by 100.                       |
| period      | This is the default. If the received charge contains decimals, the charge is displayed at the calling endpoint's display with a period as the decimal point. Divides the charge value by 100. |
| none        | No decimal point is displayed.  |

**Related topics:**

[Charge Advice](#) on page 723

[Direction](#) on page 724

[Trunk Direction](#) on page 825

**Digital Loss Group**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 19     | Determines which administered two-party row in the loss plan applies to this trunk group if the call is carried over a digital signaling port in the trunk group. If values other than 18 or between 11 and 15 are administered, a warning message displays stating that the loss group may not be appropriate for this trunk group. |

**Disconnect Supervision-In**

Indicates whether Communication Manager receives disconnect supervision for incoming calls over this trunk group.

Available only for incoming or two-way trunk groups.

| Valid Entry | Usage   |
|-------------|---|
| y           | Allows trunk-to-trunk transfers involving trunks in this group. The far-end server or switch sends a release signal when the calling party releases an incoming call, and the far-end server or switch is responsible for releasing the trunk. Enhances Network Call Redirection. |

| Valid Entry | Usage   |
|-------------|---|
| n           | The far-end server or switch does not provide a release signal, the hardware cannot recognize a release signal, or timers are preferred for disconnect supervision on incoming calls. Prevents trunk-to-trunk transfers involving trunks in this group. |

 **Caution:**

In general, U.S. local telephone company central offices provide disconnect supervision for incoming calls but not for outgoing calls. Public networks in most other countries do not provide disconnect supervision for incoming or outgoing calls. Check with the network services provider.

**Related topics:**

[Direction](#) on page 724

[Trunk Direction](#) on page 825

**DS1 Echo Cancellation**

Enables or disables echo cancellation on a per port basis. If enabled, reduces voice call echo.

 **Note:**

Changes to the DS1 Echo Cancellation field do not take effect until one of the following occurs:

- Port is busied-out or released.
- Trunk group is busied-out or released.
- SAT command test trunk group is performed.
- Periodic maintenance runs.

**Outgoing Dial Type**

Sets the method used to transmit digits for an outgoing call. Usually, this method should match what the local telephone company central office provides.

DIOD trunks support pulsed and continuous E&M signaling in Brazil and discontinuous E&M signaling in Hungary.

Available for Access, APLT, CO, DIOD, DMI-BOS, FX, RLT, and WATS trunk groups. Also available for Tie trunk groups when the **Trunk Signaling Type** is blank, cont, or dis.

| Valid Entry | Usage  |
|-------------|--|
| tone        | Uses Dual Tone Multifrequency (DTMF) addressing, also known as “touchtone” in the U.S. Allows the trunk group to support both DTMF and rotary signals. For pulsed and continuous E&M signaling in Brazil and for discontinuous E&M signaling in Hungary, use tone or mf. |
| rotary      | Allows only the dial pulse addressing method used by non-touch tone telephones. For example, this value is appropriate for an internal full  |

| Valid Entry | Usage  |
|-------------|--|
|             | touch tone system and for a connection to a local telephone company central office that only supports rotary dialing.  |
| r1mf        | For CAMA trunk groups. It is the only outgoing dial type allowed on CAMA trunk groups. Allows Russian MF Packet Signaling on outgoing trunks. Russian MF Packet Signaling carries calling party number and dialed number information.<br>Available only for co trunk groups.   |
| mf          | Used if a <b>Trunk Signaling Type</b> is not administered. For pulsed and continuous E&M signaling in Brazil and for discontinuous E&M signaling in Hungary, use tone or mf.<br>Available only if Multifrequency Signaling is enabled for the system. Not available if this trunk is used for DCS.                     |
| automatic   | For tie trunks if the <b>Trunk Signaling Type</b> is not administered. This provides “cut-through” operation to outgoing callers who dial a trunk access code, connecting them directly to local telephone company central office dial tone and bypassing any toll restrictions administered on Communication Manager. |

**Related topics:**

[Group Type](#) on page 725

[Multifrequency Signaling](#) on page 948

[Trunk Signaling Type](#) on page 990

**Prefix-1**

If enabled, the prefix “1” is added to the beginning of the digit string for outgoing calls. Use this field for outgoing and two-way trunk groups handling long distance service. Do not enable for trunk groups in AAR or ARS route patterns.

Available only for CO, FX, and DIOD trunk groups.

**Receive Answer Supervision**

If enabled, the network provides answer supervision. For Outbound Call Management applications, use for trunks supporting network answer supervision. For trunks that do not receive a real answer, this field determines when the CallVisor Adjunct-Switch Application Interface (ASAI) connect event is sent.

**Related topics:**

[Administer Timers](#) on page 733

[Answer Supervision Timeout](#) on page 733

**Trunk Direction****! Important:**

This setting must match the provider's settings.

The direction of the traffic on this trunk group.

| Valid Entry | Usage  |
|-------------|--|
| incoming    | Traffic on this trunk group is incoming.   |
| outgoing    | Traffic on this trunk group is outgoing  |
| two-way     | Traffic on this trunk group is incoming and outgoing. Required for <b>Network Call Redirection</b> . |

**Related topics:**

[Charge Conversion](#) on page 739

**Trunk Gain**

Specifies the amplification applied to the trunks in this group. With the values administered for **Trunk Termination** and **Country** code, the value in this field also determines the input and trans-hybrid balance impedance for TN465B, TN2146, TN2147, and TN2184 ports. All other CO and DID circuit packs are set automatically to high.

| Valid Entry | Usage   |
|-------------|---|
| high        | Used if users complain of low volume.         |
| low         | Used if users complain of squeal or feedback. |

**Related topics:**

[Country](#) on page 822

[Trunk Termination](#) on page 827

**Personal CO Line Group: page 1**

**Trunk Type**

Controls the seizure and start-dial signaling used on this trunk group. Entries in this field vary according to the function of the trunk group and must match the corresponding setting on the far-end server or switch.

Available only for CO, DID, FX, and WATS trunk groups.

| Valid Entry  | Usage   |
|--------------|---|
| ground-start | Use ground-start signaling for two-way trunks whenever possible. Ground-start signaling avoids glare and provides answer supervision from the far end.  |
| loop-start   | In general, loop-start signaling is used only for one-way trunks. Loop-start signaling is susceptible to glare and does not provide answer supervision. |

| Valid Entry  | Usage  |
|--|--|
| auto/auto<br>auto/delay<br>auto/immed<br>auto/wink | <p>The term before the slash tells Communication Manager how and when it receives incoming digits. The term after the slash tells Communication Manager how and when it should send outgoing digits.</p> <ul style="list-style-type: none"> <li>• auto — Used for immediate connection to a single preset destination (incoming central office trunks, for example). No digits are sent, because all calls terminate at the same place.</li> <li>• delay — The sending server running Communication Manager does not send digits until it receives a delay dial signal (an off-hook signal followed by an on-hook signal) from the far-end server or switch, indicating that it is ready to receive the digits.</li> <li>• immed — The sending server running Communication Manager sends digits without waiting for a signal from the far-end server or switch.</li> <li>• wink — The sending server running Communication Manager does not send digits until it receives a wink start (momentary off-hook) signal from the far-end server or switch, indicating that it is ready to receive the digits.</li> </ul> |
| 2-wire-ac<br>2-wire-dc<br>3-wire                   | <p>These entries are used with local telephone company central office (CO) trunks in Russia. The specific CO should match one of these values. Available only if the <b>Country</b> code is 15 and the CO trunks use ports on a TN2199 circuit board.</p>  |

**Related topics:**

[Country](#) on page 822

**Trunk Termination**

Adjusts the impedance of the trunk group for optimal transmission quality.

| Valid Entry | Usage   |
|-------------|---|
| 600ohm      | The distance to the local telephone company central office (CO) or to the server at the other end of the trunk is less than 3,000 feet. |
| rc          | The distance to the CO or to the server at the other end of the trunk is more than 3,000 feet.  |

**Personal CO Line Group: page 2****Ext**

The extension of telephones that have a **CO Line** button.

**Name**

The name assigned to telephones that have a **CO Line** button.

## Pickup Group

Implements call pickup groups. A pickup group is a group of users authorized to answer calls to a telephone extension within that group of users. A telephone extension can belong to only one pickup group, and a pickup group can have up to 50 extensions.

Example command: `add pickup-group n`, where *n* is the pickup group number.

### GROUP MEMBER ASSIGNMENTS

#### **Ext**

The extension of the pickup group number. A VDN cannot be assigned to a Call Pickup group.

#### **Name**

The name assigned to the pickup group number extension.

#### **Extended Group Number**

Available only if the **Extended Group Call Pickup** is administered as flexible.

| Valid Entry       | Usage   |
|-------------------|---|
| 1 to 100<br>blank | The Extended Group number. The extended group is a collection of pickup groups that can answer calls from other pickup groups in the same extended group. |

#### **Related topics:**

[Extended Group Call Pickup](#) on page 585

#### **Group Number**

The pickup group number.

## Policy Routing Table

Allows you to distribute calls among a set of call centers based on specified percent allocation. Various types of incoming calls that arrive at a particular VDN can be directed to a Policy Routing Table (PRT) instead of to a vector. The PRT then distributes the calls to the administered Route-to VDNs based on the specified percent allocation targets. Use this screen to implement and monitor percentage allocation routing by assigning destination routes and target percentages.

Example command: `change policy-routing-table n`, where *n* is the policy routing table number.

#### **Actual %**

The actual percent of total calls routed to a VDN. Calculated to six decimal places, but only the first decimal place is displayed.

#### **Call Counts**

The current number of calls routed to a VDN.

**Index**

The sequential number of the row in a Policy Routing Table.

**Name**

The name of the Policy Routing Table (PRT). Accepts a string of up to 15 alphanumeric characters.

**Number**

The number of the Policy Routing Table (PRT).

**Period**

The period for resetting the call counts and actual percentages.

| Valid Entry | Usage   |
|-------------|---|
| 100_count   | Resets the call counts (and displayed %) when total calls for the PRT reach 100. At this point, the total calls match the target routing pattern percentages. This ensures that the routing points have equal distribution of calls all the time. This is the default.      |
| max_count   | Call counts are maintained until calls delivered to at least one of the VDNs exceed 65,400. At this point, calls continue to be distributed over the VDNs but the call counts are reset when the actual percentages equal the targets for all of the VDNs at the same time. |
| Half-hour   | Resets the call counts at the top of the hour and at the 30-minute point.   |
| hour        | Resets the call counts at the top of the hour.  |
| daily       | Resets the call counts at midnight, every night.  |
| weekly      | Resets the call counts at midnight on Saturday.   |

**Route-to VDN**

VDN extension to which calls are to be routed. Accepts up to 15 extensions containing 1 to 13 digits.

**Target %**

| Valid Entry | Usage  |
|-------------|--|
| 0 to 100    | The target percent of total calls to be routed to a VDN. Use whole numbers only, no decimal fractions. |

**Totals**

Displays totals for **Target %** and **Call Counts** for all the assigned VDNs in the PRT. The total for **Target %** is always 100 for form submittal.

**Type**

The type of algorithm the Policy Routing Table (PRT) supports.

**VDN Name**

The name of a VDN, if a name has been assigned previously.

## Precedence Routing Digit Analysis Table

Communication Manager compares dialed numbers with the dialed strings in this table and determines the route pattern of an outgoing Multiple Level Precedence and Preemption (MLPP) call.

Example command: `change precedence-routing analysis n`, where *n* is the precedence-routing digit analysis table number.

### Dialed String

Dialed numbers are matched to the dialed string entry that most closely matches the dialed number. For example, if 297-1234 is dialed and the table has dialed string entries of 297-1 and 297-123, the match is on the 297-123 entry.

An exact match is made on a user-dialed number and dialed string entries with wildcard characters and an equal number of digits. For example, if 424 is dialed, and there is a 424 entry and an X24 entry, the match is on the 424 entry.

Accepts up to 18 digits that the call-processing server analyzes. Also accepts x and X wildcard characters.

### Max

The maximum number of user-dialed digits the system collects to match to the dialed string.

### Min

The minimum number of user-dialed digits the system collects to match to the dialed string.

### Percent Full

| Value    | Comments  |
|----------|---|
| 0 to 100 | The percentage of system memory resources that have been used by the table. |

### Preempt Method

The preemption method used by the server running Communication Manager for this dialed string.

| Valid Entry | Usage   |
|-------------|---|
| group       | The system checks the first trunk group in the route pattern to determine if any trunks are idle. If the system finds an idle trunk, the system connects the call. This is the default. |
| route       | The system checks each trunk group in the route pattern to determine if any trunks are idle. If the system finds an idle trunk, the call is connected.                                  |

## Route Pattern

| Valid Entry | Usage  |
|-------------|--|
| 1 to 999    | The number of the route pattern used by Communication Manager to route calls that match the dialed string. |
| deny        | Blocks the call.   |

## Precedence Routing Digit Conversion Table

Assigns the Precedence Routing digit conversion. Digit conversion takes digits dialed on incoming calls and converts the digits to local telephone numbers, usually extension numbers.

Example command: `change precedence-routing digit-conversion n`, where *n* is the precedence routing digit conversion table number.

### Conv

Allows or prohibits additional digit conversion.

### Del

Number of digits the system deletes from the beginning of the dialed string.

### Matching Pattern

The number that the server running Communication Manager uses to match dialed numbers. Accepts up to 18 digits and the x and X wildcard characters.

### Max

The maximum number of user-dialed digits the system collects to match to the dialed string.

### Min

The minimum number of user-dialed digits the system collects to match to the dialed string.

### Net

| Valid Entry | Usage  |
|-------------|--|
| ext         | Extension. Uses ARS tables or AAR tables to route the call.                |
| pre         | Precedence routing. Uses the Precedence Analysis Tables to route the call. |

## Replacement String

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9, *   | The digits that replace the deleted portion of the dialed number. Accepts up to 18 digits. |
| #           | Indicates end-of-dialing used at the end of the digit string.                              |
| blank       | Deletes the digits without replacement.  |

## Route Pattern

| Valid Entry | Usage  |
|-------------|--|
| 1 to 999    | The number of the route pattern used by Communication Manager to route calls that match the dialed string. |
| deny        | Blocks the call.   |

## PRI Endpoint

Administers PRI Endpoints for the Wideband Switching feature.



**Note:**

A PRI Endpoint with a width greater than 1 can be administered only if Wideband Switching has been enabled for the system.

A PRI Endpoint is an endpoint application connected to line-side ISDN-PRI facilities and has standard ISDN-PRI signaling interfaces to the system.

A PRI Endpoint is defined as 1 to 31 adjacent DS0s/B-channels, addressable via a single extension, and signaled via a D-channel (Signaling Group) over a standard T1 or E1 ISDN-PRI interface.

Example command: `add pri-endpoint n`, where *n* is the extension number.

**Related topics:**

[Wideband Switching](#) on page 950

## COR

| Valid Entry | Usage   |
|-------------|---|
| 0 to 995    | The class of restriction (COR) used to determine calling and called party privileges. |

## COS

| Valid Entry | Usage  |
|-------------|--|
| 0 to 15     | The Class of Service (COS) used to determine the features that can be activated by, or on behalf of, the endpoint. |

## Extension

The extension number used to access the PRI endpoint.

## Maintenance Tests

If enabled, runs hourly maintenance tests on this PRI Endpoint.

## Name

The name of the endpoint. Accepts up to 27 alphanumeric characters.

**Originating Auto Restoration**

If enabled, automatically restores calls originating from this PRI Endpoint (while maintaining endpoint call status) in the case of network failure if the call is over SDDN network facilities.

**Signaling Group**

| Valid Entry       | Usage  |
|-------------------|--|
| 1 to 416<br>blank | The D-channel or D-channel pair that provides the signaling information for the set of B-channels that make up the PRI Endpoint. |

**Simultaneous Calls**

If enabled, specifies that multiple simultaneous calls can be placed to/from the PRI Endpoint.

**(Starting) Port**

The seven-character starting port of the PRI Endpoint.

| Valid Entry                              | Usage   |
|--|---|
| 1 to 64                                  | First and second characters are the cabinet number. |
| A to E                                   | Third character is the carrier.                     |
| 0 to 20                                  | Fourth and fifth character are the slot number.     |
| 01 to 04 (Analog TIE trunks)<br>01 to 31 | Six and seventh characters are the circuit number.  |

**TN**

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

**Width**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 31     | The number of adjacent DS0 ports beginning with the administered Starting Port, that make up the PRI Endpoint. This field cannot be blank. A width of 6 defines a PRI Endpoint that can support data rates up to 384 Kbps. |

**Related topics:**

[\(Starting\) Port](#) on page 833

**WIDEBAND SUPPORT OPTIONS*****Contiguous***

Available only if “N by DS-zero” (NXDS0) multi-rate service is enabled.

| Valid Entry | Usage   |
|-------------|---|
| y           | Specifies the “floating” scheme. NXDS0 calls are placed on a contiguous group of B-channels large enough to satisfy the requested bandwidth without constraint on the starting channel (no fixed starting point trunk). Not available with H0 ISDN information transfer rate. |
| n           | Specifies the “flexible” scheme. NXDS0 calls are placed on any set of B-channels on the same facility as long as the requested bandwidth is satisfied. There are no constraints, such as contiguity of B-channels or fixed starting points                                    |

**Related topics:**

[NxDS0](#) on page 758

[NXDS0](#) on page 834

**H0**

If enabled, specifies the ISDN information transfer rate for 384 Kbps of data, which is comprised of six B-channels. When a PRI Endpoint is administered to support H0, the hunt algorithm to satisfy a call requiring 384 Kbps of bandwidth uses a fixed allocation scheme.

**H11**

If enabled, specifies the ISDN information transfer rate for 1536 Kbps of data, which is comprised of 24 B-channels. When a PRI Endpoint is administered to support H11, the hunt algorithm to satisfy a call requiring 1536 Kbps of bandwidth uses a fixed allocation scheme.

**H12**

If enabled, specifies the ISDN information transfer rate for 1920 Kbps data, which includes 30 B-channels. When a PE is administered to support H12, the hunt algorithm to satisfy a call requiring 1920 Kbps of bandwidth uses a fixed allocation scheme.

**NXDS0**

If enabled, specifies the NXDS0 multi-rate service.

**Processor Channel Assignment**

Assigns each local processor channel to an interface link channel, and defines the information associated with each processor channel on an Ethernet link.

 **Note:**

You cannot remove a service from this screen if that service has overrides defined on the Survivable Processor screen.

Example command: `change communication-interface processor-channels`

**Appl**

Specifies the server application type or adjunct connection used on this channel.

| Valid Entry | Usage   |
|-------------|---|
| audix       | Voice Messaging.  |
| ccr         | Contact Center Reporting, now known as Avaya IQ.  |
| dcs         | Distributed Communication System.   |
| fp-mwi      | ISDN Feature Plus Message Waiting Indication. This channel passes message waiting light information for subscribers on the messaging system, from a messaging adjunct on a main switch for a phone on a satellite switch. The terminating location (far end) of this channel must be a Communication Manager system compatible with ISDN Feature Plus proprietary protocol. |
| gateway     | Supports an X.25 connected AUDIX connected to an ISDN DCS network.  |
| gateway-tcp | Supports a TCP-connected voice messaging system connected to an ISDN DCS network.   |
| mis         | Management Information System, otherwise known as the Call Management System.   |
| qsig-mwi    | QSIG Message Waiting Indication. Used with a QSIG-based interface to a messaging system, this channel passes message waiting light information for subscribers on the messaging system.   |

### Destination Node

Identifies the server or adjunct at the far end of this link. The destination node can be an adjunct name, server name, far end IP address, or node name for services local to the Avaya server. For ppp connections, match the Destination Node Name administered for the ppp data module.

### Destination Port

| Valid Entry   | Usage                               |
|---------------|-------------------------------------|
| 5000 to 64500 | The number of the destination port. |
| 0             | Any port can be used.               |

### Enable

Enables or disables this processor channel on the main server.

### Gtwy to

A number that identifies the processor channel to which the specified processor channel is serving as a gateway.

### Interface Channel

The channel number or the TCP/IP listen port channel to carry this processor (virtual) channel.

| Valid Entry   | Usage  |
|---------------|--|
| 5000 to 64500 | For ethernet or ppp. For TCP/IP, interface channel numbers are in the range 5000 to 64500. The value 5001 is recommended for CMS, and 5003 is recommended for DCS. |

## Managing inventory

| Valid Entry | Usage                 |
|-------------|-----------------------|
| 0           | Any port can be used. |

## Interface Link

| Valid Entry   | Usage  |
|---------------|--|
| 1 to 254      | The physical link carrying this processor (virtual) channel.                           |
| p (processor) | Communication Manager's Processor Ethernet interface is used for adjunct connectivity. |
| blank         | Not administered.  |

## Mach ID

| Valid Entry  | Usage   |
|--|---|
| 1 to 63 for MWI<br>1 to 63 for DCS<br>1 to 99 for voice messaging<br>blank | The destination server ID defined on the dial plan of the destination server. |

### Related topics:

[Mach ID](#) on page 872

## Mode

| Valid Entry                   | Usage   |
|-------------------------------|---|
| c(lient)<br>s(erver)<br>blank | Indicates whether the IP session is passive (client) or active (server). This field must be blank if the interface link is procr-intf. This field cannot be blank if the type of interface link is ethernet or ppp. |

## Proc Chan

The number assigned to each processor channel.

## Session - Local/Remote

| Valid Entry       | Usage  |
|-------------------|--|
| 1 to 384<br>blank | The Local and Remote Session numbers. For each connection, the Local Session number on the Avaya server must equal the Remote Session number on the remote server and vice versa. It is allowed, and sometimes convenient, to use the same number for the Local and Remote Session numbers for two or more connections. Local and Remote Session numbers must be consistent between endpoints. |

## QSIG to DCS TSC Gateway

This screen determines when and how to convert messages from a QSIG NCA-TSC to an administered AUDIX NCA-TSC. This screen maps the QSIG subscriber number to the appropriate AUDIX signaling group and TSC index.

Available only if **Interworking with DCS** is enabled for the system.

Example command: `change isdn qsig-dcs-tsc-gateway`

### Related topics:

[Interworking with DCS](#) on page 955

### Sig Grp

| Valid Entry | Usage                                |
|-------------|--------------------------------------|
| 1 to 650    | The assigned signaling group number. |

### Subscriber Number

A subscriber number up to 20 characters in length. Accepts \*, x, and X as wildcard characters.

### TSC Index

The TSC Index for each machine ID.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 64     | The assigned signaling group number for the qsig-mwi application type. |

## Reason Code Names

Assigns names to reason codes. Each reason code can have a different name for Aux Work and for Logout. These screens appear when the **Two-Digit Aux Work Reason Codes** is enabled for the system.

### Note:

Logout reason codes can only be in the range of 0 to 9, even if **Two-Digit Aux Work Reason Codes** is active.

Example command: `change reason-code-names`

### Aux Work

The name associated with a reason code when the agent uses the reason code to enter Aux Work mode. Accepts up to 16 alphanumeric characters.

### Default Reason Code

The default reason code names. A separate name can be administered for the Aux Work Reason Code of 0 and for the Logout Reason Code of 0. If an agent changes to Aux Work mode and the Aux Work Reason Code Type is set to none, the agent is put into Aux Work

mode with the default Aux Work reason code, even if a different reason code is administered for the **Aux** button. If an agent logs out when the Logout Reason Code Type is set to none, the agent is logged out with the default Logout reason code.

Accepts up to 16 alphanumeric characters.

### **Interruptible**

Specifies whether or not each reason code is interruptible.



**Note:**

The Default Reason Code, Auto-answer IP Failure Aux Work Reason Code, and Maximum Agent Occupancy Aux Work Reason Code cannot be made interruptible.

### **Logout**

The name associated with a reason code when the agent uses the reason code to log out. Accepts up to 16 alphanumeric characters.

## **Remote Access**

Implements the Remote Access feature. Remote Access permits a caller located outside the system to access the system through the public or private network and then use the features and services of the system.



**Security alert:**

The Remote Access feature, when properly administered, enables the customer to minimize the ability of unauthorized persons to gain access to the network. It is the customer's responsibility to take the appropriate steps to properly implement the features, evaluate and administer the various restriction levels, protect access codes, and distribute them only to individuals who have been advised of the sensitive nature of the access information. Each authorized user should be instructed concerning the proper use and handling of access codes.

In rare instances, unauthorized individuals make connections to the telecommunications network through use of remote access features. In such an event, applicable tariffs require the customer pay all network charges for traffic. Avaya cannot be responsible for such charges, and will not make any allowance or give any credit for charges that result from unauthorized access.

Example command: `change remote-access`

### **Authorization Code Required**

If enabled, requires an authorization code be dialed by Remote Access users to access the system's Remote Access facilities. The use of an authorization code in conjunction with a barrier code increases the security of the Remote Access feature.

### **Barrier Code**

The number users must dial to use Remote Access. Can be used with an authorization code. Accepts a four- to seven-digit number in any combination of digits. Must conform to the

administered **Barrier Code Length**. The none value is required if a **Barrier Code Length** is not administered.

**Related topics:**

[Barrier Code Length](#) on page 839

**Barrier Code Length**

| Valid Entry     | Usage   |
|-----------------|---|
| 4 to 7<br>blank | The length of the barrier code. A barrier code length of 7 provides maximum security. |

**Calls Used**

The number of calls placed using the corresponding barrier code. A usage that exceeds the expected rate indicates improper use.

**COR**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 995    | The number of the class of restriction (COR) associated with the barrier code. To provide maximum security, assign the most restrictive COR that provides only the level of service required. |

**COS**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 15     | The number of the class of service (COS) associated with the barrier code. To provide maximum security, assign the most restrictive COS that provides only the level of service required. |

**Disable Following a Security Violation**

Available only if SVN Authorization Code Violation Notification is enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| y           | Disables the Remote Access feature following detection of a Remote Access security violation. The system administrator can re-enable Remote Access using the <code>enable remote-access</code> command. |
| n           | Enables the Remote Access feature following detection of a Remote Access security violation.  |

**Related topics:**

[SVN Authorization Code Violation Notification Enabled](#) on page 851

**Expiration Date**

The date the barrier code expires. Assign an expiration date based on the expected length of time the barrier code is needed. For example, if the barrier code is expected to be used for a two-week period, assign a date two weeks from the current date. If both an **Expiration Date**

and **No. of Calls** are assigned, the corresponding barrier code expires when the first of these criteria is satisfied.

**No. of Calls**

| Valid Entry        | Usage   |
|--------------------|---|
| 1 to 9999<br>blank | The number of Remote Access calls that can be placed using the associated barrier code. If both an <b>Expiration Date</b> and <b>No. of Calls</b> are assigned, the corresponding barrier code expires when the first of these criteria is satisfied. |

**Related topics:**

[Expiration Date](#) on page 839

**Permanently Disable**

If enabled, permanently blocks remote access to the administration interface. Reactivation of remote access to the interface requires the intervention of Avaya Services.

**Remote Access Dial Tone**

Enables or disables the user hearing dial tone as a prompt for entering the authorization code. Disabling this feature provides maximum security. Available only if Authorization Codes are required for Remote Access.

**Related topics:**

[Authorization Code Required](#) on page 838

**Remote Access Extension**

The extension assigned to handle Remote Access calls. The remote access extension is used as if it was a DID extension. Only one DID extension can be assigned as the remote access extension. Calls to that number are treated the same as calls on the remote access trunk.

When a trunk group is dedicated to Remote Access, the remote access extension number is administered as the trunk group’s incoming destination.

A Vector Directory Number (VDN) extension cannot be used as the remote access extension.

Can be blank if no barrier codes are administered.

**Related topics:**

[Incoming Destination](#) on page 985

**TN**

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

## Remote Call Coverage Table

Provides automatic redirection of certain calls to alternate non-local answering positions in a coverage path.

Non-local numbers can be any ARS or AAR number, any number on the public network, any international number, or a UDP/DCS extension up to 16 digits or blank, which includes any ARS/AAR facility access code, any trunk dial access code (TAC), long distance dialing code, or international dial code.

Example command: `change coverage remote n`, where *n* is the remote coverage number.

### 01-1000

The identifier for the destination coverage point. Accepts up to 16 digits. Two places are used for L, D, ',', and %.

| Valid Entry | Usage   |
|-------------|---|
| *           | DTMF digit asterisk   |
| #           | DTMF digit pound  |
| L           | Uses a coverage point only when in Survivable Remote or Survivable Core Server mode |
| D           | Represents the called extension digits  |
| ,           | Pauses for 1.5 seconds  |
| %           | Remaining digits are for end-to end signaling                                       |
| blank       | Not administered  |

## Remote Office

Supports the Remote Office feature, an arrangement whereby a user can set up a remote office without having an on-premises physical desk-set. An R300 is issued to connect remote DCP and analog telephones, IP telephones, and H.323 trunks to the Communication Manager server using IP.

Example command: `change remote-office n`, where *n* is the assigned remote office number.

### Location

| Valid Entry | Usage  |
|-------------|--|
| 1 to 250    | (Depending on your server configuration, see <i>Avaya Aura™ Communication Manager System Capacities Table</i> , 03-300511.) Assigns the location number to the remote office comprised of the associated time zone and the appropriate numbering plan. See the Location sections in <i>Avaya Aura™</i> |

| Valid Entry | Usage  |
|-------------|--|
|             | <i>Communication Manager Feature Description and Implementation</i> , 555-245-205, for the other ways, and for a list of features that use location. |
| blank       | Obtains the location from the cabinet containing the CLAN or the media gateway that the endpoint registered with. By default, the value is blank.    |

### Network Region

| Valid Entry       | Usage  |
|-------------------|--|
| 1 to 250<br>blank | The network region assigned to all stations supported at this remote office. |

### Node Name

The node name of the remote office.

### Site Data

Any desired site information. Accepts up to 30 alphanumeric characters.

## RHNPA Table

Defines route patterns for specific three-digit codes, usually direct distance dialing (DDD) prefix numbers.

Example command: `change rhnpa n`, where *n* is the prefix number.

### CODES

The 100-block of codes being administered.

### Code-Pattern Choice Assignments

| Valid Entry | Usage   |
|-------------|---|
| 1 to 24     | A pattern choice number associated with each office code. |

### Pattern Choices

| Valid Entry       | Usage  |
|-------------------|--|
| 1 to 999<br>blank | The route pattern number associated with each code. If you use one pattern for most of the codes, assign that pattern to choice 1. |

### RHNPA TABLE

The RHNPA table number.

## Route Pattern

Defines the route patterns used by the server running Communication Manager. Each route pattern contains a list of trunk groups that can be used to route the call. The maximum number of route patterns and trunk groups allowed depends on the configuration and memory available in the system.

This screen is used to:

- Insert or delete digits so AAR or ARS calls route over different trunk groups.
- Convert an AAR number into an international number.
- Insert an area code in an AAR number to convert an on-network number to a public network number.
- Insert the dial access code for an alternative carrier into the digit string when a call directly accesses a local telephone company central office (CO), if the long-distance carrier provided by the CO is not available.

Example command: `change route-pattern n`, where *n* is the route pattern number.

## Band

A number that represents the OUTWATS band number (US only).

Available only if **Services/Features** is administered as outwats-bnd and **ISDN-PRI** or **ISDN-BRI Trunks** are enabled for the system. **Band** is required by Call-by-Call Service Selection.

### Related topics:

[Service/Feature](#) on page 849

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

## BCC Value

Identifies the type of call appropriate for a trunk group. Available only if **ISDN-PRI** or **ISDN-BRI Trunks** are enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| y/n         | If enabled, (0, 1, 2, 3, 4, or W) indicates the BCC value is valid for the routing preference. A trunk group preference can have more than one BCC. |

BCC values:

| BCC Value | Description                |
|-----------|----------------------------|
| 0         | Voice-Grade Data and Voice |
| 1         | 56-kbps Data (Mode 1)      |
| 2         | 64-kbps Data (Mode 2)      |

| BCC Value | Description                      |
|-----------|----------------------------------|
| M         | Multimedia call                  |
| 4         | 64-kbps Data (Mode 0)            |
| W         | 128 to 1984-kbps Data (Wideband) |

**Related topics:**

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

**BCIE (Bearer Capability Information Element)**

Determines how to create the ITC codepoint in the setup message. Applies to ISDN trunks. Available only if the Information Transfer Capability (ITC) is administered as both.

| Valid Entry | Usage        |
|-------------|--------------|
| ept         | endpoint     |
| unr         | unrestricted |

**Related topics:**

[ITC \(Information Transfer Capability\)](#) on page 846

**CA-TSC Request**

CA-TSC is used for ISDN B-channel connections.

| Valid Entry | Usage  |
|-------------|--|
| as-needed   | The <b>CA-TSC</b> is set up only when needed. This causes a slight delay. Avaya recommends this entry for most situations. |
| at-setup    | The <b>CA-TSC</b> is automatically set up for every B-channel call whether or not it is needed.                            |
| none        | No <b>CA-TSC</b> is set up. Permits tandeming of NCA-TSC setup requests.   |

**DCS/QSIG Intw**

Enables or disables DCS/QSIG Voice Mail Interworking. Available only if **Interworking with DCS** is enabled for the system.

**Related topics:**

[Interworking with DCS](#) on page 955

**FRL**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 7      | The Facility Restriction Level (FRL) associated with the group routing preference. 0 is the least restrictive, and 7 is the most restrictive. The calling party's FRL must be greater than or equal to this FRL to access the associated trunk group. |

**Security alert:**

For system security reasons, use the most restrictive FRL possible.

**Grp No**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 2000   | The trunk group number associated with the routing preference. |

**Hop Lmt**

The number of hops for each routing preference. Communication Manager blocks a hop equal to or greater than the number entered.

| Valid Entry | Usage  |
|-------------|--|
| blank       | There is no limit to the number of hops for this preference.           |
| 1 to 9      | Valid for limiting the number of hops if using the tandem hop feature. |
| 1 to 32     | Valid for limiting the number of hops if using the transit feature.    |

**Inserted Digits**

The digits to insert for routing. Communication Manager can send up to 52 digits. This includes up to 36 digits entered here plus up to 18 digits originally dialed. Special symbols count as two digits each.

| Valid Entry | Usage  |
|-------------|--|
| *           | When * is in the route pattern and the outgoing trunk is signaling type "mf", the MFC tone for the "end-of-digits" is sent out to the local telephone company central office (CO) in place of the *.                                   |
| #           | When # is in the route pattern and the outgoing trunk is signaling type "mf", the MFC tone for the "end-of-digits" is sent out to the CO in place of the #.  |
| , (comma)   | Creates a 1.5 second pause between digits being sent. Do not use as the first character in the string unless absolutely necessary. Misuse can result in some calls, such as Abbreviated Dialing or Last Number Dialed, not completing. |
| +           | Wait for dial tone up to the Off Premises Tone Detection Timer and then send digits or intercept tone depending on system-wide feature administration.   |
| %           | Start End-to-End Signaling.  |
| !           | Wait for dial tone without timeout and then send DTMF digits.  |
| &           | Wait for ANI that is used for Russian pulse trunks.  |
| p           | The associated trunk group must be of type sip. The single digit p is used for fully qualified E.164 numbers. The p is translated to a + and is prepended to the digit string.   |

**Related topics:**

[Off-Premises Tone Detect Timeout Interval \(seconds\)](#) on page 577

[Outpulse Without Tone](#) on page 607

**ITC (Information Transfer Capability)**

Identifies the type of data transmission or traffic that this routing preference can carry. The ITC applies only to data calls (BCC 1 through 4).

This field must be both or unre for a **BCC Value** of W.

| Valid Entry     | Usage  |
|-----------------|--|
| both            | Calls from restricted and unrestricted endpoints can access the route pattern. |
| rest(ri)cted)   | Calls from restricted endpoints can access the route pattern.                  |
| unre(stri)cted) | Calls from unrestricted endpoints can access the route pattern.                |

**Related topics:**

[BCC Value](#) on page 843

**IXC**

Identifies the carrier, such as AT&T, used for calls that route using an Inter-Exchange Carrier (IXC), and for Call Detail Recording (CDR).

Available only if **ISDN-PRI** or **ISDN-BRI Trunks** are enabled for the system.

| Valid Entry        | Usage  |
|--------------------|--|
| Valid carrier code | Identifies the carrier for IXC calls.  |
| user               | For presubscribed carrier. Used when an IXC is not specified.  |
| none               | Must be none for non-ISDN trunk groups and for Telcordia Technologies NI-2 Operator Service Access. If it is necessary to send an IXC code for a non-ISDN trunk group, the IXC code can be entered as <b>Inserted Digits</b> . |

**Related topics:**

[Inserted Digits](#) on page 845

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

**LAR**

The routing-preference for Look Ahead Routing.

| Valid Entry | Usage  |
|-------------|--|
| next        | Go to the next routing preference and attempt the call again.                              |
| rehu        | Re-hunt within the current routing preference for another trunk to attempt the call again. |

| Valid Entry | Usage   |
|-------------|---|
| none        | Look Ahead Routing is not enabled for the preference. |

### No. Del. Digits

Modifies the dialed number so an AAR or ARS call routes over different trunk groups that terminate in servers or switches with different dial plans.

| Valid Entry      | Usage  |
|------------------|--|
| 0 to 28<br>blank | <p>The total number of digits the system deletes before it sends the number out on the trunk. Use for calls that route:</p> <ul style="list-style-type: none"> <li>• To or through a remote server.</li> <li>• Over tie trunks to a private network server.</li> <li>• Over local telephone company central office (CO) trunks to the serving CO.</li> </ul> |

### No. Dgts Subaddress

Available only if **ISDN Feature Plus** is enabled for the system.

| Valid Entry     | Usage   |
|-----------------|---|
| 1 to 5<br>blank | <p>The number of dialed digits to send in the calling party subaddress IE. Allows a caller to reach a number where the media server's digit processing deletes the dialed number and inserts the listed directory number (LDN). The LDN then is sent to the destination address and the dialed extension is sent in the calling party subaddress information element (IE). At the receiving end, the call terminates to the user indicated by the subaddress number instead of the attendant.</p> |

#### Related topics:

[ISDN Feature Plus](#) on page 947

### NPA

The three-digit Numbering Plan Area (NPA) or area code for the terminating endpoint of the trunk group. Not required for AAR.

The local telephone company can verify this number. For WATS trunks, the terminating NPA is the same as the home NPA unless the Local Exchange Carrier requires 10 digits for local NPA calls.

Leave blank for AAR calls and for tie trunks.

### Numbering Format

Specifies the format of the routing number used for the trunk group for this routing preference. Applies only to ISDN trunk groups.

| Valid Entry | Numbering Plan Identifier | Type of Numbering |
|-------------|---------------------------|-------------------|
| blank       | E.164(1)                  | 1-MAX             |

| Valid Entry   | Numbering Plan Identifier       | Type of Numbering   |
|---|---------------------------------|---------------------|
| natl-pub  | E.164(1)                        | national(2)         |
| intl-pub  | E.164(1)                        | international(1)    |
| locl-pub  | E.164(1)                        | local/subscriber(4) |
| pub-unk   | E.164(1)                        | unknown(0)          |
| lev0-pvt  | Private Numbering Plan - PNP(9) | local(4)            |
| lev0-pvt (enter to allow Network Call Redirection/ Transfer |                                 |                     |
| lev1-pvt  | Private Numbering Plan - PNP(9) | Regional Level 1(2) |
| lev2-pvt  | Private Numbering Plan - PNP(9) | Regional Level 2(1) |
| unk-unk   | unknown(0)                      | unknown(0)          |



**Note:**

To access Telcordia Technologies NI-2 Operator Service Access, **Inserted Digits** must be unk-unk.

**Pattern Name**

An alphanumeric name for the route pattern.

**Pattern Number**

The route pattern number.

**Prefix Mark**

Sets the requirements for sending a prefix digit 1, indicating a long-distance call. Prefix Marks apply to 7- or 10-digit Direct Distance Dialing (DDD) public network calls. A prefix digit 1 is sent only when call type is foreign number plan area (FNPA) or home numbering plan area (HNPA) in the ARS Digit Analysis table.

Not required for AAR. ARS requires a number from 0 to 4 or blank.

For a WATS trunk, the **Prefix Mark** is the same as the local telephone company central office (CO) trunk.

| Valid Entry | Usage  |
|-------------|--|
| 0           | <ul style="list-style-type: none"> <li>• Suppresses a user-dialed prefix digit 1 for 10-digit FNPA calls.</li> <li>• Leaves a user-dialed prefix digit 1 for 7-digit HNPA calls.</li> <li>• Leaves a prefix digit 1 on 10-digit calls that are not FNPA or HNPA calls.</li> </ul> <p>Should not be used in those areas where all long-distance calls must be dialed as 1+10 digits. Check with the local network provider.</p> |

| Valid Entry | Usage  |
|-------------|--|
| 1           | Sends a 1 on 10-digit calls, but not on 7-digit calls.<br>Used for HNPA calls that require a 1 to indicate long-distance calls.  |
| 2           | Sends a 1 on all 10-digit and 7-digit long-distance calls.<br>Refers to a Toll Table to define long-distance codes.  |
| 3           | Sends a 1 on all long-distance calls and keep or insert the NPA (area code) so that all long-distance calls are 10-digit calls. The NPA is inserted when a user dials a prefix digit 1 plus 7 digits.<br>Refers to a Toll Table to define long-distance codes. |
| 4           | Always suppress a user-dialed prefix digit 1.<br>Used, for example, when ISDN calls route to a server that rejects calls with a prefix digit 1.  |
| blank       | For tie trunks.  |

### SCCAN

If enabled, indicates that the route pattern supports incoming SCCAN calls. Available only if Enhanced EC500 is enabled for the system.

#### Related topics:

[Enhanced EC500](#) on page 945

### Secure SIP

If enabled, specifies using the SIP or SIPS prefix when the call is routed to a SIP Enablement Services (SES) trunk preference. If SES trunks are not specified, the call is routed over whatever trunk is specified.

### Service/Feature

An identifier of the Service/Feature carried by the information element (IE) in a call in this route preference. Required by Call-by-Call Service Selection, and Network Call Redirection Transfer. Accepts up to 15 characters.

#### Note:

User-defined service types for network facilities can also be used. Any user-defined **Facility Type** of 0 (feature), 1 (service), or 3 (outgoing) is allowed.

Available only if **ISDN-PRI** or **ISDN-BRI Trunks** are enabled for the system.

| Valid Entry |                                    |  |
|-------------|------------------------------------|--|
| accunet     | multiquest                         | sdn (allows Network Call Redirection/Transfer) |
| i800        | operator                           | sub-operator                                   |
| lds         | oper-meg<br>(operator and megacon) | sub-op-meg<br>(sub-operator and megacom)       |
| mega800     | oper-sdn<br>(operator and sdn)     | sub-op-sdn<br>(sub-operator and sdn)           |

| Valid Entry |             |              |
|-------------|-------------|--------------|
| megacom     | outwats-bnd | wats-max-bnd |

**Related topics:**

- [Facility Type](#) on page 812
- [ISDN-BRI Trunks](#) on page 947
- [ISDN-PR!](#) on page 947

**Toll List**

| Valid Entry      | Usage  |
|------------------|--|
| 1 to 32<br>blank | The number of the ARS Toll Table associated with the terminating NPA of the trunk group. Required for <b>Prefix Mark 2</b> or 3. Not required for AAR. |

**Related topics:**

- [Prefix Mark](#) on page 848

**TSC**

If enabled, allows Call-Associated TSCs and incoming Non-Call-Associated TSC requests to be tandemed out for each routing preference. Also allows feature transparency on DCS+ calls and QSIG Call Completion.

**Security related system parameters**

Determines when Avaya Communication Manager reports a security violation. Many of the fields on this screen repeat for each type of security violation. They are explained once here, but the usage is the same for all.

Example command: `change system-parameters security`

**Security related system parameters: page 1**  
**SECURITY VIOLATION NOTIFICATION PARAMETERS**

**Announcement Extension**

The announcement extension where the Security Violation Notification (SVN) announcement resides. The server running Communication Manager calls the referral destination, then plays this announcement upon answer.

**Originating Extension**

The extension that initiates the referral call in the event of a security violation. It also sends the appropriate alerting message or display to the referral destination. If notification for more than one type of security violation is established, a different extension must be assigned to each one. When Communication Manager generates a referral call, this extension and the type of violation appear on the display at the referral destination.

**Referral Destination**

The extension that receives the referral call when a security violation occurs. The referral destination telephone must have a display, unless it is an Announcement Extension. The

extension can be the telephone, attendant console, or vector directory number (VDN) that receives the referral call for each type of violation. This can be the same extension for all type of violations.

The **Announcement Extension** field is used for a VDN. Call Vectoring Time-of-Day routing is used to route the referral call to different destinations based on the time of day or the day of the week.

**Related topics:**

[Announcement Extension](#) on page 850

**SVN Authorization Code Violation Notification Enabled**

Enables or disables Authorization Code Violation Security Notification. Use with **SVN Remote Access Violation Notification Enabled** to establish parameters for remote access security violations. A remote access violation occurs if a user enters incorrect barrier codes. The system cannot disable remote access following a security violation unless this field has been enabled.

**Related topics:**

[SVN Remote Access Violation Notification Enabled](#) on page 851

**SVN Login (Violation Notification, Remote Access, Authorization Code) Enabled**

Enables or disables login violation notification. If enabled, Communication Manager sends a notification when a login violation occurs.

**SVN Remote Access Violation Notification Enabled**

Enables or disables Remote Access Violation Notification. Use with **SVN Authorization Code Violation Notification Enabled** to establish parameters for remote access security violations. A remote access violation occurs if a user enters incorrect barrier codes. The system cannot disable remote access following a security violation unless this field is enabled.

**Related topics:**

[SVN Authorization Code Violation Notification Enabled](#) on page 851

**Time Interval**

| Valid Entry  | Usage   |
|--------------|---|
| 0:01 to 7:59 | This time range, in conjunction with <b>Login Threshold</b> , determines if a security violation has occurred.<br>The range for the time interval is one minute to eight hours, entered in the screen x:xx. For example, one minute is entered as 0:01 and seven and one-half hours is entered as 7:30. |

**Security related system parameters: page 2**

**ACCESS SECURITY GATEWAY PARAMETERS**

These fields are available only if **Access Security Gateway (ASG)** is enabled for the system.

**Related topics:**

[Access Security Gateway \(ASG\)](#) on page 942

Managing inventory

EPN

Indicates whether or not any entry attempt through a port that is a direct connection to the Expansion Port Network receives a challenge response.

INADS

Indicates whether or not any entry attempt through a port that is a direct connection to the Initialization and Administration System (INADS) receives a challenge response. INADS is used to remotely initialize and administer Communication Manager

MGR1

Indicates whether or not any entry attempt through a port that is a direct connection to the system administration and maintenance access interface located on the processor circuit pack receives a challenge response.

NET

Indicates whether or not any entry attempt through a port that is a dialed-in or dialed-out connection to the Network Controller circuit pack receives a challenge response.

Translation-ID Number Mismatch Interval (days)

| Valid Entry | Usage  |
|-------------|--|
| 1 to 90     | The number of days the system allows access to system administration commands. When this interval expires, only init logins have the ability to execute system administration commands to modify translation data. |

### **REMOTE MANAGED SERVICES**

Port Board Security Notification

Enables or disables port board denial of service notification. Available only if **RMS Feature Enabled** is enabled.

#### **Related topics:**

[RMS Feature Enabled](#) on page 853

Port Board Security Notification Interval

| Valid Entry                    | Usage   |
|--------------------------------|---|
| 60 to 3600 in increments of 10 | <p>The interval in seconds between port board Denial of Service notifications (traps). Default is 60.</p> <p> <b>Note:</b><br/>There is no delay before the first trap is sent. The interval administered in this field applies only to the period between the sending of the traps. Available only if Remote Managed Services and Port Board Security Notification are enabled.</p> |

#### **Related topics:**

[REMOTE MANAGED SERVICES](#) on page 852

[Port Board Security Notification](#) on page 852

**RMS Feature Enabled**

Enables or disables Remote Managed Services.

**SECURITY VIOLATION NOTIFICATION PARAMETERS****SVN Station Security Code Violation Notification Enabled**

Enables or disables station security code parameters. Station Security codes are used to validate logins to a particular extension.

**STATION SECURITY CODE VERIFICATION PARAMETERS****Minimum Station Security Code Length**

| Valid Entry | Usage   |
|-------------|---|
| 3 to 8      | The minimum required length of the station security codes. Longer codes are more secure. If station security codes are used for external access to telecommuting features, the minimum length should be seven or eight. |

**Receive Unencrypted from IP Endpoints**

Allows or blocks unencrypted data from IP endpoints.

**Security Code for Terminal Self Administration Required**

Specifies whether or not a Personal Station Access code is required to enter the Self-Administration mode.

**Related topics:**

[Personal Station Access \(PSA\)](#) on page 948

**Service Hours Table**

Specifies office service hours using up to 99 different tables. Available only if basic vectoring is enabled.

Example command: `change service-hours-table n`, where *n* is the service hours table number.

**Description**

A name that provides a description of the table. Accepts up to 27 characters. The default is blank.

**Example**

Call-ahead Reservations

**Number**

The table number.

**Start/End**

The range of office hours for each day of the week.

A time is considered to be in the table from the first second of the start time (for example, 08:00:00) until the last second of the end time (for example, 17:00:59).

| Valid Entry | Usage   |
|-------------|---|
| 0 to 23     | Hour range. The hour range must be within the specified day, from 00:00 (midnight) until 23:59. |
| 0 to 59     | Minute range.   |

### Use Time Adjustments from Location

The location number that specifies how time zone offset and daylight savings rule adjustments are performed.

**Related topics:**

[Loc Number](#) on page 771

## Signaling group

Establishes signaling group parameters for ISDN-PRI, H.323, ATM, and SIP Enablement Services (SES) trunks. Because these trunk types vary in the types of parameters needed, the fields that appear on this screen change depending on the **Group Type**.

Example command: `add signaling-group n`, where *n* is the signaling group number.

### Signaling group: page 1

#### *Alternate Route Timer*

Available only if **Group Type** is sip.

| Valid Entry | Usage   |
|-------------|---|
| 2 to 30     | The time in seconds Communication Manager waits before trying for an alternate route to establish a call. The default value is 6 seconds. |

**Related topics:**

[Group Type](#) on page 860

#### *Associated Signaling*

Available only if **Group Type** field is isdn-pri.

| Valid Entry | Usage                                      |
|-------------|--|
| y           | Enables associated signaling.              |
| n           | Enables non-facility associated signaling. |

**Related topics:**

[Group Type](#) on page 860

**Bypass If IP Threshold Exceeded**

Available only if **Group Type** is h.323 or sip.

| Valid Entry | Usage  |
|-------------|--|
| y           | Automatically remove from service the trunks assigned to this signaling group when IP transport performance falls below administered system-wide limits. |
| n           | Signaling group trunks stay in service when IP transport performance falls below limits.   |

**Related topics:**

[IP options system parameters: page 1](#) on page 701

[Group Type](#) on page 860

**Calls Share IP Signaling Connection**

Available only if **Group Type** is h.323 or sip.

| Valid Entry | Usage  |
|-------------|--|
| y           | <p>Enables inter-connection between servers running Avaya Communication Manager. Not available if a RAS-Location Request (LRQ) is enabled.</p> <p> <b>Note:</b><br/>When the near and far-end servers are running Avaya Communication Manager, this value must match the value administered for enabling the Layer 3 test.</p> |
| n           | Disables inter-connection between servers running Avaya Communication Manager. Used if the local or remote server is <i>not</i> running Avaya Communication Manager.   |

**Related topics:**

[Enable Layer 3 Test](#) on page 858

[Group Type](#) on page 860

[LRQ Required](#) on page 863

**Circuit Type**

Available only if **Group Type** is atm.

| Valid Entry | Usage   |
|-------------|---|
| T1          | U.S., Canadian, and Japanese digital transmission format. |
| E1          | European digital transmission format.                     |

**Related topics:**

[Group Type](#) on page 860

**Connect**

To control communications at layers 2 and 3 of the ISDN-PRI protocol, this field specifies what is on the far end of the link.

Available only if **Group Type** is atm.

| Valid Entry | Usage   |
|-------------|---|
| host        | The link connects Communication Manager to a computer.  |
| network     | The link connects Communication Manager to a local telephone company central office or any other public network switch. |
| pbx         | The link is connected to another switch in a private network.   |

**Related topics:**

[Group Type](#) on page 860

**Country Protocol**

The country protocol used by the local telephone company central office where the link terminates. This value must match the country protocol used by the far-end server. For connections to a public network, the network service provider can tell you which country protocol they are using.

Available only if **Group Type** is atm.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 25     | The country code.   |
| etsi        | The network service provider uses the protocol of the European Telecommunications Standards Institute (ETSI). Used only if the <b>Signaling Mode</b> is isdn-pri. |

**Related topics:**

[Group Type](#) on page 860

[Signaling Mode](#) on page 868

[Country options table](#) on page 935

**D Channel**

Available only if the **Group Type** is atm.

| Valid Entry                              | Usage  |
|--|--|
| 1 to 64                                  | First and second characters are the cabinet number |
| A to E                                   | Third character is the carrier                     |
| 0 to 20                                  | Fourth and fifth character are the slot number     |
| 01 to 04 (Analog TIE trunks)<br>09 to 32 | Six and seventh characters are the circuit number  |

**Related topics:**

[Group Type](#) on page 860

**DCP/Analog Bearer Capability**

Sets the information transfer capability in a bearer capability IE of a setup message to speech or 3.1kHz. Available only if **Group Type** is atm or h.323.

| Valid Entry | Usage   |
|-------------|---|
| 3.1kHz      | Provides 3.1kHz audio encoding in the information transfer capability. This is the default. |
| speech      | Provides speech encoding in the information transfer capability.                            |

**Related topics:**

[Group Type](#) on page 860

**Direct IP-IP Audio Connections**

Allows or disallows direct audio connections between H.323 endpoints. Direct audio connections save bandwidth resources and improve sound quality of voice over IP (VoIP) transmissions. For SIP Enablement Services (SES) trunk groups, allows direct audio connections between SES endpoints. Available only if **Group Type** is h.323 or sip.

**Related topics:**

[Group Type](#) on page 860

**DTMF Over IP**

Specifies the touchtone signals that are used for dual-tone multifrequency (DTMF) telephone signaling. Available only if **Group Type** is sip.

| Valid Entry  | Usage   |
|--------------|---|
| in-band      | All G711 and G729 calls pass DTMF in-band. DTMF digits encoded within existing RTP media stream for G.711/G.729 calls. G.723 is sent out-of-band.   |
| in-band-g711 | Only G711 calls pass DTMF in-band.  |
| out-of-band  | All IP calls pass DTMF out-of-band. For IP trunks, the digits are done with either Keypad IEs or H245 indications. This value is not supported for SIP signaling. This is the default for newly added H.323 signaling groups. |
| rtp-payload  | This is the method specified by RFC1533. This is the default for newly added SIP signaling groups. Support for SIP Enablement Services (SES) trunks requires the default entry of rtp-payload.                                |

**Related topics:**

[Group Type](#) on page 860

### Enable Layer 3 Test

Enables or disables a Layer 3 test. Communication Manager runs the Layer 3 test to verify that all connections known at the near-end are recognized at the far-end. Available only if **Group Type** is h.323.

 **Note:**

The Layer 3 test should be enabled for an H.323 signaling group type when the **Calls Share IP Signaling Connection** is enabled and the far-end is Communication Manager. Requires administration of a **Far-end Node Name**.

**Related topics:**

[Calls Share IP Signaling Connection](#) on page 855

[Far-end Node Name](#) on page 860

[Group Type](#) on page 860

### Enforce SIPS URI for SRTP

Appears when the **Group Type** field is sip. Use this field to enable or disable Communication Manager to enforce SIPS URI for any incoming SIP message with security descriptions (used for SRTP negotiation) in SDP.

| Valid Entry | Usage   |
|-------------|---|
| y           | Enable Communication Manager to enforce SIPS URI for any incoming SIP message with security descriptions (used for SRTP negotiation) in SDP. Note: The system displays y as the default value for the <b>Enforce SIPS URI for SRTP</b> field. |
| n           | Disable Communication Manager from enforcing SIPS URI for any incoming SIP message with security descriptions (used for SRTP negotiation) in SDP.   |

### ETSI CCBS Support

Available only if **Group Type** is isdn-pri and **TSC Supplementary Service Protocol** is set to c for ETSI.

| Valid Entry     | Usage  |
|-----------------|--|
| none            | Interface supports neither incoming nor outgoing ETSI CCBS. This is the default.   |
| incoming        | Interface supports only incoming ETSI CCBS.  |
| outgoing        | Interface supports only outgoing ETSI CCBS.  |
| both directions | Interface supports incoming and outgoing ETSI CCBS.<br><br> <b>Note:</b><br>When upgrading from a version of Communication Manager that is earlier than 5.1, this is the default. |

**Related topics:**

[Group Type](#) on page 860

[TSC Supplementary Service Protocol](#) on page 869

**Far-end Domain**

The name of the network region that is assigned to the far-end of the trunk group. For example, to route SES calls within an enterprise, the domain assigned to the proxy server is used. For external SES calling, the domain name could be that of the SES service provider. Available only if **Group Type** is sip.

| Valid Entry             | Usage  |
|-------------------------|--|
| <i>Character string</i> | A maximum of 40 characters used to define the name of the IP domain for which the far-end proxy is responsible, if different than the near-end domain. |
| blank                   | <b>Far-end domain</b> is unspecified and the far-end IP address is used. Use if the domains are the same.  |

**Related topics:**

[Group Type](#) on page 860

**Far-end Listen Port**

Available only if **Group Type** is h.323 or sip.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 65535  | Must match the number administered for <b>Near-end Listen Port</b> . Typically, this is the default of 5061 for SIP over TLS. |
| blank       | Far-end listen port is unspecified.   |

**Related topics:**

[Group Type](#) on page 860

[Near-end Listen Port](#) on page 865

**Far-end Network Region**

Available only if **Group Type** is h.323 or sip.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 250    | The number of the network region that is assigned to the far-end of the trunk group. The region is used to obtain the codec set used for negotiation of trunk bearer capability. |
| blank       | Selects the region of the near-end node and the far-end network region is unspecified.   |

**Related topics:**

[Group Type](#) on page 860

**Far-end Node Name**

The node name for the far-end Control LAN (C-LAN) IP interface used for trunks assigned to this signaling group. The node name must be previously administered.

Available only if **Group Type** is atm or sip.

**Related topics:**

[Node Name](#) on page 684

[Group Type](#) on page 860

**Group Number**

The signaling group number.

**Group Type**

The type of protocol used with the signaling group.

| Valid Entry | Usage   |
|-------------|---|
| atm         | Asynchronous Transfer Mode signaling trunks               |
| h.323       | h.323 protocols or SBS signaling trunks                   |
| isdn-pri    | Integrated Service Digital Network Primary Rate Interface |
| sip         | For SIP Enablement Services (SES)                         |

**H.235 Annex H Required**

Enables or disables the requirement that the Communication Manager server uses the H. 235 Annex H (now called H.235.5) protocol for authentication during registration. Available only if **Group Type** is h.323. Requires that RAS-Location Request (LRQ) is enabled.

**Related topics:**

[Group Type](#) on page 860

[LRQ Required](#) on page 863

**H.245 DTMF Signal Tone Duration (msec)**

Available only if **DTMF over IP** is set to out-of-band .

| Valid Entry        | Usage  |
|--------------------|--|
| 80 to 350<br>blank | Specifies the duration of DTMF tones sent in H.245-signal messages.<br>The default is blank. |

**Related topics:**

[DTMF Over IP](#) on page 857

[Group Type](#) on page 860

**H.323 Station Outgoing Direct Media**

Available only if **Group Type** is h.323 and **Direct IP-IP Audio Conections** is enabled.

| Valid Entry | Usage  |
|-------------|--|
| y           | <p>A call from an H.323 station over a trunk that uses this signaling group starts as a direct media call. The IP address and port of the H.323 station are sent as the media and media control channel addresses in the SETUP/INVITE message.</p> <p> <b>Note:</b><br/>On an outgoing Direct Media call from an IP (H.323) telephone over this trunk, if an attempt is made to transfer the call, conference another party, or put the call on hold while the call is still in ringing state, the operation fails.</p> |
| n           | The IP address of the MEDPRO board is sent in the SETUP/INVITE message. This is the default.   |

**Related topics:**

[Direct IP-IP Audio Connections](#) on page 857

[Group Type](#) on page 860

**Idle Code**

An eight-digit string that is compatible with the protocol used by the far-end switch or server. Sets the signal sent out over idle DS0 channels.

Available only if **Group Type** is atm.

**Related topics:**

[Group Type](#) on page 860

**IMS Enabled**

Enables or disables accepting SIP requests that match the domain in the **Far-End Domain**. Outgoing SIP messages use a trunk group with signaling set to IMS. Available only if **Group Type** is sip.

**Related topics:**

[Far-end Domain](#) on page 859

[Group Type](#) on page 860

**Incoming Dialog Loopbacks**

Appears on the Signaling Group screen when the **Group Type** field is sip.

| Valid entries | Usage   |
|---------------|---|
| allow         | Communication Manager software connects the call and allows the SIP trunks to remain in the looparound connection. Avaya recommends that if the trunk group controlled by this SIP signaling group is used for IGAR calls, the value be set to allow. |
| eliminate     | Communication Manager software connects the call and eliminates the SIP trunks from the looparound connection. The default value is eliminate.  |

**Related topics:**

[IGAR Over IP Trunks](#) on page 589

**Initial IP-IP Direct Media**

Communication Manager initially plays the media directly between the endpoints.

**Interface**

Controls how your server negotiates glare with the far-end switch. Available only for a far-end PBX connection.

| Valid entry  | Usage   |
|--|---|
| U.S. private network applications  |   |
| network  | The server overrides the other end when glare occurs. For servers connected to a host computer.                               |
| user   | The server releases the contested circuit and looks for another when glare occurs. For servers connected to a public network. |
| Private networks, including QSIG networks, applications outside the U.S. |   |
| peer-master  | The switch overrides the other end when glare occurs.   |
| peer-slave   | The switch releases the contested circuit and looks for another when glare occurs.  |

**Related topics:**

[Connect](#) on page 856

**Interface Companding**

The companding algorithm expected by the system at the far end.

| Valid Entry | Usage   |
|-------------|---|
| a-law       | Algorithm expected at the far-end for E1 service. |
| mu-law      | Algorithm expected at the far-end for T1 service. |

**Interworking Message**

Determines what message Communication Manager sends when an incoming ISDN trunk call is routed over a non-ISDN trunk group.

| Valid Entry | Usage  |
|-------------|--|
| PROGress    | Requests the public network to cut through the B-channel and let the caller hear tones such as ringback or busy tone provided over the non-ISDN trunk. Normally-selected value.  |
| ALERTing    | Causes the public network in many countries to play ringback tone to the caller. This value is used only if the DS1 is connected to the public network, and it is determined that callers hear silence (rather than ringback or busy tone) when a call incoming over the DS1 interworks to a non-ISDN trunk. |

**IP Audio Hairpinning**

Enables or disables hairpinning for H.323 or SIP Enablement Services (SES) trunk groups. H.323 and SES-enabled endpoints are connected through the IP circuit pack without going through the time division multiplexing (TDM) bus. Available only if **Group Type** is h.323 or sip.

**Related topics:**

[Group Type](#) on page 860

**IP Video**

Enables or disables IP video capability for this signaling group. Available only if the signaling group type h.323 and sip.

**Link Loss Delay Timer (sec)**

Specifies how long to hold the call state information in the event of an IP network failure or disruption. Communication Manager preserves calls and starts this timer at the onset of network disruption (signaling socket failure). If the signaling channel recovers before the timer expires, all call state information is preserved and the signaling channel is recovered. If the signaling channel does not recover before the timer expires, the system:

- Raises an alarm against the signaling channel
- Maintains all connections with the signaling channel
- Discards all call state information about the signaling channel

| Valid Entry | Usage   |
|-------------|---|
| 1 to 180    | The number of seconds to delay the reaction of the call controller to a link bounce. Default is 90. |

**Location for Routing Incoming Calls**

Appears only when the **Group Type** field on the Signaling Group screen is h.323 and **Multiple Locations** field on the Optional Feature screen is y.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 50     |   |
| blank       | The location of CLAN's cabinet or the location of the Processor Ethernet (PE) is taken for routing the call, depending on whether CLAN or PE is being used to carry that H.323 signaling channel. By default, the value is blank. |

**LRQ Required**

Enables or disables RAS-Location Request (LRQ) messages. Available only if **Group Type** is h.323.

| Valid Entry | Usage   |
|-------------|---|
| y           | Allows IP trunk availability to be determined on a per call basis. An LRQ message is sent to the far-end gatekeeper prior to each call over the IP trunk. The far-end gatekeeper responds with a RAS-Location Confirm |

| Valid Entry | Usage  |
|-------------|--|
|             | (LCF) message, and the call proceeds. Required if <b>H.235 Annex H Required</b> is enabled. <b>Calls Share IP Signaling Connection</b> must be disabled. |
| n           | For far-end servers running Communication Manager, unless <b>H.235 Annex H Required</b> is enabled.  |

**Related topics:**

[Calls Share IP Signaling Connection](#) on page 855

[Group Type](#) on page 860

[H.235 Annex H Required](#) on page 860

**Max number of CA TSC**

Available only if **Group Type** is atm, h.323, or isdn-pri.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 619    | The maximum number of simultaneous call-associated Temporary Signaling Connections that can exist in the signaling group. Typically this is the number of ISDN-PRI trunk group members controlled by this signaling group. |

**Related topics:**

[Group Type](#) on page 860

**Max number of NCA TSC**

Available only if **Group Type** is atm, h.323, or isdn-pri.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 256    | The maximum number of simultaneous non-call-associated Temporary Signaling Connections. The TSCs carry signaling for features not associated with a specific call, for example, signals to turn on Leave Word Calling. |

**Related topics:**

[Group Type](#) on page 860

**Media Encryption**

Enables or disables encryption for trunk calls assigned to this signaling group. If encryption for the signaling group is not enabled, then trunk calls using this signaling group do not get encrypted regardless of IP Codec Set administration. Available only if Media Encryption is enabled in Communication Manager and the **Group Type** is h.323.

**Related topics:**

[Group Type](#) on page 860

**Name**

A name that identifies the signaling group. Accepts up to 15 alphanumeric characters.

 **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Related topics:**

[Group Type](#) on page 860

**Near-end Listen Port**

Available only if **Group Type** is h.323 or sip.

| Valid Entry  | Usage   |
|--------------|---|
| 5000 to 9999 | An unused port number for the near-end listen port. The default for SIP Enablement Services (SES) over TLS is 5061. |
| 1719         | For LRQ-enabled ports   |
| 1720         | For h.323-enabled ports   |

**Related topics:**

[Group Type](#) on page 860

[H.323 Station Outgoing Direct Media](#) on page 860

[LRQ Required](#) on page 863

**Near-end Node Name**

The node name for the Control LAN (C-LAN) IP interface in the Avaya S8XXX Server. The node name must be previously administered.

Available only if **Group Type** is atm or sip.

**Related topics:**

[Node Name](#) on page 684

[Name](#) on page 700

[Group Type](#) on page 860

**Network Call Transfer**

Enables or disables Network Call Transfer so that D-channels support Explicit Network Call Transfer (ENCT). Available only if **Group Type** is atm.

**Related topics:**

[Group Type](#) on page 860

**Passphrase**

The passphrase used to generate a shared “secret” for symmetric encryption of the media session key. The same passphrase must be assigned to the corresponding signaling groups at both ends of an IP trunk. The passphrase:

## Managing inventory

- Consists of 8 to 30 alphanumeric characters
- Is case sensitive
- Must contain at least one alphabetic and at least one numeric
- Valid characters also include letters, numbers, and these symbols: !&\*?;'^(),.-

The passphrase is used for both Media Encryption and authentication. This field cannot be left blank.

Available only if Media Encryption is enabled or the **H.235 Annex H Required** is enabled.

### Related topics:

[H.235 Annex H Required](#) on page 860

### Primary D Channel

Available only if **Group Type** is isdn-pri.

| Valid Entry                              | Usage  |
|--|--|
| 1 to 64                                  | First and second characters are the cabinet number |
| A to E                                   | Third character is the carrier                     |
| 0 to 20                                  | Fourth and fifth character are the slot number     |
| 01 to 04 (Analog TIE trunks)<br>09 to 32 | Six and seventh characters are the circuit number  |

### Related topics:

[Group Type](#) on page 860

### Priority Video

Enables or disables the priority video function that specifies that incoming video calls have an increased likelihood of receiving bandwidth, and are also allocated a larger maximum bandwidth per call.

Available only if:

- **Group Type** is h.323 or sip
- Multimedia SIP trunking is enabled for the system

### Related topics:

[Group Type](#) on page 860

[Multimedia IP SIP Trunking](#) on page 948

### Protocol Version

Available only if **Group Type** is atm.

| Valid Entry      | Usage  |
|------------------|--|
| a<br>b<br>c<br>d | In countries whose public networks allow multiple layer-3 signaling protocols for ISDN-PRI service. Selects the protocol that matches the network service provider's protocol. |

**Related topics:**

[Group Type](#) on page 860

**Q-SIP**

Appears only when the **Group Type** field is h.323 or sip.

| Valid Entry | Usage  |
|-------------|--|
| y           | Enables the QSIG over SIP (Q-SIP) feature for the signaling group. |
| n           | The QSIG over SIP feature is disabled. By default, the value is n. |

**QSIG Signaling Group**

Appears only when the **Group Type** field is sip and the **Q-SIP** field is set to y.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 999    | Assigns a number for the QSIG signaling group.                       |
| blank       | No QSIG signaling group is assigned. By default, the value is blank. |

**Remote Office**

Enables or disables administering this signaling group for a remote office. Available only if **Group Type** is h.323.

**Related topics:**

[Group Type](#) on page 860

**RFC 3389 Comfort Noise**

Appears on the Signaling Group screen when the **Group Type** field is sip.

| Valid entries | Usage   |
|---------------|---|
| y             | This enables SIP signaling for comfort noise. If <b>RFC 3389 Comfort Noise</b> field is set to y, this field overrides the <b>Silence Suppression</b> field on the IP Codec Set screen. |
| n             | This disables SIP signaling for comfort noise. Default is n.  |

**RRQ Required**

Enables or disables the requirement that a vendor registration be sent. Available only if **Group Type** is h.323.

**Related topics:**

[Group Type](#) on page 860

**SBS**

Enables or disables the Separation of Bearer and Signaling (SBS) trunk groups. If this field is enabled, both the **Trunk Group for NCA TSC** and the **Trunk Group for Channel Selection** must be set to the signaling group number administered for the SBS trunk group. Available only if **Group Type** is set to h.323.

**Related topics:**

- [Group Type](#) on page 860
- [Trunk Group for Channel Selection](#) on page 869
- [Trunk Group for NCA TSC](#) on page 869

**Session Establishment Timer (min)**

Available only if **Group Type** is sip.

| Valid Entry | Usage  |
|-------------|--|
| 3 to 120    | The time in minutes Communication Manager waits before tearing down a ring no answer call. The default is 3 minutes. |

**Related topics:**

- [Group Type](#) on page 860

**Signaling Mode**

Displays the isdn-pri signaling mode. Available only if **Group Type** is atm.

**Related topics:**

- [Group Type](#) on page 860

**SIP Signaling Group**

Appears only when the **Group Type** field is h.323 and the **Q-SIP** field is set to y.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 999    | Assigns a number for the SIP signaling group.                       |
| blank       | No SIP signaling group is assigned. By default, the value is blank. |

**T303 Timer (sec)**

Available only if **Group Type** is h.323.

| Valid Entry | Usage   |
|-------------|---|
| 2 to 10     | The number of seconds the system waits for a response from the far end before invoking Look Ahead Routing. Default is 10. |

**Related topics:**

- [Group Type](#) on page 860

**Transport Method**

Available only if **Group Type** is sip.

| Valid Entry | Usage  |
|-------------|--|
| tcp         | Transport is accomplished using Transmission Control Protocol (TCP).                 |
| tls         | Transport is accomplished using Transport Layer Security (TLS). This is the default. |

**Related topics:**

[Group Type](#) on page 860

**Trunk Group for Channel Selection**

Available only if **Group Type** is atm, h.323, or isdn-pri.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 2000   | Trunk group number used for channel selection. |

**Related topics:**

[Group Type](#) on page 860

**Trunk Group for NCA TSC**

Available only if **Group Type** is atm, h.323, or isdn-pri.

| Valid Entry        | Usage  |
|--------------------|--|
| 1 to 2000<br>blank | Trunk group number used for non-call-associated Temporary Signaling Connections. |

**Related topics:**

[Group Type](#) on page 860

**TSC Supplementary Service Protocol**

The supplementary service protocol used for temporary signaling connections.

Available only if **Group Type** is atm, h.323, or isdn-pri.

| Valid Entry | Usage  |
|-------------|--|
| a           | AT&T, Telcordia Technologies, Nortel.  |
| b           | ISO QSIG. Also, for SBS signaling groups.  |
| c           | ETSI. Available only if <b>Group Type</b> is isdn-pri.   |
| d           | ECMA QSIG  |
| e           | Allows DCS with rerouting. <b>DCS with Rerouting</b> must be enabled, and <b>Used for DCS</b> must be enabled for the trunk group. |
| f           | Feature Plus   |
| g           | ANSI. Available only if <b>ISDN-PRI</b> , or <b>ISDN-BRI</b> , or <b>Used for DCS</b> are enabled for the system.                  |

**Related topics:**

- [Group Type](#) on page 860
- [DCS with Rerouting](#) on page 945
- [ISDN-BRI Trunks](#) on page 947
- [ISDN-PRI](#) on page 947
- [Used for DCS](#) on page 1023

**Virtual Channel Identifier**

Available only if **Group Type** is atm.

| Valid Entry         | Usage  |
|---------------------|--|
| 32 to 1023<br>blank | The number used as a Virtual Channel Identifier. |

**Related topics:**

- [Group Type](#) on page 860

**Virtual Path Identifier**

Available only if **Group Type** is atm.

| Valid Entry         | Usage   |
|---------------------|---|
| 32 to 1023<br>blank | The number used as a Virtual Path Identifier. |

**Related topics:**

- [Group Type](#) on page 860

**X-Mobility/Wireless Type**

The type of X-Mobile endpoints allowed. Available only if **Group Type** is isdn-pri.

| Valid Entry | Usage   |
|-------------|---|
| DECT        | The remote end of the trunk group controlled by the signaling group is a DECT mobility controller. This allows X-Mobility to work over ISDN-PRI trunks between the server/switch and adjunct. |
| none        | Not administered.   |

**Related topics:**

- [Group Type](#) on page 860

**Signaling group: page 2**

This screen must be filled in for ATM signaling groups. It provides two functions:

- Defines fractional T1 and fractional E1 facilities, specifying how many and which channels to use.
- Specifies the port numbers to use. Port numbers must be unique for all signaling boards on the same ATM board.

Available only if **Group Type** is atm.

### **LIMIT SIGNALING GROUP USAGE**

Controls where H.323 trunks are used. Available only if **Group Type** is h.323 and the **Near-end Name** is procr.

#### **Related topics:**

[Group Type](#) on page 860

[Near-end Node Name](#) on page 865

Enable on Survivable Processors (ESS and LSP)

| Valid Entry | Usage  |
|-------------|--|
| all         | Enables both Survivable Core Server (Enterprise Survivable Server) and Survivable Remote Server (Local Survivable Processor) survivable processors.                      |
| ess-all     | Enables H.323 trunks on Survivable Core processors but not Survivable Remote processors.   |
| none        | Blocks H.323 trunks on survivable processors.  |
| selected    | Specifies which survivable processors are allowed to use H.323 trunks. Additional fields are made available in order to specify the node names of survivable processors. |

Enable on the Main Processor(s)?

Enables or disables the use of H.323 trunks on only the main server.

Selected Survivable Processor Node Names

The node names of the survivable processors that can use H.323 trunks. Available only if survivable processors are enabled for selection.

#### **Related topics:**

[Enable on Survivable Processors \(ESS and LSP\)](#) on page 871

### **SIGNALING GROUP**

Chan Port

| Valid Entry         | Usage   |
|---------------------|---|
| 009 to 256<br>blank | The port number for non-signaling channels.<br>The signaling channel (port 16 for an E1 and port 24 for a T1) must be a port between 9 and 32. A port number used here cannot be used on any other ATM signaling group on the same board.<br>The channels used must match exactly the channels used on the other end of the signaling group. For example, if your T1 is set up to use channels 1 through 5, 7, and 24 (the signaling channel), the far end must also use channels 1 through 5, 7, and 24. |

**Signaling group: NCA-TSC Assignment page**

**Appl.**

Specifies the application for this administered NCA-TSC.

| Valid Entry | Usage  |
|-------------|--|
| audix       | The ISDN-PRI D-channel DCS Audix feature   |
| dcs         | The DCS Over ISDN-PRI D-channel feature.   |
| gateway     | The administered NCA-TSC is used as one end in the gateway channel.  |
| masi        | The NCA-TSC is one end of a multimedia application server interface.   |
| qsig-mwi    | Message conversion from an administered AUDIX NCA-TSC to a QSIG CISC. A Machine ID between 1 and 20 is required. |

**As-needed Inactivity Time-out (min)**

| Valid Entry       | Usage                               |
|-------------------|-------------------------------------|
| 10 to 90<br>blank | Applies only to as-needed NCA-TSCs. |

**Dest. Digits**

An ISDN interface extension number. Accepts up to 15 characters including \* and #.

**Enabled**

Enables or disables the administered NCA-TSC.

**Established**

The strategy for establishing this administered NCA-TSC.

| Valid Entry | Usage  |
|-------------|--|
| permanent   | The administered NCA-TSC can be established by either the near end or the far end.   |
| as-needed   | The administered NCA-TSC is established the first time the administered NCA-TSC is needed. The NCA-TSC can be set up either by the near end or far end switch. |

**Local Ext**

The local extension of the ISDN interface.

**Mach ID**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 20     | A unique machine ID. The system does not allow you to specify an ID that you already administered for the Processor Channel. |

**Related topics:**

[Mach ID](#) on page 836

**Service/Feature**

| Valid Entry  | Usage  |
|--|--|
| accunet<br>i800<br>inwats<br>lds<br>mega800<br>megacom<br>multiquest<br>operator<br>sdn<br>sub-operator<br>wats-max-band | The assigned service or feature. In addition to pre-defined services or features, any user-defined Facility Type of 0 (feature) or 1 (service) is allowed. |

**Signaling group: NCA-TSC Assignment page****Appl.**

Specifies the application for this administered NCA-TSC.

| Valid Entry | Usage  |
|-------------|--|
| audix       | The ISDN-PRI D-channel DCS Audix feature   |
| dcs         | The DCS Over ISDN-PRI D-channel feature.   |
| gateway     | The administered NCA-TSC is used as one end in the gateway channel.  |
| masi        | The NCA-TSC is one end of a multimedia application server interface.   |
| qsig-mwi    | Message conversion from an administered AUDIX NCA-TSC to a QSIG CISC. A Machine ID between 1 and 20 is required. |

**As-needed Inactivity Time-out (min)**

| Valid Entry       | Usage                               |
|-------------------|-------------------------------------|
| 10 to 90<br>blank | Applies only to as-needed NCA-TSCs. |

**Dest. Digits**

An ISDN interface extension number. Accepts up to 15 characters including \* and #.

**Enabled**

Enables or disables the administered NCA-TSC.

**Established**

The strategy for establishing this administered NCA-TSC.

| Valid Entry | Usage  |
|-------------|--|
| permanent   | The administered NCA-TSC can be established by either the near end or the far end.   |
| as-needed   | The administered NCA-TSC is established the first time the administered NCA-TSC is needed. The NCA-TSC can be set up either by the near end or far end switch. |

**Local Ext**

The local extension of the ISDN interface.

**Mach ID**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 20     | A unique machine ID. The system does not allow you to specify an ID that you already administered for the Processor Channel. |

**Related topics:**

[Mach ID](#) on page 836

**Service/Feature**

| Valid Entry  | Usage  |
|--|--|
| accunet<br>i800<br>inwats<br>lds<br>mega800<br>megacom<br>multiquest<br>operator<br>sdn<br>sub-operator<br>wats-max-band | The assigned service or feature. In addition to pre-defined services or features, any user-defined Facility Type of 0 (feature) or 1 (service) is allowed. |

**SIT Treatment for Call Classification**

The treatment of Special Information Tones (SITs) used for Outbound Call Management type calls with USA tone characteristics. The port network TN744 Call Classifier circuit pack ports or H.248 Media Gateway internal tone detector resources in classified mode are used to detect SITs. The classifiers are capable of detecting the following SITs:

- SIT Ineffective Other
- SIT Intercept
- SIT No Circuit
- SIT Reorder

- SIT Vacant Code
- SIT Unknown
- AMD (Answering Machine Detected) Treatment

Available only if **ASAI Link Core Capabilities** and **ASAI Link Plus Capabilities** are enabled for the system.

Example command: `change sit-treatment`

#### Related topics:

[ASAI Link Core Capabilities](#) on page 943

[ASAI Link Plus Capabilities](#) on page 943

### AMD Treatment

Specifies the treatment for Answering Machine Detected. An ASAI adjunct can request AMD for a call. If Answering Machine is detected, one of two treatments is specified.

| Valid Entry | Usage  |
|-------------|--|
| answered    | Calls are classified as answered, and are therefore sent to an agent.                              |
| dropped     | Calls are classified as not answered, and are therefore not sent to an agent. This is the default. |

### Pause Duration

Fractions of a second pause duration, as opposed to **Talk Duration** that is for full seconds.

| Valid Entry                                     | Usage   |
|---|---|
| 0.1 to 2.0 seconds in increments of 0.1 seconds | The amount of time Communication Manager looks for a pause before it classifies the call as a live person.<br>The Pause Duration timer should be set longer than the typical silence between words in an answering machine greeting, but shorter than the typical space between words in a live greeting.<br>Defaults to 0.5 seconds. |

### SIT Ineffective Other

The treatment for "Ineffective Other" messages. An example of an Ineffective Other message is "You are not required to dial a 1 when calling this number" .

| Valid Entry | Usage  |
|-------------|--|
| answered    | Calls are classified as answered, and are therefore sent to an agent.                              |
| dropped     | Calls are classified as not answered, and are therefore not sent to an agent. This is the default. |

### SIT Intercept

The treatment for intercept messages that direct callers to another number or extension.

| Valid Entry | Usage  |
|-------------|--|
| answered    | Calls are classified as answered, and are therefore sent to an agent. This is the default. |
| dropped     | Calls are classified as not answered, and are therefore not sent to an agent.              |

**Example**

An example of an intercept message is "XXX-XXXX has been changed to YYY-YYYY, please make a note of it" .

**SIT No Circuit**

The treatment for calls with circuit problems, such as busy.

| Valid Entry | Usage  |
|-------------|--|
| answered    | Calls are classified as answered, and are therefore sent to an agent.                              |
| dropped     | Calls are classified as not answered, and are therefore not sent to an agent. This is the default. |

**SIT Reorder**

The treatment for reorder calls.

| Valid Entry | Usage  |
|-------------|--|
| answered    | Calls are classified as answered, and are therefore sent to an agent.                              |
| dropped     | Calls are classified as not answered, and are therefore not sent to an agent. This is the default. |

**SIT Unknown**

The treatment for calls when a situation or condition that is unknown to the network is encountered.

| Valid Entry | Usage  |
|-------------|--|
| answered    | Calls are classified as answered, and are therefore sent to an agent.                              |
| dropped     | Calls are classified as not answered, and are therefore not sent to an agent. This is the default. |

**SIT Vacant Code**

The treatment for calls when a vacant code is encountered.

| Valid Entry | Usage  |
|-------------|--|
| answered    | Calls are classified as answered, and are therefore sent to an agent.                              |
| dropped     | Calls are classified as not answered, and are therefore not sent to an agent. This is the default. |

## Talk Duration

Full second talk duration, as opposed to **Pause Duration** that is for fractions of a second.

| Valid Entry                                     | Usage  |
|---|--|
| 0.1 to 5.0 seconds in increments of 0.1 seconds | The amount of time Communication Manager looks for voice energy. If it finds that much continuous speech, Communication Manager classifies the call as an answering machine.<br>The Talk Duration timer should be set to a time longer than it takes to say a typical live greeting.<br>Defaults to 2.0 seconds. |

## Site Data

Provides descriptive information about the buildings, floors and telephone set colors. Values must be supplied here before site data can be entered for the station.

Example command: `change site-data`

## Station

Administers individual telephone sets or virtual telephones. All of the fields that can appear on the Station screens are included. Some of the fields are used for specific telephone types; others are used for all telephone types.

Example command: `add station n`, where *n* is the extension number.

## 1-Step Clearing

Enables or disables call termination at the WCBRI terminal when the user drops from the call.

## Abbreviated Dialing List 1, List 2, List 3

Assigns up to three abbreviated dialing lists to each telephone.

| Valid Entry | Usage   |
|-------------|---|
| enhanced    | Allows the telephone user to access the enhanced system abbreviated dialing list.   |
| group       | Allows the telephone user to access the specified group abbreviated dialing list. Requires administration of a group number.                |
| personal    | Allows the telephone user to access and program their personal abbreviated dialing list. Requires administration of a personal list number. |
| system      | Allows the telephone user to access the system abbreviated dialing list.  |

## Access Code

A five-digit access code used to place a wireless terminal into service. The access code is a temporary, shorter version of the complete User Authentication Key (UAK) required by the

system when the terminal is first put into service. It is used to automatically generate a unique UAK for that wireless terminal over-the-air.

Available only if a wireless terminal model number is selected as the station type.

**Related topics:**

[Type](#) on page 909

**Active Station Ringing**

Defines how calls ring to the telephone when it is off-hook without affecting how calls ring at this telephone when the telephone is on-hook.

| Valid Entry    | Usage   |
|----------------|---|
| continuous     | All calls to this telephone ring continuously.  |
| single         | Calls to this telephone receive one ring cycle and then ring silently.  |
| if-busy-single | Calls to this telephone ring continuously when the telephone is off-hook and idle. Calls to this telephone receive one ring cycle and then ring silently when the telephone is off-hook and active. |
| silent         | All calls to this station ring silently.  |

**Adjunct Supervision**

Available only if the station type is 500, 2500, k2500, 8110, ops, ds1fd, ds1sa, VRU, VRUFD, or VRUSA.

| Valid Entry | Usage   |
|-------------|---|
| y           | An analog disconnect signal is sent automatically to the port after a call terminates. Analog devices, such as answering machines and speakerphones, use this signal to turn the devices off after a call terminates.                         |
| n           | Required hunt group agents are alerted to incoming calls. In a hunt group environment, the disconnect signal blocks the reception of zip tone and incoming call notification by an auto-answer station when a call is queued for the station. |

**Related topics:**

[Type](#) on page 909

**Always Use**

Enables or disables the following emergency call handling settings:

- A softphone can register no matter what emergency call handling settings the user has entered into the softphone. If a softphone dials 911, the administered **Emergency Location Extension** is used. The softphone's user-entered settings are ignored.
- If an IP telephone dials 911, the administered **Emergency Location Extension** is used.
- If a call center agent dials 911, the physical station extension is displayed, overriding the administered **LoginID for ISDN Display** .

Does not apply to SCCAN wireless telephones, or to extensions administered as type h.323.

**Related topics:**

[Emergency Location Ext](#) on page 59

**Assigned Member — Ext**

The extension of the user who has an associated **Data Extension** button and shares the module.

**Assigned Member — Name**

The name associated with the extension of the user who has an associated **Data Extension** button and shares the module.

**Att. Call Waiting Indication**

Attendant call waiting allows attendant-originated or attendant-extended calls to a busy single-line telephone to wait and sends distinctive call-waiting tone to the single-line user.

| Valid Entry | Usage  |
|-------------|--|
| y           | Activates Call Waiting for the telephone without Caller ID information. This feature must be enabled when the <b>Type</b> is set to H.323. This is the default.  |
| n           | Call Waiting is not enabled for the station. Disable this feature if: <ul style="list-style-type: none"> <li>• <b>Data Restriction</b> is enabled</li> <li>• <b>Switchhook Flash</b> field is disabled</li> <li>• <b>Data Privacy</b> is enabled for the telephone's class of service (COS)</li> </ul> |
| c           | Enables the Caller ID Delivery with Call Waiting feature, which displays CID information on for the waiting call. Available only if the station <b>Type</b> is CallrID.  |

**Related topics:**

[Data Restriction](#) on page 69

[Data Privacy](#) on page 492

[Switchhook Flash](#) on page 908

[Type](#) on page 909

### Audible Message Waiting

Enables or disables an audible message waiting tone indicating the user has a waiting message consisting of a stutter dial tone when the user goes off-hook.

This field does *not* control the Message Waiting lamp.

Available only if **Audible Message Waiting** is enabled for the system.

#### Related topics:

[Audible Message Waiting](#) on page 944

### AUDIX Name

The voice messaging system associated with the station. Must contain a user-defined adjunct name that was previously administered.

#### Related topics:

[Name](#) on page 700

### Auto-A/D

Enables or disables automatic abbreviated/delayed ringing for a call appearance. Available only if **Per Button Ring Control** is enabled.

#### Related topics:

[Per Button Ring Control](#) on page 72

### Auto Answer

In EAS environments, the auto answer setting for the Agent LoginID can override a station's setting when an agent logs in.

| Valid Entry | Usage  |
|-------------|--|
| all         | All ACD and non-ACD calls terminated to an idle station cut through immediately. Does not allow automatic hands-free answer for intercom calls. With non-ACD calls, the set is also rung while the call is cut through. The ring can be prevented by activating the ringer-off feature button when the <b>Allow Ringer-off with Auto-Answer</b> is enabled for the system.                       |
| acd         | Only ACD split /skill calls and direct agent calls to auto answer. Non-ACD calls terminated to a station ring audibly. For analog stations, the station is off-hook and idle, only the ACD split/skill calls and direct agent calls auto answer; non-ACD calls receive busy treatment. If the station is active on an ACD call and a non-ACD call arrives, the Agent receives call-waiting tone. |
| none        | All calls terminated to this station receive an audible ringing treatment.   |
| icom        | Allows a telephone user to answer an intercom call from the same intercom group without pressing the <b>intercom</b> button.   |

#### Related topics:

[Allow Ringer-off with Auto-Answer](#) on page 619

## Automatic Moves

Allows a DCP telephone to be unplugged from one location and moved to a new location without additional Communication Manager administration. Communication Manager automatically associates the extension to the new port.

### **Caution:**

When a DCP telephone is unplugged and moved to another physical location, the **Emergency Location Extension** must be changed for that extension or the USA Automatic Location Identification data base must be manually updated. If the **Emergency Location Extension** is not changed or if the USA Automatic Location Identification data base is not updated, the DID number sent to the Public Safety Network could send emergency response personnel to the wrong location.

| Valid Entry | Usage   |
|-------------|---|
| always      | The DCP telephone can be moved anytime without additional administration by unplugging from one location and plugging into a new location.  |
| once        | The DCP telephone can be unplugged and plugged into a new location once. After a move, the field is set to done the next time that routine maintenance runs on the DCP telephone.<br>Use when moving a large number of DCP telephones so each extension is removed from the move list. Also use to prevent automatic maintenance replacement. |
| no          | Requires administration to move the DCP telephone.  |
| done        | Communication Manager sets the field to done after the telephone is moved and routine maintenance runs on the DCP telephone.  |
| error       | Communication Manager sets the field to error, after routine maintenance runs on the DCP telephone, when a non-serialized telephone is set as a movable telephone.  |

### Related topics:

[Emergency Location Ext](#) on page 59

## Auto Select Any Idle Appearance

Enables or disables automatic selection of any idle appearance for transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being transferred or conferenced has. If that attempt fails, Communication Manager selects the first idle appearance.

## Automatic Selection of DID Numbers

Enables or disables the Automatic Selection of DID Numbers for Guest Rooms feature. This feature assigns a two- to five-digit extension from a predetermined list of numbers to a hotel room telephone number that is not associated with the room number.

## BCC

Indicates voice or voice-grade data when the value is set to 0. The Bearer Capability Classes (BCC) value is used to determine compatibility when non-ISDN facilities are connected to ISDN

facilities (ISDN Interworking). Available only if **ISDN-PRI** or **ISDN-BRI Trunks** are enabled for the system.

**Bearer**

Used when Secure Terminal Equipment (STE) telephones are administered as 8510 telephones. This field appears for 8503, 8510, and 8520 stations in Communication Manager 2.1 and 2.2 only. **Secure Terminal Equip** is for Bearer functionality in Communication Manager 3.0 and later.

| Valid Entry | Usage  |
|-------------|--|
| speech      | Forces the Bearer Cap IE to “speech” before a call is delivered to the 85xx BRI station.   |
| 3.1khz      | Leaves the Bearer Cap IE unchanged. Use 3.1khz to let secure calls from Secure Terminal Equipment (STE) telephones to work properly. |

**Related topics:**

[Secure Terminal Equip](#) on page 904

**Bridged Appearance Origination Restriction**

Restricts or allows call origination on the bridged appearance.

| Valid Entry | Usage   |
|-------------|---|
| y           | Call origination on the bridged appearance is restricted.   |
| n           | Call origination on the bridged appearance is allowed. This is normal behavior, and is the default. |

**Bridged Call Alerting**

Controls how the user is alerted to incoming calls on a bridged appearance.

| Valid Entry | Usage   |
|-------------|---|
| y           | The bridged appearance rings when a call arrives at the primary telephone.  |
| n           | The bridged appearance flashes but does not ring when a call arrives at the primary telephone. This is the default.<br>If disabled and <b>Per Button Ring Control</b> is also disabled, audible ringing is suppressed for incoming calls on bridged appearances of another telephone’s primary extension. |

**Related topics:**

[Per Button Ring Control](#) on page 72

**Bridged Idle Line Preference**

Specifies whether the selected line for incoming bridged calls is always an idle line.

| Valid Entry | Usage   |
|-------------|---|
| y           | The user connects to an idle call appearance instead of the ringing call. |
| n           | The user connects to the ringing call appearance.                         |

## Building

A valid building location.

### Related topics:

[Site Data](#) on page 877

## Busy Auto Callback without Flash

Enables or disables automatic callback for a calling analog station without flashing the hook. Available for analog telephones only if **Without Flash** is enabled for the system.

### Related topics:

[Without Flash](#) on page 598

## BUTTON ASSIGNMENTS

The feature assigned to each button on the station. Feature buttons are assigned by entering the abbreviated feature. For a list of feature buttons, see Telephone Feature Buttons Table in *Administering Avaya Aura™ Communication Manager*, 03-300509.



### Note:

To use Terminal Translation Initialization (TTI), a call appearance (call-appr) must be assigned to the first button position. TTI needs the button on the first call appearance to get dial tone.

## Cable

Identifies the cable that connects the telephone jack to the system.

## Call Appearance Display Format

Specifies the display format for the station. Bridged call appearances are not affected by this field. Use this field to Available only on telephones that support downloadable call appearance buttons, such as the 2420 and 4620 telephones.



### Note:

This field sets the administered display value only for an individual station.

| Valid Entry       | Usage  |
|-------------------|--|
| loc-param-default | The system uses the administered system-wide default value. This is the default.                                 |
| inter-location    | The system displays the complete extension on downloadable call appearance buttons.                              |
| intra-location    | The system displays a shortened or abbreviated version of the extension on downloadable call appearance buttons. |

**Related topics:**

[Display Parameters](#) on page 536

**Caller ID Message Waiting Indication**

Allows or prevents aliasing of various non-Avaya telephones and adjuncts. Available only if **Type** is CallrID. For CallrID type telephones or analog telephones with Caller ID adjuncts only.

 **Note:**

The Caller ID Message Waiting Indication administration is independent of the administration of LED or NEON-lamp Communication Manager Message Waiting Indication (MWI). For example, it is possible to administer a Caller ID telephone with **Caller ID Message Waiting Indication** is disabled and **Message Waiting Indicator** set to neon.

**Related topics:**

[Message Waiting Indicator](#) on page 896

[Type](#) on page 909

**Calls Allowed**

Identifies the Extension to Cellular call filter type for an XMOBILE station. This field allows an XMOBILE station to function as a bridge and still be restricted. Available only with an EC500-type XMOBILE station and with a **Mapping Mode** of termination or both.

| Valid Entry | Usage  |
|-------------|--|
| internal    | External calls are blocked. Internal calls terminate to the XMOBILE station. Attendant-originated and attendant-delivered calls are not delivered  |
| external    | Internal calls are blocked. External calls terminate to the XMOBILE station.   |
| all         | All calls terminate to the XMOBILE station.  |
| none        | Prevents calls from terminating to the XMOBILE station. Can be used to prevent business-related calls from accruing telephone charges on cellular telephones that are lost, being transferred to a new user, or being disabled for other business reasons. |

 **Note:**

Interswitch calls on DCS trunks are treated as internal calls. When this field is set to:

- internal or all, DCS calls are delivered to the cell telephone
- external or none, DCS calls are not delivered

Incoming calls from other Extension to Cellular users are internal if office caller ID is enabled for the XMOBILE station associated with the cell telephone. When this field is set to:

- internal or all, calls from other Extension to Cellular users are delivered
- external or none, calls from other Extension to Cellular users are not delivered

**Related topics:**

[Mapping Mode](#) on page 895

[XMOBILE Type](#) on page 915

**Call Waiting Indication**

Allows user, attendant-originated, and outside calls to a busy single-line telephone to wait and sends a distinctive call-waiting tone to the single-line user. Not available if **Data Restriction** is enabled, **Switchhook Flash** is disabled, or if Data Privacy is active by way of the telephone COS assignment.

| Valid Entry | Usage  |
|-------------|--|
| y           | Activates Call Waiting without Caller ID information for the telephone. This is the default.   |
| n           | Call Waiting is not enabled for the station.   |
| c           | Enables the Caller ID Delivery with Call Waiting feature, which displays CID information on for the waiting call. This value can only be entered when the station type is CallRID. |

**Related topics:**

[Data Restriction](#) on page 69

[Data Privacy](#) on page 492

[Switchhook Flash](#) on page 908

[Type](#) on page 909

**CDR Privacy**

Enables or disables Call Privacy for each station. Allows digits in the called number field of an outgoing call record to be blanked on a per-station basis. The number of blocked digits is administered system-wide as CDR parameters.

**Related topics:**

[Privacy — Digits to Hide](#) on page 473

**Cell Phone Number**

The unformatted cell telephone's published external number consisting of 1 to 15 digits. This field can contain a three-digit area code plus the seven-digit main number. If the same Cell Phone Number is administered for multiple XMOBILE stations, then the Dial Prefix associated with each instance of the Cell Phone Number must be the same. Avaya recommends that this number consist of a full 10-digit Cell Phone Number regardless of whether the cell telephone is local or not.

**Configuration Set**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 10     | The configuration set number that contains the call treatment options desired for the XMOBILE station. This field must be administered if: |

| Valid Entry | Usage   |
|-------------|---|
|             | <ul style="list-style-type: none"> <li>• The <b>XMOBILE Type</b> is EC500.</li> <li>• The <b>Mobility Trunk Group</b> is a trunk group number and the administered trunk group is non-DECT or non-PHS.</li> <li>• The <b>Mobility Trunk Group</b> is aar or ars.</li> </ul> |
| blank       | If the <b>Mobility Trunk Group</b> is a trunk group number and the administered trunk group is DECT or PHS, this field can be left blank.   |

**Related topics:**

[Configuration Set](#) on page 494

[Mobility Trunk Group](#) on page 897

[XMOBILE Type](#) on page 915

**Conf/Trans On Primary Appearance**

Enables or disables the forced use of a primary appearance when the held call to be conferenced or transferred is a bridge. This is regardless of the administered value for **Auto Select Any Idle Appearance** .

**Related topics:**

[Auto Select Any Idle Appearance](#) on page 68

**COR**

Class of Restriction (COR) number with the desired restriction.

**Cord Length**

The length of the cord attached to the receiver. This is a free-form entry, and can be in any measurement units.

**COS**

The Class of Service (COS) number used to select allowed features.

**Country Protocol**

The protocol that corresponds to the supported initialization and codesets. The Country Protocol must match any previously-administered endpoint on the same port.

**Related topics:**

[Country options table](#) on page 935

**Coverage After Forwarding**

Governs whether an unanswered forwarded call is provided coverage treatment.

| Valid Entry | Usage   |
|-------------|---|
| y           | Coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters. |

| Valid Entry | Usage  |
|-------------|--|
| n           | No coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters. |
| s(system)   | Administered system-wide coverage parameters determine treatment.  |

**Related topics:**

[Coverage After Forwarding](#) on page 932

**Coverage Module**

Indicates whether or not a coverage module is connected to the station.

**Coverage Msg Retrieval**

Allows or denies users in the telephone's Coverage Path to retrieve Leave Word Calling (LWC) messages for this telephone. Applies only if the telephone is enabled for LWC Reception.

**Coverage Path 1 or Coverage Path 2**

The coverage-path number or time-of-day table number assigned to the station.

**Note:**

If Modified Misoperation is active, a Coverage Path must be assigned to all stations on Communication Manager.

**Related topics:**

[Misoperation Alerting](#) on page 607

**CRV Length**

| Valid Entry | Usage  |
|-------------|--|
| 1 or 2      | The length of the Call Reference Value (CRV) for each interface. Only for ASAI stations. |

**Custom Selection of VIP DID Numbers**

Allows or disallows the selection of a DID number assigned to a room when a guest checks in. Available only if **Automatic Selection of DID Numbers** is enabled.

**Related topics:**

[Automatic Selection of DID Numbers](#) on page 640

**Customizable Labels**

Enables or disables the Increase Text for Feature Buttons feature for this station. This feature expands the text labels associated with Abbreviated Dial buttons from the current five uppercase alphanumeric characters to a maximum of 13 upper and lower case alphanumeric characters. Ensures that there will always be sufficient customized button resources to support VIP users. Available only when the station type is one of the following:

- 2410 (Release 2 or later)
- 2420 (Release 4 or later)

- 4610 (IP Telephone Release 2.2 or later)
- 4620 (IP Telephone Release 2.2 or later)
- 4621 (IP Telephone Release 2.2 or later)
- 4622 (IP Telephone Release 2.2 or later)
- 4625 (IP Telephone Release 3.1 or later)

**Related topics:**

[Type](#) on page 909

**Data Extension**

The extension number assigned to the data module. This value must agree with the system dial plan. Accepts a one- to five-digit number.

**Data Module**

Indicates whether or not this telephone has an associated data module.

**Data Option**

| Valid Entry | Usage   |
|-------------|---|
| analog      | A second line on the telephone is administered on the I-2 channel.            |
| data module | A second line on the telephone is <i>not</i> administered on the I-2 channel. |
| none        | The data option is not administered.  |

**Data Restriction**

Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Cannot be assigned if **Auto Answer** is administered as all or acd. If enabled, whisper page to this station is denied.

**Related topics:**

[Auto Answer](#) on page 61

**Default Dialing Abbreviated Dialing Dial Code**

The list number associated with the abbreviated dialing list.

When the user goes off-hook for a data call and presses the **Enter** button following the DIAL prompt, the system dials the AD number.

Available only if the **Special Dialing Option** is set to default.

**Related topics:**

[Special Dialing Option](#) on page 906

**Dial Prefix**

The unformatted sequence of up to four digits or characters that are prepended to the cell telephone's published cell telephone number before dialing. Accepts the \* and # characters.

If the same Cell Phone Number is administered on multiple XMOBILE stations, then the Dial Prefix associated with each instance of the Cell Phone Number must be the same.

### Direct IP-IP Audio Connections

Allows or denies direct audio connections between IP endpoints that saves on bandwidth resources and improves sound quality of voice over IP transmissions.

### Display Caller ID

Enables or disables transmission of calling party information to the Caller ID telephone or adjunct. For CallrID type telephones or analog telephones with Caller ID adjuncts only. Available only if the station type is CallrID.

#### Related topics:

[Type](#) on page 909

### Display Cartridge

Enables or disables displaying the cartridge associated with the station. For 7404 D telephones only.

### Display Client Redirection

Enables or disables the display of redirection information for a call originating from a station with Client Room Class of Service and terminating to this station. When disabled, only the client name and extension or room display. Available only if Hospitality is enabled for the system.

#### Note:

This field must be enabled for stations administered for any type of voice messaging that needs display information.

#### Related topics:

[Hospitality \(Basic\)](#) on page 946

[Hospitality \(G3V3 Enhancements\)](#) on page 946

### Display Language

| Valid Entry   | Usage   |
|---|---|
| english<br>french<br>italian<br>spanish<br>user-defined | The language that displays on stations.<br>Time of day is displayed in 24-hour format (00:00 - 23:59) for all languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.).  |
| unicode   | Displays English messages in a 24-hour format . If no Unicode file is installed, displays messages in English by default.<br><br> <b>Note:</b><br>Unicode display is only available for Unicode-supported telephones. Currently, 4610SW, 4620SW, 4621SW, 4622SW, Sage, Spark, and 9600-series telephones (Avaya one-X Deskphone Edition SIP R2 or later) support Unicode display. Unicode is also an option for DP1020 |

| Valid Entry | Usage  |
|-------------|--|
|             | (aka 2420J) and SP1020 (Toshiba SIP Phone) telephones when enabled for the system. |

### Distinctive Audible Alert

Enables or disables distinctive audible alerts that allow telephones to receive three different types of ringing patterns that identify the type of incoming calls. Distinctive ringing might not work properly for off-premises telephones.

### Emergency Location Ext

The Emergency Location Extension for this station. This extension identifies the street address or nearby location when an emergency call is made. Defaults to the telephone's extension. Accepts up to eight digits.



**Note:**

On the ARS Digit Analysis Table in Communication Manager, 911 must be administered to be call type emer or alrt for the E911 Emergency feature to work properly.

**Related topics:**

[Remote Softphone Emergency Calls](#) on page 63

### EMU Login Allowed

Enables or disables using the station as a visited station by an Enterprise Mobility User (EMU).

### Endpt ID

Available only if Endpt Init is enabled.

| Valid Entry | Usage   |
|-------------|---|
| 00 to 62    | A unique two-digit number for this endpoint. Each Endpt ID field must have a unique value for each endpoint on the same port. |

**Related topics:**

[Endpt Init](#) on page 890

### Endpt Init

Indicates the terminal's endpoint initialization capability. Endpoint initialization is a procedure, required for multipoint operation, by which User Service Order Profile (USOP) is associated with an endpoint on the ISDN-BRI. This association is made through the SPID, administered into the system, and entered into the ISDN-BRI terminal.

Available only if **MIM Support** is enabled.

| Valid Entry | Usage   |
|-------------|---|
| y           | The terminal supports Telcordia Technologies ISDN-1 terminal initialization procedures. |
| n           | For all other country protocols.  |

**Related topics:**

[MIM Support \(Management Information Message Support\)](#) on page 897

**Expansion Module**

Indicates whether or not this telephone has an expansion module. Enables the administration of the buttons for the expansion module.

**Extension**

The extension for this station.

For a virtual extension, a valid physical extension or a blank can be entered. Blank allows an incoming call to the virtual extension to be redirected to the virtual extension “busy” or “all” coverage path.

**Feature Module**

Indicates whether or not the station is connected to a feature module.

**Fixed TEI**

Indicates whether or not the endpoint has a fixed Terminal Endpoint Identifier (TEI). The TEI identifies a unique access point within a service. TEIs must be administered for fixed TEI terminals. Must be enabled for ASAI.

Available only for ISDN-BRI data modules, NI-BRI telephones, WCBRI data modules, and ASAI links.

**Floor**

A valid floor location.

**Forwarded Destination**

A destination extension for both internal and external calls for each of the three types of enhanced call forwarding (Unconditional, Busy, and No Reply). Accepts up to 18 digits. The first digit can be an asterisk \*.

Requires administration to indicate whether the specific destination is active (enabled) or inactive (disabled).

**H.320 Conversion**

Enables or disables the conversion of H.320 compliant calls made to this telephone to voice-only. Because the system can handle only a limited number of conversion calls, the number of telephones with H.320 conversion should be limited.

**Headset**

Indicates whether or not the telephone has a headset.

**Home**

Indicates the roaming status of the wireless user. Available only when a wireless terminal model number is selected as the station type.

| Valid Entry | Usage                                 |
|-------------|---------------------------------------|
| y           | The user's home. This is the default. |

| Valid Entry | Usage               |
|-------------|---------------------|
| n           | The roaming system. |

**Related topics:**

[Type](#) on page 909

**HOT LINE DESTINATION — Abbreviated Dialing Dial Code**

Available only if **Special Dialing Option** is hot-line.

Hot Line Service is used when very fast service is required and when a telephone is used only for accessing a certain facility.

**HOT LINE DESTINATION — Abbreviated Dialing List Number**

The abbreviated dialing list where the hotline destination number is stored.

**HOT LINE DESTINATION — Dial Code**

The dial code in the specified abbreviated dialing list where the hotline destination number is stored.

**Hunt-to Station**

The extension the system should hunt to for this telephone when the telephone is busy. A station hunting chain can be created by assigning a hunt-to station to a series of telephones.

**Idle/Active Ringing (Callmaster)**

Defines how a call rings to the telephone when it is on-hook. Applies to CALLMASTER telephones.

| Valid Entry    | Usage   |
|----------------|---|
| continuous     | All calls to this telephone ring continuously.  |
| if-busy-single | Calls to this telephone ring continuously when the telephone is off-hook and idle, and calls to this telephone receive one ring cycle and then ring silently when the telephone is off-hook and active. |
| silent-if-busy | Calls ring silently when this station is busy.  |
| single         | Calls to this telephone receive one ring cycle and then ring silently.  |

**Idle Appearance Preference**

Indicates which call appearance is selected when the user lifts the handset and there is an incoming call.

| Valid Entry | Usage   |
|-------------|---|
| y           | The user connects to an idle call appearance instead of the ringing call.                       |
| n           | The Alerting Appearance Preference is set and the user connects to the ringing call appearance. |

**Ignore Rotary Digits**

Indicates whether or not rotary digits from the set are ignored. If enabled, the short switch-hook flash (50 to 150) from a 2500-type set is ignored.

**IPEI**

Available when a wireless terminal model number is selected as the station type.

| Valid Entry                         | Usage  |
|-------------------------------------|--|
| 0 to 9<br>a to f<br>A to F<br>blank | The International Portable Equipment Identifier of the wireless terminal. Accepts a unique nine-character hexadecimal ID number. |

**IP Audio Hairpinning**

Indicates whether or not IP endpoints are allowed to connect through the IP circuit pack in the server without going through the time division multiplexing (TDM) bus.

Available only if the group type is h.323 or sip.

**IP Phone Group ID**

Available only for H.323 station types.

| Valid Entry       | Usage                                 |
|-------------------|---------------------------------------|
| 0 to 999<br>blank | The Group ID number for this station. |

**IP Softphone**

Indicates whether or not this extension is either a PC-based multifunction station or part of a telecommuter complex with a call-back audio connection.

Available only for DCP station types and IP Telephones.

**IP Video**

Indicates whether or not this extension has IP video capability. Available only for station type h.323.

**IP Video Softphone**

Indicates whether or not this extension is a video softphone. Available only if **IP Softphone** is enabled.

**ITC (Information Transfer Capability)**

The type of transmission facilities used for ISDN calls originating from this endpoint. Not available for voice-only or BRI stations.

| Valid Entry | Usage   |
|-------------|---|
| restricted  | Either restricted or unrestricted transmission facilities are used to complete the call. A restricted facility is a transmission facility that enforces 1's density digital transmission. In other words, a sequence of |

| Valid Entry  | Usage   |
|--------------|---|
|              | eight digital zeros are converted to a sequence of seven zeros and a digital one.   |
| unrestricted | Only unrestricted transmission facilities are used to complete the call. An unrestricted facility is a transmission facility that does not enforce 1's density digital transmission. In other words, digital information is sent exactly as is. |

**Jack**

Alpha-numeric identification of the jack used for this station.

**Location**

This field appears only when the **Multiple Locations** field is set to y and the **Type** field is set to H.323 or SIP station types.

| Valid entry | Usage  |
|-------------|--|
| 1 to 250    | (Depending on your server configuration, see <i>Avaya Aura™ Communication Manager System Capacities Table</i> , 03-300511.) Assigns the location number to a particular station. Allows IP telephones and softphones connected through a VPN to be associated with the branch an employee is assigned to. This field is one way to associate a location with a station. For the other ways and for a list of features that use location, see the Location sections in <i>Avaya Aura™ Communication Manager Feature Description and Implementation</i> , 555-245-205. |
| blank       | Indicates that the existing location algorithm applies. By default, the value is blank.  |

**Lock Messages**

Controls access to voice messages by other users.

| Valid Entry | Usage   |
|-------------|---|
| y           | Restricts other users from reading or canceling the voice messages, or retrieving messages using Voice Message Retrieval. |
| n           | Allows other users to read, cancel, or retrieve messages.   |

**Loss Group**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 17     | Determines which administered two-party row in the loss plan applies to each station. Does not appear for stations that do not use loss — such as x-mobile stations and MASI terminals. |

**LWC Activation**

Activates or deactivates the Leave Word Calling (LWC) feature. LWC allows internal telephone users on this extension to leave short pre-programmed messages for other internal users.

LWC should be used if:

- The system has hospitality and the guest-room telephones require LWC messages indicating that wakeup calls failed
- LWC messages are stored in a voice-messaging system

### LWC Log External Calls

Determines whether or not unanswered external call logs are available to end users. When external calls are not answered, Communication Manager keeps a record of up to 15 calls provided information on the caller identification is available. Each record consists of the latest call attempt date and time.

### LWC Reception

Indicates where Leave Word Calling (LWC) messages are stored.

| Valid Entry | Usage   |
|-------------|---|
| audix       | LWC messages are stored on the voice messaging system.                          |
| none        | LWC messages are not be stored.   |
| spe         | LWC messages are stored in the system or on the switch processor element (spe). |

### Related topics:

[AUDIX Name](#) on page 662

### Mapping Mode

Controls the mode of operation in which the cell telephone operates when mapped to this XMOBILE extension. An XMOBILE station can be bridged to a deskset. These restrictions or modes exist because the COR of a bridge is ignored; instead the principal's COR is used. This field allows an XMOBILE station to function as a bridge and still be restricted.

When a cell telephone is mapped to more than one XMOBILE station, then only one of the mapped XMOBILE station can have origination or both as its Mapping Mode. Therefore, only one of the XMOBILE stations mapped to the cell telephone number is permitted to originate calls.

| Valid Entry | Usage  |
|-------------|--|
| both        | The cell telephone can be used to originate and terminate calls from its associated XMOBILE extension. This is the default when the XMOBILE type is PHS or DECT.       |
| none        | The XMOBILE station is disabled administratively and cannot originate and terminate calls from its associated internal extension.                                      |
| origination | The cell telephone can be used only to originate calls from its associated internal XMOBILE extension by dialing into the office server running Communication Manager. |

| Valid Entry | Usage  |
|-------------|--|
| termination | The cell telephone can be used only to terminate calls from its associated internal XMOBILE extension. This is the default when the XMOBILE type is EC500. |

**Map-to Station**

The extension of a physical telephone used for calls to a virtual extension. Cannot be used with an xmobile, xdid or any other virtual extension.

**Media Complex Ext**

When used with Multi-media Call Handling, indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to place either a voice or a data call, and voice conversion, coverage, and forwarding apply as if the call were made to the 1-number.

| Valid Entry                | Usage  |
|----------------------------|--|
| A valid BRI data extension | For MMCH, enter the extension of the data module that is part of this multimedia complex.  |
| H.323 station extension    | For 4600 series IP Telephones, enter the corresponding H.323 station. For IP Softphone, enter the corresponding H.323 station. If you enter a value in this field, you can register this station for either a road-warrior or telecommuter/Avaya IP Agent application. |
| blank                      | Leave this field blank for single-connect IP applications.   |

**Message Lamp Ext**

The extension of the station tracked with the message waiting lamp.

**Message Server Name**

Specifies which Message Server is associated with the station. Must contain a user-defined adjunct name that was previously administered. Names must be administered in alphabetical order.

**Message Waiting Indicator**

Specifies the type of message waiting indicator. This field is independent of the administration of the Caller ID Message Waiting Indication for CallrID telephones. Must be set to a value other than none when the station type is set to H.323.

Available only for ISDN-BRI data modules and for 500, 2500, K2500, 7104A, 6210, 6218, 6220, 8110, H.323 and VRU telephones.

| Valid Entries | Usage  |
|---------------|--|
| led           | The message waiting indicator is a light-emitting diode (LED). |
| neon          | The message waiting indicator is a neon indicator.             |

| Valid Entries | Usage  |
|---------------|--|
|               |  <b>Note:</b><br>The neon message waiting indicator is supported only on a small subset of boards, including older US-only boards, such as the TN746 and the TN793. Check the documentation for your board to see if neon is supported. Available only if the <b>Analog Ringing Cadence</b> is set to 1 (US) for the location parameters. |
| none          | No message waiting indicator is selected. This is the default.   |

### Message Waiting Type

| Valid Entry | Usage  |
|-------------|--|
| DISPL       | The MW text is added to the end of the display line during an incoming or outgoing call. |
| ICON        | The MWI message is used to update to the Wireless Terminal.                              |
| NONE        | No MWI message is sent to the Wireless Terminal  |

### MIM Mtce/Mgt

Indicates if the telephone supports MIM Maintenance and Management capabilities other than endpoint initialization. Available only if **MIM Support** is enabled.

#### Related topics:

[MIM Support \(Management Information Message Support\)](#) on page 897

### MIM Support (Management Information Message Support)

Enables or disables MIM endpoint initialization (SPID support) and other Maintenance or Management capabilities. Available only for ISDN-BRI data modules and ASAI. Must be disabled for ASAI.

### Mobility Trunk Group

Associates the XMOBILE station to a trunk.

| Valid Entries | Usage   |
|---------------|---|
| 2000          | A valid trunk group number for mobility routing. This trunk group is used for routing.  |
| aar           | The Automatic Alternate Routing (AAR) capabilities of Communication Manager are used to direct the call to an ISDN trunk. If no ISDN trunk is available, the call is not extended out of the server. It provides ringback to the calling company and might eventually go to coverage. |
| ars           | The Automatic Route Selection (ARS) capabilities of Communication Manager are used to direct the call to an ISDN trunk. If no ISDN trunk is available, the call is not extended out of the server. It provides ringback to the calling company and might eventually go to coverage.   |
| blank         | Not administered.   |

**Model**

The model of the NI-BRI telephone.

| Valid Entry           | Usage  |
|-----------------------|--|
| L-3 Communication STE | The NI-BRI telephone is a model L-3 Communication STE.               |
| Tone Commander        | The NI-BRI telephone is a model 6210 and 6220 Tone Commander.        |
| Other                 | The NI-BRI telephone is another model (for example, a Nortel 5317T). |

**Mounting**

Indicates whether the station mounting is d(esk) or w(all).

**Multimedia Early Answer**

Enables or disables multimedia early answer on a station-by-station basis.

The station should be enabled for this feature if the station receives coverage calls for multimedia complexes, but is not multimedia-capable. This ensures that calls are converted and the talk path is established before ringing at this station.

**Mute Button Enabled**

Enables or disables the mute button on the station.

**MWI Served User Type**

Controls the auditing or interrogation of a served user’s message waiting indicator (MWI).

| Valid Entries | Usage  |
|---------------|--|
| fp-mwi        | The station is a served user of an fp-mwi message center.  |
| qsig-mwi      | The station is a served user of a qsig-mwi message center.   |
| blank         | The served user’s MWI is not audited or if the user is not a served user of either an fp-mwi or qsig-mwi message center. |

**Name**

The name of the person associated with this telephone or data module. The system uses this value to create the system directory.

 **Note:**

This field is supported by Unicode language display for the 4610SW, 4620SW, 4621SW, and 4622SW telephones.

For more information on Unicode language display, see *Administering Unicode*.

 **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

 **Note:**

Consider the display for emergency notification when completing the **Name** field. Put the most important identifying information at the beginning of the field. When an emergency call is made and a crisis alert station with a 27-character display is notified, only 17 characters of the **Name** field appear on the first display line, followed by the extension. The second line contains the last three characters of the **Name** field, followed by the word `EMERGENCY`. Characters 18 through 24 of the **Name** field do not appear at all.

### Off Premises Station

Available only for analog telephones.

| Valid Entries | Usage  |
|---------------|--|
| y             | This telephone is <i>not</i> located in the same building with the system. Requires administration of R Balance Network. |
| n             | The telephone is located in the same building with the system.   |

#### Related topics:

[R Balance Network](#) on page 901

### PCOL/TEG Call Alerting

Enables or disables alerting at the station for Personal CO Line/Terminating Extension Group calls.

Available only for 510 telephones.

### Per Button Ring Control

Enables or disables per button ring control by the station user.

| Valid Entries | Usage   |
|---------------|---|
| y             | Allows users to select ring behavior individually for each call-appr, brdg-appr, or abrdg-appr on the station and to enable Automatic Abbreviated and Delayed ring transition for each call-appr on the station. Prevents the system from automatically moving the line selection to a silently alerting call unless that call was audibly ringing earlier. |
| n             | Calls on <b>call-appr</b> buttons always ring the station and calls on <b>brdg-appr</b> or <b>abrdg-appr</b> buttons always ring or not ring based on the <b>Bridged Call Alerting</b> value. Allows the system to move line selection to a silently alerting call if there is no call audibly ringing the station.   |

#### Related topics:

[Bridged Call Alerting](#) on page 68

### Personalized Ringing Pattern

Defines the personalized ringing pattern for the station. Personalized Ringing allows users of some telephones to have one of 8 ringing patterns for incoming calls. For virtual stations, this field dictates the ringing pattern on its mapped-to physical telephone.

L = 530 Hz, M = 750 Hz, and H = 1060 Hz

| Valid Entries | Usage                  |
|---------------|------------------------|
| 1             | MMM (standard ringing) |
| 2             | HHH                    |
| 3             | LLL                    |
| 4             | LHH                    |
| 5             | HHL                    |
| 6             | HLL                    |
| 7             | HLH                    |
| 8             | LHL                    |

### Per Station CPN - Send Calling Number

Determines Calling Party Number (CPN) information sent on outgoing calls from this station.

| Valid Entries | Usage  |
|---------------|--|
| y             | All outgoing calls from the station deliver the CPN information as "Presentation Allowed."                                     |
| n             | No CPN information is sent for the call.   |
| r             | Outgoing non-DCS network calls from the station delivers the Calling Party Number information as "Presentation Restricted."    |
| blank         | The sending of CPN information for calls is controlled by administration on the outgoing trunk group the calls are carried on. |

### Port

The port assigned to the station.

| Valid Entry | Usage   |
|-------------|---|
| 01 to 64    | First and second numbers are the cabinet number   |
| A to E      | Third character is the carrier  |
| 01 to 20    | Fourth and fifth characters are the slot number   |
| 01 to 32    | Sixth and seventh characters are the circuit number   |
| x or X      | Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) stations, as well as for SBS Extensions. |
| IP          | Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have an IP set. This is automatically entered for certain   |

| Valid Entry | Usage  |
|-------------|--|
|             | IP station set types, but you can enter for a DCP set with softphone permissions. This changes to the s00000 type when the set registers.  |
| xxxVmpp     | Specifies the media gateway. <ul style="list-style-type: none"> <li>• xxx is the gateway number, which is in the range 001 to 250.</li> <li>• m is the module number, which is in the range 1 to 9.</li> <li>• pp is the port number, which is in the range 01 to 32.</li> </ul> |

### Precedence Call Waiting

Activates or deactivates Precedence Call Waiting for this station.

### R Balance Network

| Valid Entry | Usage   |
|-------------|---|
| y           | Selects the R Balance Capacitor network. Use all cases except for those listed under n.   |
| n           | Selects the standard resistor capacitor network. Required if administered for an off-premise station. Use when the station port circuit is connected to terminal equipment, such as SLC carriers or impedance compensators, optioned for 600-ohm input impedance and the distance to the equipment from the system is less than 3,000 feet. |

#### Related topics:

[Off Premises Station](#) on page 899

### Recall Rotary Digit

Enables or disables the Recall Rotary Digit dialing that enables this user to perform conference and transfer operations.

Available only if the station type is 500 or 2500.

#### Related topics:

[Recall Rotary Digit](#) on page 626

[Type](#) on page 909

### Redirect Notification

Enables or disables redirection notification that gives a half ring at this telephone when calls to this extension are redirected through Call Forwarding or Call Coverage. Must be enabled if LWC messages are stored on a voice-messaging system.

#### Related topics:

[LWC Reception](#) on page 65

### Remote Office Phone

Indicates whether or not this station is used as an endpoint in a remote office configuration.

## Remote Softphone Emergency Calls

Tells Communication Manager how to handle emergency calls from the IP telephone.

 **Caution:**

An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. Please be advised that an Avaya IP endpoint cannot dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. Do not use an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations. Please contact your Avaya representative if you have questions about emergency calls from IP telephones.

Available only if the station is an IP Softphone or a remote office station.

| Valid Entry | Usage  |
|-------------|--|
| as-on-local | <p>If the emergency location extension that corresponds to this station's IP address is not administered (left blank), the value as-on-local sends the station emergency location extension to the Public Safety Answering Point (PSAP).</p> <p>If the administrator populates the IP address mapping with emergency numbers, the value as-on-local functions as follows:</p> <ul style="list-style-type: none"> <li>• If the station emergency location extension is the same as the IP address mapping emergency location extension, the value as-on-local sends the extension to the Public Safety Answering Point (PSAP).</li> <li>• If the station emergency location extension is different from the IP address mapping emergency location extension, the value as-on-local sends the IP address mapping extension to the Public Safety Answering Point (PSAP).</li> </ul> |
| block       | <p>Prevents the completion of emergency calls. Use this entry for users who move around but always have a circuit-switched telephone nearby, and for users who are farther away from the server than an adjacent area code served by the same 911 Tandem office. When users attempt to dial an emergency call from an IP Telephone and the call is blocked, they can dial 911 from a nearby circuit-switched telephone instead.</p>  |
| cesid       | <p>Allows Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP. The end user enters the emergency information into the IP Softphone.</p> <p>Use this entry for IP Softphones with road warrior service that are near enough to the server that an emergency call routed over the it's trunk reaches the PSAP that covers the server or switch. If the server uses ISDN trunks for emergency calls, the digit string is the telephone number, provided that the number is a local direct-dial number with the local area code, at the physical location of the IP Softphone. If the server uses CAMA trunks for emergency calls, the end user enters a specific digit</p>   |

| Valid Entry | Usage  |
|-------------|--|
|             | string for each IP Softphone location, based on advice from the local emergency response personnel.  |
| option      | Allows the user to select the option (extension, block, or cesid) that the user selected during registration and the IP Softphone reported. This entry is used for extensions that can be swapped back and forth between IP Softphones and a telephone with a fixed location.<br>The user chooses between block and cesid on the softphone. A DCP or IP telephone in the office automatically selects the extension. |

**Related topics:**

[Emergency Location Ext](#) on page 59

[IP Softphone](#) on page 71

[Emergency Location Extension](#) on page 674

[Remote Office Phone](#) on page 901

**Restrict Last Appearance**

| Valid Entries | Usage   |
|---------------|---|
| y             | Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only. |
| n             | Last idle call appearance is used for incoming priority calls and outgoing call originations.                 |

**Rg**

| Valid Entry   | Usage   |
|---|---|
| a(bbreivated-ring)<br>d(elayed-ring)<br>n(o-ring)<br>r(ing) | The type of automatic abbreviated/delayed ringing for each call appearance when per button ring control is enabled. Default is r. |

**Related topics:**

[Per Button Ring Control](#) on page 72

**Room**

| Valid Entry               | Usage  |
|---------------------------|--|
| <i>Telephone location</i> | Identifies the telephone location. Accepts up to 10 characters.  |
| <i>Guest room number</i>  | Identifies the guest room number if this station is one of several to be assigned a guest room and the <b>Display Room Information in Call Display</b> is enabled for the system. Accepts up to five digits. |

**Related topics:**

[Display Room Information in Call Display](#) on page 642

**SAC/CF Override**

Allows the user of a station with a **Team** button administered, who is monitoring another station, to directly reach the monitored station by pushing the **Team** button. This overrides any currently active rerouting, such as Send All Calls and Call Forwarding, on the monitored station.

| Valid Entries | Usage  |
|---------------|--|
| Ask           | The system asks if the user wants to follow the rerouting or override it. When the user has the option to decide whether rerouting should take place or not, a message is sent to the station that displays the active rerouting and the number of the forwarded to station. |
| No            | Cannot override rerouting. The station does not have the ability to override the rerouting of a monitored station.   |
| Yes           | Can override rerouting. The station has the ability to override the rerouting the monitored station has set, as long as one incoming call appearance is free.  |

**Secure Terminal Equip**

Used when Secure Terminal Equipment (STE) telephones are administered as 8510 telephones. Available only for 8503, 8510, and 8520 stations in Communication Manager 3.0 and later.

| Valid Entries | Usage  |
|---------------|--|
| y             | Leave the Bearer Cap IE unchanged. 3.1khz is used to let secure calls from Secure Terminal Equipment (STE) telephones work properly. |
| n             | Force the Bearer Cap IE to “speech” before a call is delivered to the 85xx BRI station.  |

**Security Code**

The security code required by users for specific system features and functions, including the following: Personal Station Access, Redirection of Calls Coverage Off-Net, Leave Word Calling, Extended Call Forwarding, Station Lock, Message Retrieval, Terminal Self-Administration, and Demand Printing. The required security code length is administered system-wide.

**Related topics:**

[Minimum Station Security Code Length](#) on page 853

**Select Last Used Appearance**

| Valid Entry | Usage  |
|-------------|--|
| y           | Indicates a station’s line selection is not to be moved from the currently selected line button to a different, non-alerting line button. The line selection on an on-hook station only moves from the last used line button |

| Valid Entry | Usage  |
|-------------|--|
|             | to a line button with an audibly alerting call. If there are no alerting calls, the line selection remains on the button last used for a call.       |
| n           | The line selection on an on-hook station with no alerting calls can be moved to a different line button that might be serving a different extension. |

### Service Link Mode

Determines the duration of the service link connection. The service link is the combined hardware and software multimedia connection between an Enhanced mode complex's H.320 DVC system and a server running Avaya Communication Manager that terminates the H.320 protocol. When the user receives or makes a call during a multimedia or IP Softphone or IP Telephone session, a "service link" is established.

| Valid Entry | Usage  |
|-------------|--|
| as-needed   | Used for most multimedia, IP Softphone, or IP Telephone users. Setting the Service Link Mode to as-needed leaves the service link connected for 10 seconds after the user ends a call so that they can immediately place or take another call. After 10 seconds the link is dropped and a new link would have to be established to place or take another call. |
| permanent   | Used for busy call center agents and other users who are constantly placing or receiving multimedia, IP Softphone, or IP Telephone calls. In permanent mode, the service link stays up for the duration of the multimedia, IP Softphone, or IP Telephone application session.  |

### Set Color

Indicates the set color. Valid entries include the following colors: beige, black, blue, brown, burg (burgundy), gray, green, ivory, orng (orange), red, teak, wal (walnut), white, and yel (yellow).

### Short/Prefixed Registration Allowed

If the **IP Stations** or the **IP Softphone** field is set to y, the **Short/Prefixed Registration Allowed** field appears for this H.323 IP set types: 1603, 1608, 1616, 4601, 4601P, 4602, 4602P, 4606, 4610, 4612, 4620, 4622, 4624, 4630, 9610, 9620, 9630, and 9650.

| Valid Entry | Usage   |
|-------------|---|
| y           | Call processing allows the short registration to proceed per station basis. This entry overrides the System Parameters IP Options screen field value for that station.            |
| n           | Call processing rejects the short registration per station basis. This entry overrides the System Parameters IP Options screen field value for that station.                      |
| default     | Call processing uses the <b>Short/Prefixed Registration Allowed</b> field option on the System Parameters IP Options screen for short registration. The default value is default. |

**Related topics:**

[Short/Prefixed Registration Allowed](#) on page 702

**Speaker**

Indicates whether or not the station is equipped with a speaker.

**Speakerphone**

Controls the behavior of speakerphones.

| Valid Entry | Usage   |
|-------------|---|
| 1-way       | Indicates that the speakerphone listen-only.  |
| 2-way       | Indicates that the speakerphone is both talk and listen.  |
| grp-listen  | Group Listen allows a telephone user to talk and listen to another party with the handset or headset while the telephone's two-way speakerphone is in the listen-only mode. Others in the room can listen, but cannot speak to the other party through the speakerphone. The person talking on the handset acts as the spokesperson for the group. Group Listen provides reduced background noise and improves clarity during a conference call when a group needs to discuss what is being communicated to another party.<br>Available only with 6400-series and 2420/2410 telephones. |
| none        | Not administered for a speakerphone.  |

**Special Dialing Option**

Identifies the type of dialing for calls when this data module originates calls.

| Valid Entry | Usage  |
|-------------|--|
| hot-line    | The Hot Line Service destination number is stored in an Abbreviated Dialing List. When the user goes off-hook on a Data Hot Line call, the system dials the AD number. |
| default     | The system dials the default dialing AD number.  |
| blank       | Normal keyboard dialing.   |

**SPID — (Service Profile Identifier)**

The Service Profile Identifier (SPID) for this station. The SPID is a variable length parameter required for ISDN-BRI stations.

The SPID is a numeric string, which means that the value of 00 is different from 000. The SPID must be different for all terminals on the BRI and from the Service SPID. The SPID should always be assigned. If the SPID is not assigned for the first BRI on a port, any other BRI assignment to that port is blocked.

 **Note:**

If you have not administered a port for an ISDN-BRI extension and intend to use Terminal Translation Initialization (TTI) to assign the port, then the SPID number must equal the station number.

Available only if the terminal supports ISDN terminal initialization procedures.

**Related topics:**

[Endpt ID](#) on page 890

**Survivable COR**

Sets a level of restriction for stations to be used with the survivable dial plan to limit certain users to only to certain types of calls. You can list the restriction levels in order from the most restrictive to least restrictive. Each level assumes the calling ability of the ones above it. This field is used by PIM module of the Integrated Management to communicate with the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for Standard Local Survivability (SLS) on the H.248 gateways.

Available for all analog and IP station types.

| Valid Entries | Usage  |
|---------------|--|
| emergency     | This station can only be used to place emergency calls.  |
| internal      | This station can only make intra-switch calls. This is the default.  |
| local         | This station can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables.                                      |
| toll          | This station can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables.                                  |
| unrestricted  | This station can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users. |

**Related topics:**

[Survivable ARS Analysis Table](#) on page 919

**Survivable GK Node Name**

Any valid previously-administered IP node name. Identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the H.248 gateways. When a valid IP node name is entered into this field, Communication Manager adds the IP address of this gateway to the bottom of the Alternate Gatekeeper List for this IP network region. As H.323 IP stations register with Communication Manager, this list is sent down in the registration confirm message. This allows the IP station to use the IP address of this Survivable Gatekeeper as the call controller of last resort.

If blank, there are no external gatekeeper nodes within a customer's network. This is the default value.

Available only if the station type is an H.323 station for the 46xx or 96xx models.

**Related topics:**

[Name](#) on page 700

[Type](#) on page 909

### Survivable Trunk Dest

Designates certain telephones as not being allowed to receive incoming trunk calls when the Media Gateway is in survivable mode. This field is used by the PIM module of the Integrated Management to successfully interrogate the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for SLS on the H.248 gateways.

Available for all analog and IP station types.

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows this station to be an incoming trunk destination while the Media Gateway is running in survivability mode. This is the default. |
| n           | Prevents this station from receiving incoming trunk calls when in survivable mode.   |

### Switchhook Flash

| Valid Entry | Usage   |
|-------------|---|
| y           | Allows users to use the switchhook flash function to activate Conference/Transfer/Hold and Call Waiting. Required for H.323 station types.                    |
| n           | Disables the flash function so that when the switchhook is pressed while active on a call, the call drops. Requires that Call Waiting Indication is disabled. |

#### Related topics:

[Call Waiting Indication](#) on page 885

### TEI

Available only if the station has a fixed Terminal Endpoint Identifier (TEI).

| Valid Entry | Usage  |
|-------------|--|
| 0 to 63     | A one- or two-digit number that identifies the TEI of the station. |

#### Related topics:

[Fixed TEI](#) on page 891

### Tests

| Valid Entry | Usage   |
|-------------|---|
| y           | Enables port maintenance tests.   |
| n           | Disables port maintenance tests. Required if the equipment (dictaphone) connected to the port does not support these tests. |

## Time of Day Lock Table

| Valid Entry | Usage   |
|-------------|---|
| 1 to 5      | Assigns the station to a Time of Day (TOD) Lock/Unlock table. The assigned table must be administered and active. |
| blank       | Indicates no TOD Lock/Unlock feature is active. This is the default.  |

## TN

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

## Type

The type of telephone. A station type must be administered for each station added to the system.

The following table lists the telephones, virtual telephones, and personal computers that can be administered on Communication Manager. Telephones that are not in the table, require an alias to a supported set type.

 **Note:**

Analog telephones administered with hardware to a virtual extension cannot be changed if TTI is enabled for the system. Contact your Avaya representative for more information.

| Telephone type     | Model                                   | Administer as |
|--------------------|---|---------------|
| Single-line analog | 500                                     | 500           |
|                    | 2500, 2500 with Message Waiting Adjunct | 2500          |
|                    | 6210                                    | 6210          |
|                    | 6211                                    | 6210          |
|                    | 6218                                    | 6218          |
|                    | 6219                                    | 6218          |
|                    | 6220                                    | 6220          |
|                    | 6221                                    | 6220          |
| CallerID           | Analog telephone w/Caller ID            | CallrID       |
|                    | 7101A, 7102A                            | 7101A         |
|                    | 7103A Programmable and Original         | 7103A         |
|                    | 7104A                                   | 7104A         |
|                    | 8110                                    | 8110          |
|                    | DS1FD                                   | DS1FD         |

| Telephone type                               | Model  | Administer as       |
|--|--|---------------------|
|  | 7302H, 7303H                                   | 7303S               |
|  | VRU (voice response unit) with C&D; tones      | VRU                 |
|  | VRU without C&D; tones                         | 2500                |
| Single-line DS1/<br>DSO (Lineside<br>T1/DS1) | DS1 device without forward disconnect          | ops                 |
|  | VRU with forward disconnect without C&D; tones | ds1fd or ds1sa      |
|  | VRU with forward disconnect without C&D; tones | VRUFD or VRUSA      |
| Terminals                                    | 510D   | 510                 |
|  | 515BCT   | 515                 |
| Multi-<br>appearance<br>hybrid               | 7303S  | 7303S, 7313H        |
|  | 7305H  | 7305S               |
|  | 7305S  | 7305S, 7316H, 7317H |
|  | 7309H  | 7309H, 7313H        |
|  | 7313H  | 7313H               |
|  | 7314H  | 7314H               |
|  | 7315H  | 7315H               |
|  | 7316H  | 7316H               |
|  | 7317H  | 7317H               |
| Multi-<br>appearance<br>digital              | 2402   | 2402                |
|  | 2410   | 2410                |
|  | 2420   | 2420                |
|  | 6402   | 6402                |
|  | 6402D  | 6402D               |
|  | 6408   | 6408                |
|  | 6408+  | 6408+               |
|  | 6408D  | 6408D               |
|  | 6408D+   | 6408D+              |
|  | 6416D+   | 6416D+              |
|  | 6424D+   | 6424D+              |
| 7401D  | 7401D  |                     |

| Telephone type           | Model   | Administer as              |
|--------------------------|---|----------------------------|
|                          | 7401+   | 7401+                      |
|                          | 7403D   | 7403D                      |
| Multi-appearance digital | 7404D   | 7404D                      |
|                          | 7405D   | 7405D                      |
|                          | 7406D   | 7406D                      |
|                          | 7406+   | 7406+                      |
|                          | 7407D   | 7407D                      |
|                          | 7407+   | 7407+                      |
|                          | 7410D   | 7410D                      |
|                          | 7410+   | 7410+                      |
|                          | 7434D   | 7434D                      |
|                          | 7444D   | 7444D                      |
|                          | 8403B   | 8403B                      |
|                          | 8405B   | 8405B                      |
|                          | 8405B+  | 8405B+                     |
|                          | 8405D   | 8405D                      |
|                          | 8405D+  | 8405D+                     |
|                          | 8410B   | 8410B                      |
|                          | 8410D   | 8410D                      |
|                          | 8411B   | 8411B                      |
|                          | 8411D   | 8411D                      |
|                          | 8434D   | 8434D                      |
|                          | CALLMASTER I  | 602A1                      |
|                          | CALLMASTER II, III, IV  | 603A1, 603D1, 603E1, 603F1 |
|                          | CALLMASTER VI   | 606A1                      |
|                          | IDT1  | 7403D                      |
| IDT2                     | 7406D   |                            |
| IP Telephone             | 4601+<br> <b>Note:</b><br>When adding a new 4601 IP telephone, you must use the 4601+ station type. This station | 4601+                      |

|                           |   |   |
|---------------------------|---|---|
|                           | type enables the Automatic Callback feature.  |   |
| 4602+                     |  <b>Note:</b><br>When adding a new 4602 IP telephone, you must use the 4602+ station type. This station type enables the Automatic Callback feature. | 4602+   |
| 4606                      |   | 4606  |
| 4610                      |   | 4610  |
| 4612                      |   | 4612  |
| 4620SW IP (G3.5 hardware) |   | 4620  |
| 4621                      |   | 4621  |
| 4622                      |   | 4622  |
| 4624                      |   | 4624  |
| 4625                      |   | 4625  |
| 4690                      |   | 4690  |
| 9610                      |   |  <b>Note:</b><br>If your version of Communication Manager is earlier than version 4.0, administer as 4606. |
| 9620                      |   |  <b>Note:</b><br>If your version of Communication Manager is earlier than version 4.0, administer as 4610. |
| 9630                      |   |  <b>Note:</b><br>If your version of Communication Manager is earlier than version 4.0, administer as 4620. |
| 9640                      |   | 9640  |

|                  |   |   |
|------------------|---|---|
|                  |   |  <b>Note:</b><br>If your version of Communication Manager is earlier than version 4.0, administer as 4620.         |
|                  | 9650  | 9650<br> <b>Note:</b><br>If your version of Communication Manager is earlier than version 4.0, administer as 4620. |
| SIP IP Telephone | <ul style="list-style-type: none"> <li>• 4602SIP with SIP firmware</li> <li>• 4610SIP with SIP firmware</li> <li>• 4620SIP with SIP firmware</li> <li>• 4620SIPCC (Call Center)</li> <li>• Avaya one-X (tm) Deskphone 9620, 9630, 9630G 9640, 96 40G with SIP firmware</li> <li>• SIP Softphone/Avaya one-X Desktop</li> <li>• 1616SIP (Call Center)</li> <li>• Toshiba SP-1020A</li> </ul>  <b>Note:</b><br>Any model telephone that has SIP firmware and is being used for SIP networking must be administered as a 4620SIP telephone. | 4620SIP   |
| IP SoftPhone     | Road-warrior application  | H.323 or DCP type   |
|                  | Native H.323  | H.323   |
|                  | Single-connect  | H.323 or DCP type   |
| ISDN-BRI station | —   | asai  |
|                  | Any NI-BRI (N1 and N2) telephone  | NI-BRI  |
|                  | 7505D   | 7505D   |
|                  | 7506D   | 7506D   |
|                  | 7507D   | 7507D   |
|                  | 8503D   | 8503D   |
|                  | 8510T   | 8510T   |

|   |   |  |
|---|---|--|
|   | 8520T                                     | 8520T  |
| Personal computer                                   | 6300/7300                                 | PC   |
| (voice/data)  | 6538/9                                    | Constellation  |
| Test Line   | ATMS                                      | 105TL  |
| No hardware assigned at the time of administration. |   | <ul style="list-style-type: none"> <li>• XDID (use when Communication Manager later assigns a DID number to this station)</li> <li>• XDIDVIP (use when the administrator later assigns a DID number to this station) virtual (use to map this and other extensions to one physical telephone)</li> </ul> |
| Key telephone system interface                      | —   | K2500  |
| ASAI  | asai link computer telephony adjunct link | asai adjlk   |
| AWOH  | any digital set                           | same as “Multi-appearance Digital”   |
|   | CTI station                               | CTI  |
| CTI   | CTI station                               | CTI  |
| XMOBILE   | EC500, DECT, PHS                          | XMOBILE  |
| ISDN-BRI data module                                | 7500                                      | 7500   |
| SBS Extension                                       | SBS test extension (no hardware)          | sbs  |

**Type of 3PCC Enabled**

The phone number of the off-server or off-switch telephone. Default is none.

**Voice mail Number**

| Valid Entries  | Usage  |
|--|--|
| digits (1 to 9)<br>*<br>#<br>~p (pause)<br>~w/~ (wait)<br>~m (mark)<br>~s (suppress) | Provides a voice mail retrieval AUX dial button on 4xx, 46xx, and 96xx telephones. When a number is entered in this field, the telephone's fixed voice mail retrieval button acts as an autodial button, dialing the number entered in this field to access voice mail. Accepts up to 24 digits.<br><br> <b>Note:</b><br>If this field is left blank, the telephone's fixed voice mail retrieval button acts as a “transfer to voice mail” button that only works for INTUITY AUDIX or QSIG-integrated voice mail systems. Avaya recommends that for INTUITY AUDIX and QSIG-integrated voice mail systems, this |

| Valid Entries | Usage   |
|---------------|---|
|               | field should be left blank. For non-QSIG integrated voice mail systems, this field should be filled in with the appropriate number. |

**XID**

Identifies Layer 2 XID testing capability. Available only for an ISDN-BRI data module or an ASAI link.

**XMOBILE Type**

The type of XMOBILE station. Available only if the **Type** field is XMOBILE and the **Mobility Trunk Group** field is administered.

| Valid Entry | Usage  |
|-------------|--|
| DECT        | The DECT Access System or the AGCS (ROAMEO) IS-136 (TDMA cellular). This represent the ISDN-based DECT system. |
| EC500       | Any public cellular networks.  |
| IPDECT      | The H.323 IP-based DECT system. This can either be the ASCOM or the DeTeWe product.                            |
| PHS         | The DENSO 300M.  |

**Related topics:**

[Mobility Trunk Group](#) on page 897

[Type](#) on page 909

**XOIP Endpoint type**

Available only for 500, 2500, K2500 and CallrID station types.

| Valid Entries               | Usage  |
|-----------------------------|--|
| auto<br>modem<br>fax<br>tty | <p>Identifies the endpoint type of the analog station. Use this field for older or non-standard external equipment such as modems, fax, and TTY devices that are not easily recognized by VoIP resources within Communication Manager. By identifying this external equipment through administration, VoIP firmware can determine whether to immediately attempt to put a call in pass-through mode, or allow the system to handle it normally. Default is auto.</p> <p> <b>Note:</b><br/>This field is intended for exception cases only. For the majority of stations, use the default setting of auto.</p> |

**Related topics:**

[Type](#) on page 909

## Stations With Off-PBX Telephone Integration

Maps an office phone to a cell phone through the Extension to Cellular feature. The office phone can be a standard office number or an administration without hardware (AWOH) station.

Example command: `add off-pbx-telephone station-mapping`

### Stations With Off-PBX Telephone Integration: page 1

#### **Application**

The type of off-PBX application that is associated with the office phone. More than one application can be assigned to an office phone.

| Valid Entry | Usage   |
|-------------|---|
| blank       | Default is blank.   |
| CSP         | cell phone with Extension to Cellular provided by the cellular service provider |
| EC500       | cell phone with Extension to Cellular   |
| HEMU        | Home Enterprise Mobility User   |
| OPS         | SIP Enablement Services (SES)-enabled phone                                     |
| PBFMC       | Public Fixed Mobile Convergence   |
| PVFMC       | Private Fixed Mobile Convergence  |
| SCCAN       | wireless SIP Enablement Services (SES) phone and cell phone                     |
| VEMU        | Visited Enterprise Mobility User  |
| VIEMU       | Visited Initial Enterprise Mobility User  |

#### **CC**

The country code associated with the extension. Accepts up to three digits. Multiple entries that use the same phone number must also have the same country code.

Country code changes made to existing stations or XMOBILE entries are applied to all instances of the phone number.

SAFE (Self-Administered Feature Access Code for EC500) is not recommended on an extension that has an administered country code. Origination mapping can occur with or without a country code. Default is blank.

#### **Configuration Set**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 99     | The Configuration Set number that contains the desired call treatment options for the Extension to Cellular station. |

| Valid Entry | Usage   |
|-------------|---|
|             | The SCCAN application requires two different configuration sets selected for each station. The first set is the value for the WLAN followed by a slash. The second is the value for the cellular network. |
| blank       | Shows blank for Enterprise Mobility User (EMU). Default is blank.   |

### **Dial Prefix**

The dial prefix the system prepends to the off-switch phone number before dialing the off-switch phone. The system deletes the dial prefix when a user enters their cell phone number using the Self Administration Feature (SAFE) access code. The routing tables must be set properly so that the dial prefix “1” is not necessary for correct routing.

- “\*” or “#” must be in the first digit position
- “1” must be used if the phone number is long-distance
- “011” must be used if the phone number is international

### **Phone Number**

The telephone number of the off-switch phone.

May be blank for:

- The first EC500, CSP or PBFMC phones administered
- EC500, CSP, PBFMC, which support Self-Administered Feature Access Code for EC500 (SAFE)

### **Station Extension**

The number of the office telephone that is mapped to the cell telephone. Accepts up to eight digits. This number must be an administered extension. Default is blank.

### **Trunk Selection**

| Valid Entry                         | Usage   |
|-------------------------------------|---|
| ars<br>aar<br>trunk group<br>number | Indicates which trunk group is used for outgoing calls. |

## **Stations With Off-PBX Telephone Integration: page 2**

### **Bridged Calls**

Determines if bridged call appearances extend to the Extension to Cellular cell telephone.

| Valid Entry | Usage   |
|-------------|---|
| termination | Users can use their Extension to Cellular cell telephone to only receive calls from the associated office telephone. Users cannot use the cell phone to originate calls from the associated office phone. Calls originating from the cell phone independent of the office phone are |

| Valid Entry | Usage  |
|-------------|--|
|             | independent of Extension to Cellular and behave exactly as before enabling Extension to Cellular.  |
| origination | Users can originate Extension to Cellular cell telephone calls only from the associated office phone. Users cannot use the cell phone to receive calls from the associated office phone. |
| both        | Users can originate Extension to Cellular cell telephone calls from the associated office telephone, as well as receive calls from the associated office telephone.                      |
| none        | Users cannot originate or receive calls from the office telephone with the cell telephone.   |

**Call Limit**

| Valid Entry      | Usage  |
|------------------|--|
| 1 to 10<br>blank | The maximum number of Extension to Cellular (EC500) calls that can be active simultaneously at a single station. Default is 2 for EC500, CSP, OPS, PBFMC, PVFMC. |

**Calls Allowed**

Identifies the call filter type for an Extension to Cellular station. Determines the type of calls to the office telephone that a user can receive on an Extension to Cellular cell telephone.

| Valid Entry | Usage  |
|-------------|--|
| all         | The cell telephone receives both internal and external calls. Default is all.          |
| internal    | The cell telephone receives only internal calls.                                       |
| external    | The cell telephone receives only external calls.                                       |
| none        | The cell telephone does not receive any calls made to the associated office telephone. |

**Location**

| Valid entry  | Usage   |
|--|---|
| 1 to 50 for medium configurations<br>1 to 250 for large configurations | The location value for each administered OPS, PBFMC, SPFMC or PVFMC application. <ul style="list-style-type: none"> <li>• For a DCP deskset, the location of the media gateway</li> <li>• For an IP deskset, the location of the network region belonging to the deskset</li> </ul> |
| blank  | Trunk location is used for the outgoing calls from Off-PBX endpoints and location of station is used for incoming calls to Off-PBX endpoints. Blank is the default.   |

**Related topics:**

[Loc Number](#) on page 771

[Application](#) on page 916

**Mapping Mode**

The mode of operation for the Extension to Cellular cell phone. These modes control the degree of integration between the cell phone and the office telephone. The modes are valid for Extension to Cellular calls only. For each office telephone, only one cell telephone can be assigned as the origination mode. A cell telephone cannot be assigned as either the origination or both mode more than once.

| Valid Entry | Usage   |
|-------------|---|
| termination | Users can use their Extension to Cellular cell telephone to only receive calls from the associated office telephone. Users cannot use the cell phone to originate calls from the associated office phone. Calls originating from the cell phone independent of the office phone are independent of Extension to Cellular and behave exactly as before enabling Extension to Cellular. |
| origination | Users can originate Extension to Cellular cell telephone calls only from the associated office phone. Users cannot use the cell phone to receive calls from the associated office phone.  |
| both        | Users can originate Extension to Cellular cell telephone calls from the associated office telephone, as well as receive calls from the associated office telephone.   |
| none        | Users cannot originate or receive calls from the office telephone with the cell telephone.  |

**Survivable ARS Analysis Table**

Communication Manager compares dialed numbers with the dialed strings in this table and determines the route pattern for the number.

Example command: `change survivable-ars-analysis`

**Call Type**

| Valid Entry   | Usage                                     |
|---|---|
| emer<br>npa<br>hnpa<br>intl<br>iop<br>locl<br>natl<br>op<br>svc | The call type used for the dialed string. |

## Deny

Indicates whether or not the dialed string should be blocked. The system denies a dialed string that does not match an entered pattern.

## Dialed String

Dialed numbers are matched to the dialed string entry that most closely matches the dialed number. For example, if 297-1234 is dialed and the table has dialed string entries of 297-1 and 297-123, the match is on the 297-123 entry.

An exact match is made on a user-dialed number and dialed string entries with wildcard characters and an equal number of digits. For example, if 424 is dialed, and there is a 424 entry and an X24 entry, the match is on the 424 entry.

Accepts up to 18 digits that the call-processing server analyzes. Also accepts x and X wildcard characters.

## Total Length

| Valid Entry | Usage  |
|-------------|--|
| 0 to 28     | The minimum number of digits required to validate the route. The minimum value when the dial string is populated is the length of the dialed string entry with a maximum value up to 28. Default is blank. |

## Trunk Grp No

The trunk group number that specifies the destination route for the dial plan analysis of this dialed string.

## Survivable Processor

Adds information specific to a Survivable Remote Server (Local Survivable Processor) or to connect certain adjuncts to a Survivable Remote or Survivable Core server (Enterprise Survivable Server). Before administering this screen, you must first assign node names for each Survivable Remote and Survivable Core media server on the IP Node Names screen.

While this screen is administered on the active main server, the information entered applies only to Survivable Remote and Survivable Core servers and does not apply to main servers. When translations are copied to a Survivable Remote or Survivable Core server, the Survivable Remote Server/Survivable Core Server replaces like translations for the main server with the overrides administered on the Survivable Processor screens. That is, use the Survivable Processor screen to administer overrides against adjunct links that have already been administered for the main servers. For more information about ESS, see *Avaya Aura™ Communication Manager Survivable Options*, 03-603633.

Example command: `add survivable-processor n`, where *n* is the assigned node name.

**Survivable processor: page 1****Cluster ID**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 999    | <p>The Cluster ID for the ESS server. The Cluster ID corresponds to the Module ID from the license file of the ESS server.</p> <p> <b>Note:</b><br/>The <code>statuslicense -v</code> shell command on the ESS server displays the Module ID in RFA Module ID.</p> |

**Community**

A community is a virtual group consisting of an ESS server and one or more port networks. Assigning an ESS server to a community associates the ESS server with each IPSI in each port network for that community. Each IPSI is assigned to communities system-wide. The association affects how the ESS server is prioritized for the IPSI in that community, if the ESS server is administered with a Local Preferred or Local Only preference. The Community number for an S8400 ESS server must be set to 2 or greater and must be unique.

**Related topics:**

[System Parameters Port Networks](#) on page 959

**Community Size**

| Valid Entry | Usage   |
|-------------|---|
| Sngl_PN     | For an S8400 ESS server, the value must be Sngl_PN. |
| all         | Default is all.                                     |

**Enable PE for H.248 Gateways**

Enables or disables using the PE interface of the ESS server for H.323 devices such as telephones.

**Enable PE for H.323 Endpoints**

Enables or disables using the PE interface of the ESS server for gateways.

**IP Address**

The IP address that corresponds to the node name.

There are three IP addresses, one for each node name if the survivable processor is a duplicated ESS.

**Related topics:**

[Name](#) on page 700

**Local Only**

Enables or disables the ESS server accepting a request for service from an IPSI. Can be enabled only if the IPSI is located in the same community as the ESS server. Automatically

enabled for S8400 ESS servers and cannot be changed. Otherwise, this field defaults to disabled.

**Related topics:**

[Local Preferred](#) on page 922

[System Preferred](#) on page 923

**Local Preferred**

| Valid Entry | Usage   |
|-------------|---|
| y           | The ESS server accepts a request for service from IPSIs co-located in the same geographical region, WAN segment, LAN segment, district, or business unit. |
| n           | Default when the community size is set to Sngl_PN for an S8400 ESS server and cannot be changed.  |

**Related topics:**

[Community Size](#) on page 921

[Local Only](#) on page 921

[System Preferred](#) on page 923

**Node Name**

The previously-administered name used to identify the server. If the survivable processor is duplicated, there are three node names, one each for the duplicated server pair and one for the server that is active at a given point.

**Priority Score**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 100    | The priority score for this ESS server. Default is 1. |

**Processor Ethernet Network**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 250    | The network region in which the PE interface of the Survivable Remote or Survivable Core server resides. |

**Server A — Server ID**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 256    | Server A ID corresponds to the Server ID configured on the ESS server. The administration on the main server and the configuration on the ESS server must match for the ESS server to register to the main server. |

**Server B — Server ID**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 256    | For duplicated ESS servers, displays the node name of Server B. |

**System Preferred**

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows one ESS server to replace the main server in order to keep as much of the system network intact as possible. Disables <b>Local Preferred</b> and <b>Local Only</b> and cannot be changed. This is the default except for an S8400 ESS server. |
| n           | The default for a S8400 ESS server and cannot be changed.  |

**Related topics:**

[Local Only](#) on page 921

[Local Preferred](#) on page 922

**Type**

| Valid Entry                      | Usage                          |
|----------------------------------|--------------------------------|
| lsp<br>simplex_ess<br>duplex_ess | The survivable processor type. |

**Survivable Processor: page 2 (Processor Channels page)**

Most fields on this page turn to display only when data for the processor channel is inherited from the main server.

**Appl**

Identifies the server application type or adjunct connection used on this channel.

| Valid Entry | Usage                                       |
|-------------|---|
| mis         | Call Management System channel assignments. |
| ccr         | Avaya IQ channel assignments.               |

**Destination Node**

The server or adjunct at the far end of this link consisting of an administered adjunct name, server name, far end IP address, or node name. Leave blank for services local to this server.

**Destination Port**

| Valid Entry        | Usage   |
|--------------------|---|
| 0<br>5000 to 64500 | The far-end port number of this link. An entry of 0 means any port can be used. |

**Enable**

Specifies how data for this processor channel is transferred to the survivable processor.

| Valid Entry | Usage   |
|-------------|---|
| i(nherit)   | This link is to be inherited by the Survivable Remote or Survivable Core server. The survivable processor inherits this processor channel just as it is administered on the main server. Used in the following situations: <ul style="list-style-type: none"> <li>• The main server connects to the adjuncts using a CLAN and you want the Survivable Core server to use the same connectivity</li> <li>• The main server connects to the adjuncts using the PE interface of the main server, and you want the Survivable Remote or Survivable Core server to connect to the adjunct using its PE interface.</li> </ul> |
| n(o)        | This processor channel is disabled on the Survivable Remote or Survivable Core server. The survivable processor does not use this channel. This is the default.   |
| o(verwrite) | The survivable processor overwrites the processor channel information sent in the file sync from the main server. Allows the administered adjunct attributes to be modified uniquely for each individual Survivable Remote or Survivable Core server.   |

**Interface Channel**

The channel number or the TCP/IP listen port channel to carry this processor (virtual) channel.

| Valid Entry   | Usage  |
|---------------|--|
| 5000 to 64500 | For ethernet or ppp. For TCP/IP, interface channel numbers are in the range 5000 to 64500. The value 5001 is recommended for CMS, and 5003 is recommended for DCS. |
| 0             | Any port can be used.  |

**Interface Link**

| Valid Entry   | Usage  |
|---------------|--|
| 1 to 254      | The physical link carrying this processor (virtual) channel.                           |
| p (processor) | Communication Manager's Processor Ethernet interface is used for adjunct connectivity. |
| blank         | Not administered.  |

**Mode**

| Valid Entry | Usage                      |
|-------------|----------------------------|
| c(lient)    | The IP session is passive. |
| s(erver)    | The IP session is active.  |

**Proc Chan**

Displays the processor channel number used for this link.

**Related topics:**

[Proc Chan](#) on page 836

**Session - Local/Remote**

| Valid Entry       | Usage  |
|-------------------|--|
| 1 to 384<br>blank | The Local and Remote Session numbers. For each connection, the Local Session number on the Avaya server must equal the Remote Session number on the remote server and vice versa. It is allowed, and sometimes convenient, to use the same number for the Local and Remote Session numbers for two or more connections. Local and Remote Session numbers must be consistent between endpoints. |

**Survivable Processor: page 3 (IP Services page)**

Used when an AESVCS or a CDR connects to the Survivable Remote or Survivable Core server.

**Enabled**

Specifies how data for each specified service type is transferred to the survivable processor.

| Valid Entry | Usage   |
|-------------|---|
| i(nherit)   | This link is to be inherited by the Survivable Remote or Survivable Core server. The survivable processor inherits this service type just as it is administered on the main server. Used in the following situations: <ul style="list-style-type: none"> <li>• The main server connects to the adjuncts using a CLAN and you want the Survivable Core Server to use the same connectivity</li> <li>• The main server connects to the adjuncts using the main server's PE interface and you want the Survivable Remote or Survivable Core server to connect to the adjunct using its PE interface</li> </ul> |
| n(o)        | This IP services link is disabled on the Survivable Remote or Survivable Core server. This is the default.  |
| o(verwrite) | Overwrites the processor channel information sent in the file sync from the main server. Allows the administered CDR or AE Services attributes to be modified uniquely for each individual Survivable Remote or Survivable Core server.   |

**Local Node**

Displays the previously-administered node name.

**Related topics:**

[Name](#) on page 700

**Local Port**

The originating port number. For client applications such as Call Detail Recording (CDR), this field defaults to 0.

**Remote Node**

The name at the far end of the link for the CDR. Does not apply for AESVCS.

**Remote Port**

| Valid Entry   | Usage   |
|---------------|---|
| 5000 to 65500 | The port number of the destination for CDR or AESVCS. This number must match the port administered on the CDR or AESVCS server. |

**Service Type**

| Valid Entry            | Usage                 |
|------------------------|-----------------------|
| CDR1<br>CDR2<br>AESVCS | The service provided. |

**Related topics:**

[Service Type](#) on page 717

**Store to disk**

Enables or disables the storage of the CDR data on the local hard drive of the Survivable Remote or Survivable Core server. Pertains only to service types set to CDR1 or CDR2.

**Survivable Processor: page 4 (IP Services — Session Layer Timers page)**

Available only if CDR1 or CDR2 is administered, and if processor channel information is administered to be overwritten.

**Related topics:**

[Enabled](#) on page 925

[Service Type](#) on page 926

**Connectivity Time**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 255    | The amount of time that the link can be idle before Communication Manager sends a connectivity message to ensure the link is still up. Default is 60. |

**Packet Resp Timer**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 255    | The number of seconds to wait from the time a packet is sent until a response (acknowledgement) is received from the far-end, before trying to resend the packet. Default is 30. |

**Reliable Protocol**

Enables or disables using a reliable protocol over this link. A reliable protocol should be used if the adjunct on the far end of the link supports it.

**Service Type**

Displays the previously-administered service type.

**Related topics:**

[Service Type](#) on page 926

**Session Connect Message Cntr**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 5      | The number of times Communication Manager tries to establish a connection with the far-end adjunct. |

**SPDU Cntr**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 5      | The number of times Communication Manager transmits a unit of protocol data before generating an error. |

**System Capacity**

Provides a status of administered capacity information and a snapshot status of system resources. For more information, see *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431. Detailed system capacity information can be found in *Avaya Aura™ Communication Manager System Capacities Table*, 03-300511.

**System Configuration**

The System Configuration screen shows all the boards on the system that are available for connecting telephones. Used to view the board number, board type, circuit-pack type, and status of each board's ports.

## System Parameters Call Coverage/Call Forwarding

Sets the system-wide parameters for call coverage and call forwarding.

Example command: `change system-parameters coverage-forwarding`

### CALL COVERAGE / FORWARDING PARAMETERS

#### Coverage - Caller Response Interval (seconds)

| Valid Entry | Usage  |
|-------------|--|
| 0 to 10     | The time in seconds an internal caller has before a call redirects to the called party's first coverage point. |

#### COR/FRL check for Covered and Forwarded Calls

| Valid Entry | Usage  |
|-------------|--|
| y           | Communication Manager checks the following: <ul style="list-style-type: none"> <li>• COR of the calling and forwarded-to parties for local forwarding.</li> <li>• COR and FRL of the calling party and outgoing trunk for remote forwarding and remote coverage calls.</li> </ul>                                    |
| n           | Communication Manager does not check the following: <ul style="list-style-type: none"> <li>• COR of the calling and forwarded-to parties for local forwarding.</li> <li>• COR and FRL of the calling party and outgoing trunk for remote forwarding and remote coverage calls. This is the default value.</li> </ul> |

#### Local Cvg Subsequent Redirection/CFWD No Ans Interval (rings)

| Valid Entry | Usage  |
|-------------|--|
| 1 to 99     | Specifies: <ul style="list-style-type: none"> <li>• The number of rings applied at a local coverage point before a call redirects to the next coverage point</li> <li>• The number of rings applied at the principal before a call forwards when Call Forwarding Busy/Don't Answer is activated</li> </ul> <p> <b>Note:</b><br/>When ringing local destinations, such as an office environment, a short interval often is appropriate because the intended party either is near the telephone or not present. However, if the call is left at an off-net destination for only a short interval, the call can be redirected to the next destination before the intended party has any real chance of answering the call.</p> |

#### Location for Covered and Forwarded Calls

Determines the location number used for coverage and forwarding.

| Valid Entry | Usage  |
|-------------|--|
| called      | <ul style="list-style-type: none"> <li>• If the called party is registered or in-service, coverage and forwarding use the called party's physical phone's location number.</li> <li>• If the called party is AWOH (x-port) or unregistered, coverage and forwarding use the location number associated with the administered ARS FAC.</li> <li>• When the forwarding or coverage destination is to UDP instead of to an external destination starting with the ARS FAC, routing is always based on the caller's physical phone's location regardless of how this field is administered.</li> </ul> <p>This is the default.</p> |
| caller      | Coverage and forwarding use the caller's physical phone's location number.   |

**Related topics:**

[ARS FAC](#) on page 771

***Off-Net Cvg Subsequent Redirection/CFWD No Ans Interval (rings)***

| Valid Entry | Usage  |
|-------------|--|
| 1 to 99     | <p>Specifies:</p> <ul style="list-style-type: none"> <li>• The number of rings applied at an off-net coverage point before a call is redirected to the next coverage point</li> <li>• The number of rings applied at an off-net forwarded-to destination before the call is redirected to coverage.</li> </ul> <p> <b>Note:</b><br/>When ringing local destinations, such as an office environment, a short interval often is appropriate because the intended party either is near the telephone or not present. However, if the call is left at an off-net destination for only a short interval, the call can be redirected to the next destination before the intended party has any real chance of answering the call.</p> |

***PGN/TN/COR for Covered and Forwarded Calls***

| Valid Entry | Usage  |
|-------------|--|
| called      | Communication Manager checks for permissions (tenant number, partition group number, and COR) between the actual called party (forwarding party) and forwarded-to party. When the check is successful, the call is routed to the forwarded-to party. Permission check for COR is only done if the COR/FRL check for Covered and Forwarded Calls field is set to y. |
| caller      | Communication Manager checks for permissions (tenant number, partition group number, and COR) between the calling party and  |

| Valid Entry | Usage   |
|-------------|---|
|             | forwarded-to party. When the check is successful, the call is routed to the forwarded-to party. Permission check for COR is only done if the COR/ FRL check for Covered and Forwarded Calls field is set to y. This is the default value. |

**Threshold for Blocking Off-Net Redirection of Incoming Trunk Calls**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 7      | If the number of incoming trunk calls routes within the Call Forward timer, the block commences. Applies for those occasions when an incoming call to a station redirects off-net. At that time, the Call Forward timer activates to block any further incoming calls to that station from being redirected off-net until the timer expires. |
| n (all)     | Call processing never activates the Call Forward timer. Therefore, any number of calls to a principal can be redirected off-net.   |

**COVERAGE**

**Criteria for Logged Off/PSA/TTI Stations**

Enables or disables the call coverage criteria for logged-off IP/PSA/TTI stations. By default, the value is n.

**Related topics:**

[COVERAGE CRITERIA](#) on page 509

**External Coverage Treatment for Transferred Incoming Trunk Calls**

Enables or disables external coverage treatment for incoming trunk calls that redirect to coverage.

**Immediate Redirection on Receipt of PROGRESS Inband Information**

Determines if a call is immediately redirected to coverage when an ISDN PROGRESS message is received. Pertains only to CCRON and QSIG VALU coverage calls redirected over end-to-end ISDN facilities.

However, the message might indicate that the cell telephone is not available to receive calls and should be redirected.

Available only if:

- **Coverage of Calls Redirected Off-Net** is enabled
- The Value-Added Avaya (VALU) feature is enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| y           | Immediately redirect an off-net coverage/forwarded call to the next coverage point. Users in European countries following the ETSI standard and redirecting to GSM cellular telephones should consider enabling this field. |

| Valid Entry | Usage   |
|-------------|---|
| n           | Does not immediately redirect an off-net coverage/forwarded call to the next coverage point. Users in the United States should consider disabling this field because PROGRESS messages with the <b>Progress Indicator</b> field set to inband information are sent for a variety of reasons that are not associated with unavailable cellular telephones. |

**Related topics:**

[Cvg Of Calls Redirected Off-net](#) on page 944

[Value Added \(VALU\)](#) on page 955

**Keep Held SBA at Coverage Point**

Determines how a covering user who has placed an answered coverage call on hold is treated if the original principal bridges onto the call.

| Valid Entry | Usage  |
|-------------|--|
| y           | Keeps the coverage party on the call. The coverage party remains on hold, but might enter the call along with the principal and the calling party. |
| n           | Drops the coverage party from the call.  |

**Maintain SBA At Principal**

Allows a user to maintain a simulated bridged appearance (SBA) when a call redirects to coverage.

| Valid Entry | Usage   |
|-------------|---|
| y           | Maintains a simulated bridged appearance on the principal's telephone when a call redirects to coverage. DCS with rerouting will not be attempted after coverage.                                   |
| n           | No SBA is maintained on the principal's telephone. DCS with rerouting is attempted, and if successful, the principal loses the bridged appearance and the ability to bridge onto the coverage call. |

**QSIG VALU Coverage Overrides QSIG Diversion with Rerouting**

Specifies whether or not, with both QSIG Diversion with Rerouting and QSIG VALU turned on, Coverage After Forwarding for the station works for calls that go to remote coverage.

Available only if **Basic Supplementary Services** and **Supplementary Services with Rerouting** are both enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| y           | QSIG VALU call coverage takes precedence. If Coverage After Forwarding is enabled for a station, the call can receive coverage after rerouting. |
| n           | With QSIG Diversion with Rerouting turned on, the local system passes control of a forwarded call to the remote QSIG server on which the        |

| Valid Entry | Usage   |
|-------------|---|
|             | forwarding destination resides. The forwarded call cannot return to coverage for the user who originally received the call. |

**Related topics:**

[Basic Supplementary Services](#) on page 954

[Supplementary Services with Rerouting](#) on page 955

**Station Hunt Before Coverage**

Determines whether or not a call to a busy station performs station hunting before going to coverage.

**FORWARDING**

**Call Forward Override**

Specifies how to treat a call from a forwarded-to party to the forwarded-from party.

| Valid Entry | Usage  |
|-------------|--|
| y           | Overrides the Call Forwarding feature by allowing a forwarded-to station to complete a call to the forwarded-from station. |
| n           | Directs the system to forward calls to a station even when they are from the forwarded-to party.                           |

**Coverage After Forwarding**

Determines whether or not an unanswered forwarded call is provided coverage treatment.

| Valid Entry | Usage  |
|-------------|--|
| y           | Coverage treatment is provided to unanswered forwarded calls.  |
| n           | No coverage treatment is provided to unanswered forwarded calls. The call remains at the forwarded-to destination. |

**COVERAGE OF CALLS REDIRECTED OFF-NET (CCRON)**

**Activate Answer Detection (Preserves SBA) On Final CCRON Cvg Point**

Determines whether or not a simulated bridge appearance (SBA) is maintained on the principal when a call is directed to a final off-net coverage point. This field has no consequence when the off-net call is carried end-to-end by ISDN facilities; the SBA is maintained and there is no cut-through delay.

Available only if **Coverage of Calls Redirected Off-Net Enabled** is enabled.

| Valid Entry | Usage   |
|-------------|---|
| y           | Maintains a simulated bridged appearance on the principal when redirecting to a final off-net coverage point.   |
| n           | Drops the SBA on the principal's telephone when the call redirects off-net at the last coverage point, eliminating the cut-through delay inherent in CCRON calls, but sacrificing the principal's ability to answer the call. |

**Related topics:**

[Coverage Of Calls Redirected Off-Net Enabled](#) on page 933

**Coverage Of Calls Redirected Off-Net Enabled**

Controls the Coverage of Calls Redirected Off-Net (CCRON) feature. Disables this feature if the demand on the call classifier port resources degrades other services provided by Communication Manager.

Available only if **Coverage of Calls Redirected Off-Net** is enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| y           | Communication Manager monitors off-net coverage/forwarded calls and provides further coverage treatment for unanswered calls.                    |
| n           | Communication Manager does not monitor off-net coverage/ forwarded calls. No further coverage treatment is provided if the calls are unanswered. |

**Related topics:**

[Cvg Of Calls Redirected Off-net](#) on page 944

**Disable call classifier for CCRON over ISDN trunks**

Enables or disables the use of a call classifier on a CCRON call over ISDN facilities. When a CCRON call routes offnet over ISDN end-to-end facilities, no call classifier is attached to the call. If, subsequently during the call, an ISDN PROGRESS or ALERT message is received that indicates that interworking has occurred, a call classifier is normally attached to the call and assumes precedences over ISDN trunk signalling. This field can direct Communication Manager to dispense with the call classifier on interworked calls and rely on the ISDN trunk signalling messages.

| Valid Entry | Usage   |
|-------------|---|
| y           | Disables the call classifier for CCRON calls over interworked trunk facilities. |
| n           | Enables the call classifier for CCRON calls over interworked trunk facilities.  |

**Disable call classifier for CCRON over SIP Enablement Services (SES) trunks**

| Valid Entry | Usage  |
|-------------|--|
| y           | Disables the call classifier for CCRON calls over interworked trunk facilities. Directs Communication Manager to dispense with the call classifier on interworked calls and rely on the SIP Enablement Services (SES) trunk signalling messages. |
| n           | Enables the call classifier for CCRON calls over interworked trunk facilities.   |

**Ignore Network Answer Supervision**

Administers whether or not a call classifier for network answer supervision is used to determine when a call is answered. CCRON might use a call classifier port to determine whether an off-

net coverage or forwarded call has been answered, discarding other information that might indicate an answered state.

Available only if **Coverage of Calls Redirected Off-Net Enabled** is enabled.

| Valid Entry | Usage   |
|-------------|---|
| y           | Ignore network answer supervision and rely on the call classifier to determine when a call is answered. Provides accurate answer supervision for tandem calls redirected to the public network. |
| n           | Treat network answer supervision as a true answer. Preserves network answer supervision information.  |

**Related topics:**

[Coverage Of Calls Redirected Off-Net Enabled](#) on page 933

**CHAINED CALL FORWARDING**

***Maximum Number of Call Forwarding Hops***

Available only if Chained Call Forwarding is enabled.

| Valid Entry | Usage   |
|-------------|---|
| 3 to 10     | The number of hops allowed in the forwarding chain. |

**Related topics:**

[Chained Call Forwarding](#) on page 624

***Station Coverage Path For Coverage After Forwarding***

Specifies what coverage path the call follows. Available only if Chained Call Forwarding is enabled.

**Related topics:**

[Chained Call Forwarding](#) on page 624

**System Parameters Country Options**

This screen implements parameters associated with certain international, including North American, call characteristics. This screen cannot be changed. See Avaya technical support representative to modify any of the values here. This table shows the country codes that are used in Communication Manager. The Country Code is used by various fields and screens throughout the system.

Example command: `change system-parameters customer-options`

## Country options table

| Code | Country                             | Ringing Signal Voltage, Frequency, and Cadence   |
|------|-------------------------------------|--|
| 1    | United States, Canada, Korea, India | 300v peak to peak, < 200v peak to ground; < 70 Hz; < 5s on > 1s off<br>Korea: 20 Hz, 75 to 85 Volts (AC), Cadence: 1 sec on, 2 sec off   |
| 2    | Australia, New Zealand              | 75 +/- 20 VRMS superimposed on 48 V dc at 14.5 to 55 Hz with cadence 400ms on, 200ms off, 400ms on, 2000ms off<br>New Zealand: Ringing voltage at the customer's premises not less than 38 V rms (25Hz) on top of 50V d.c; 20 Hz; 400ms on, 200ms off, 400ms on, 2000ms off                              |
| 3    | Japan                               | 75 VRMS(75-10VRMS <= x <= 75+8VRMS), 15-20 Hz and cadence of 1second on and 2 seconds off is required  |
| 4    | Italy                               | 20 to 50 Hz, 26 to 80 Volts rms superimposed on 48 V dc, 1 sec on, 4 sec off<br>ETSI countries: 30 Volts rms, superimposed on a DC voltage of 50 Volts, 25 or 50 hz, cadence of 1 sec on, 5 sec off  |
| 5    | Netherlands                         | 25 Hz, 35 to 90 Volts rms superimposed on 66 V dc, 1 sec on, 4 sec off. Note that 50 Hz is recommended, and another cadence may be 0.4 sec on, 0.2 sec off, 0.4 sec on, 4 sec off<br>ETSI countries: 30 Volts rms, superimposed on a DC voltage of 50 Volts, 25 or 50 hz, cadence of 1 sec on, 5 sec off |
| 6    | Singapore                           | 75V at 24Hz with a cadence of 0.4 seconds on, 0.2 seconds off, 0.4 seconds on and 2.0 seconds off.   |
| 7    | Mexico                              | 25 Hz, 70 +/- 20 Vrms superimposed on 48Vdc<br>Cadence 1 sec on, 4 sec off, flashhook is 100 ms  |
| 8    | Belgium, Luxembourg, Korea          | 25 Hz, 25 to 75 Volts rms superimposed on 48 V dc, 1 sec on, 3 sec off<br>Korea: 20 Hz, 75 to 85 Volts (AC), Cadence: 1 sec on, 2 sec off<br>ETSI countries: 30 Volts rms, superimposed on a DC voltage of 50 Volts, 25 or 50 hz, cadence of 1 sec on, 5 sec off   |
| 9    | Saudi Arabia                        |  |

| Code | Country                  | Ringing Signal Voltage, Frequency, and Cadence   |
|------|--------------------------|--|
| 10   | United Kingdom           | <p>U.K.: 15 to 26.25 Hz, 25 to 100 Volts rms superimposed on 48 V dc, 0.35 on, 0.22 off then start in at any point in: 0.4 sec on, 0.2 sec off, 0.4 sec on, 2 sec off. Note 1: 48v DC may be present during the whole cadence or may be confined to silent periods. Note 2: Some exchanges provide a facility known as immediate ring; in this case an initial burst of ringing 20 msec to 1 sec in length immediately precedes switching to any point in the normal ringing cycle.</p> <p>Ireland: 25 Hz, 30 to 90 Volts rms superimposed on 50 V dc, 0.4 sec on, 0.2 sec off, 0.4 sec on, 2 sec off another possible cadence is 0.375 sec on, 0.250 sec off, 0.375 sec on, 2 sec off.</p> <p>ETSI countries: 30 Volts rms, superimposed on a DC voltage of 50 Volts, 25 or 50 hz, cadence of 1 sec on, 5 sec off</p> |
| 11   | Spain                    | <p>20 to 30 Hz, 35 to 75 Volts rms superimposed on 48 V dc, 1 to 1.5 sec on, 3 sec off</p> <p>ETSI countries: 30 Volts rms, superimposed on a DC voltage of 50 Volts, 25 or 50 hz, cadence of 1 sec on, 5 sec off</p>  |
| 12   | France                   | <p>50 Hz, 28 to 90 Volts rms superimposed on 0.45 to 54 V dc, 1.5 sec on, 3.5 sec off</p> <p>ETSI countries: 30 Volts rms, superimposed on a DC voltage of 50 Volts, 25 or 50 hz, cadence of 1 sec on, 5 sec off</p>   |
| 13   | Germany                  | <p>Germany: 25 Hz, 32 to 75 Volts rms superimposed on 0 to 85 V dc, 1 sec on, 4 sec off</p> <p>Austria: 40 to 55 Hz, 25 to 60 Volts rms superimposed on 20 to 60 V dc, 1 sec on, 5 sec off +/- 20%</p> <p>ETSI countries: 30 Volts rms, superimposed on a DC voltage of 50 Volts, 25 or 50 hz, cadence of 1 sec on, 5 sec off</p>  |
| 14   | Czech Republic, Slovakia |  |
| 15   | Russia (CIS)             | <p>25+/-2 Hz, 95+/-5 Volts eff, local call cadence: first ring 0.3-4.5 sec then 1 second on 4 seconds Off toll automatic cadence 1 sec On 2 sec Off toll operator: manual sending</p>  |
| 16   | Argentina                | <p>25Hz; 75 Vrms superimposed on 48 Vdc; 1s on 4s off</p>  |

| Code | Country      | Ringling Signal Voltage, Frequency, and Cadence   |
|------|--------------|---|
| 17   | Greece       |   |
| 18   | China        | 25Hz +/- 3Hz; 75 +/- 15 Vrms; Harmonic Distortion <= 10%; 1 sec ON, 4 secs OFF  |
| 19   | Hong Kong    | 75 +/- 20 VRMS superimposed on -40 to -48 V dc at 25 Hz +/- 10% with cadence 0.4 s on, 0.2 s off, 0.4 s on, 3.0 s off   |
| 20   | Thailand     |   |
| 21   | Macedonia    |   |
| 22   | Poland       |   |
| 23   | Brazil       | 25Hz +/-2.5Hz; minimum of 40 Vrms; 1s on, 4s off for equipment supporting up to six trunks only otherwise 25Hz +/-2.5Hz; minimum of 70+/-15 Vrms at a continuous emitting condition under no load, overlapping a DC level.  |
| 24   | Nordic       | Finland: 25 Hz, 35 to 75 Volts rms superimposed on 44 to 58 V dc, 1 sec on, 4 sec off<br>25 Hz, 40 to 120 Volts rms superimposed on 44 to 56 V dc, 0,75 on, 7,5 off +/- 20 %<br>25 Hz, 28 to 90 Volts rms superimposed on 24 to 60 V dc, 1 sec on, 4 sec off<br>25 and 50 Hz, 30 to 90 Volts rms superimposed on 33 to 60 V dc, 1 sec off, 5 sec off<br>ETSI countries: 30 Volts rms, superimposed on a DC voltage of 50 Volts, 25 or 50 hz, cadence of 1 sec on, 5 sec off |
| 25   | South Africa |   |

**Related topics:**

[Analog Line Transmission](#) on page 773

**Dial Tone Validation Timer (sec)**

Available only when Tone Detection Mode is 4 or 5. Valid with TN420C or later Tone Detector circuit pack.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 6375   | Displays number of milliseconds in increments of 25 that the dial tone validation routine uses to sample transmissions. |

**Related topics:**

[Tone Detection Mode](#) on page 939

### Disconnect on No Answer by Call Type

Enables or disables the system from disconnecting calls that are not answered. Drops outgoing trunk calls, except DCS and AAR, that users leave unanswered too long.

### Directory Search Sort Order

Available only for the Cyrillic or Ukrainian display character set.

| Valid Entry | Usage   |
|-------------|---|
| Cyrillic    | Cyrillic Collation is used for integrated directory name search and result sorting. This is the default value.  |
| Roman       | Eurofont Latin Collation is used for directory name search and result sorting. The letters to be searched in the specified order for dial pad button presses are defined in the row for each key. |

#### Related topics:

[Display Character Set](#) on page 938

### Display Character Set

| Valid Entry                                | Usage   |
|--|---|
| Cyrillic<br>Katakana<br>Roman<br>Ukrainian | The character set used for all non-native name values that do not have an ASCII-only restriction. |

#### Note:

Cyrillic, Roman, and Ukrainian map to the Eurofont character set. For Katakana, the Optrex font is used. If a Communication Manager server uses non-English in any name field, characters on a BRI station are not displayed correctly.

#### Warning:

Changing the value in this field might cause some telephones to perform improperly, and can cause non-ASCII data in non-native names to display incorrectly on telephones. To correct this, non-native names of previously administered stations must be removed and re-administered using non-ASCII characters. This includes any display messages that have been administered.

### Enable Busy Tone Disconnect for Analog Loop-start Trunks

Enables or disables Busy Tone Disconnect. When enabled, Communication Manager recognizes a busy tone from the local telephone company central office as a disconnect signal.

### Howler After Busy

Enables or disables howler tone when users leave their analog telephone off-hook too long.

### Set Layer 1 timer T1 to 30 seconds

Specifies whether or not the Layer 1 timer is set to 30 seconds.

## STONE DETECTION PARAMETERS

### *Interdigit Pause*

Specifies the maximum length of the inter-digit pause. Breaks lasting less than this range will be bridged or ignored. (Valid with TN420C or later Tone Detector circuit pack.)

| Valid Entry | Usage   |
|-------------|---------|
| short       | 5–30ms  |
| long        | 20–40ms |

### *Tone Detection Mode*

The type of tone detection. The country code specifies the type of tone detection used on a TN420B or later tone-detection circuit pack.

| Valid Entry | Usage   |
|-------------|---|
| 1           | Precise Italian tone detection algorithm  |
| 2           | Precise Australian tone detection algorithm   |
| 3           | Precise UK tone detection algorithm   |
| 4           | Imprecise normal broadband filter algorithm (valid with TN420C or later Tone Detector circuit pack) |
| 5           | Imprecise wideband filter algorithm (valid with TN420C or later Tone Detector circuit pack)         |

## System Parameters Customer Options

Shows which optional features are enabled for the system, as determined by the installed license file. All fields on this screen are display only. For questions about disabling or enabling one of these features, contact an Avaya representative.

Example command: `change system-parameters customer-options`

### **System parameters customer options: page 1**

#### ***G3 Version***

Identifies the version of Avaya Communication Manager being used.

#### ***Location***

Indicates the location of this Avaya server or switch.

| Valid Entry | Usage   |
|-------------|---|
| 1           | Canada or the United States   |
| 2           | Any other location. Allows the use of International Consolidation circuit packs and telephones. |

**Maximum Off-PBX Telephones - EC500**

Stations that are administered for any Extension to Cellular (EC500/ CSP) application count against this limit.

The “license max” value is defined as follows:

- On legacy systems, the upper limit is 1/2 of the maximum number of administrable stations. Legacy platforms do not support SIP Enablement Services (SES) trunks.
- On Linux systems, the upper limit is the maximum number of administrable stations.

**Maximum Off-PBX Telephones - OPS**

Stations that are administered for any SIP Extension to Cellular/OPS application count against this limit. The “license max” value is defined as follows:

- On legacy systems, the upper limit is 1/2 of the maximum number of administrable stations. Note that legacy platforms do not support SIP Enablement Services (SES) trunks.
- On Linux systems, the maximum number of administrable stations.

**Maximum Off-PBX Telephones — PBFMC**

Number of stations administered for Public Fixed-Mobile Convergence. Each station is allowed only one PBFMC application. The “license max” value is defined as follows:

- On legacy systems, the upper limit is 1/2 of the maximum number of administrable stations. Legacy platforms do not support SIP Enablement Services (SES) trunks.
- On Linux systems, the upper limit is the maximum number of administrable stations.

**Maximum Off-PBX Telephones - PVFMC**

Number of stations administered for Private Fixed-Mobile Convergence. Each station is allowed only one PVFMC application. The “license max” upper limit is:

- On legacy systems, 1/2 of the maximum number of administrable stations. Legacy platforms do not support SIP Enablement Services (SES) trunks.
- On Linux systems, the maximum number of administrable stations.

**Maximum Off-PBX Telephones - SCCAN**

The “license max” value is defined as follows:

- SCCAN is only available on Linux systems. The upper limit is the maximum number of administrable stations.
- Stations that are administered for any Extension to Cellular/OPS application count against this limit.

**Maximum Stations**

Displays the maximum number of stations allowed in the system.

**Maximum XMOBILE Stations**

Specifies the maximum number of allowable XMOBILE stations. In general, each XMOBILE station is assigned to a wireless handset. Each XMOBILE station counts as a station and a port in terms of system configuration.

**Platform**

Displays the platform being used.

| Valid Entry | Usage   |
|-------------|---------|
| 28          | VCM     |
| 29          | VCM_ESS |
| 30          | VCM_LSP |

**Platform Maximum Ports**

Number of active ports.

**Software Package**

Indicates whether the software package license is Standard or Enterprise.

**Used**

The actual current usage as compared to the system maximum.

**System parameters customer options: page 2****Maximum Administered Ad-hoc Video Conferencing Ports**

Defines the number of ad-hoc ports allowed for the system; one for each simultaneous active conference port. The maximum number of ad-hoc video conferencing ports allowed is the sum of the maximum allowed IP trunks and the maximum allowed SIP trunks on your system.

**Maximum Administered IP Trunks**

Defines the maximum number of IP trunks administered.

**Maximum Administered Remote Office Trunks**

Defines the maximum number of IP endpoints based on the endpoint.

**Maximum Administered SIP Trunks**

Defines the maximum number of SIP Enablement Services (SES) trunks administered.

**Maximum Concurrently Registered IP eCons**

Specifies the maximum number of IP SoftConsoles that can be registered at one time. The maximum number depends on the type of system.

**Maximum Concurrently Registered IP Stations**

Specifies the maximum number of IP stations that can be registered at one time.

**Maximum G250/G350/G700 VAL Sources**

Specifies the maximum number of VAL announcement sources.

**Maximum Number of DS1 Boards with Echo Cancellation**

Displays the number of DS1 circuit packs that can have echo cancellation.

**Maximum Number of Expanded Meet-me Conference Ports**

The maximum number of Expanded Meet-me Conference ports on the system.

**Maximum TN2501 VAL Boards**

The maximum number of TN2501AP (Voice Announcement over LAN) boards allowed in this system.

**Maximum TN2602 Boards with 80 VoIP Channels**

The total number of TN2602AP boards that can be administered with 80 VoIP channels.

**Maximum TN2602 Boards with 320 VoIP Channels**

The total number of TN2602AP boards that can be administered with 320 VoIP channels.

**Maximum Video Capable IP Softphones**

The maximum number of IP Softphones that are video-capable. The maximum number depends on the type of system.

**Maximum Video Capable Stations**

The maximum number of stations that are video-capable. The maximum number depends on the type of system.

**Used**

For each item with a capacity listed, the USED value is the actual number of units currently in use.

**System parameters customer options: page 3**

**Abbreviated Dialing Enhanced List**

Provides the capability to store and retrieve dialing lists that simplify or eliminate dialing. The stored entries are organized in number lists. There are three types of number lists: personal, group, and enhanced.

**Access Security Gateway (ASG)**

Provides an additional level of security for remote administration.

**A/D Grp/Sys List Dialing Start at 01**

Allows for numbering of Abbreviated Dialing group or system lists starting with 01, rather than simply 1.

**Analog Trunk Incoming Call ID**

Allows collection and display of the name and number of an incoming call on analog trunks.

**Answer Supervision by Call Classifier**

Indicates whether or not the system contains a call classifier circuit pack. This circuit pack detects tones and voice-frequency signals on the line and determines whether a call has been answered.

**ARS**

Provides access to public and private communications networks. Long-distance calls can be routed over the best available and most economical routes. Provides partitioning of ARS routing patterns.

**ARS/AAR Dialing without FAC**

Provides for Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS) calls without dialing a feature access code (FAC).

**ARS/AAR Partitioning**

Provides the ability to partition AAR and ARS into eight user groups within a single server running Avaya Communication Manager. Can establish individual routing treatment for each group.

**ASAI Link Core Capabilities**

Provides linkage between Avaya Communication Manager and adjuncts. CallVisor ASAI improves the call handling efficiency of ACD agents and other system users by allowing an adjunct to monitor, initiate, control, and terminate calls on the server running Communication Manager.

 **Note:**

This field applies only to links administered as type asai.

**ASAI Link Plus Capabilities**

Provides linkage between Avaya Communication Manager and adjuncts. If enabled, then the following ASAI capability groups are also enabled:

- Adjunct Routing
- Answering Machine Detection
- Selective Listening
- Switch Classified Outbound Calls
- ISDN Redirecting Number Information - the original dialed number information is provided within the ASAI messages if it arrives in ISDN SETUP messages from the public networks as either Original Dialed Number or Redirecting Party Number.

 **Note:**

This field applies only to links administered as type asai.

**Asynch. Transfer Mode (ATM) PNC**

PNC ATM PNC can be enabled only if:

- All prior fiber-link administration has been removed
- All “switch-node” and “dup-switch-node” carrier types have been removed.

**Asynch. Transfer Mode (ATM) Trunking**

If ATM trunking is enabled, multiple ISDN-PRI T1 or E1 trunks can be emulated on one ATM pipe. Enables circuit emulation service (CES).

**Related topics:**

[Carrier Medium](#) on page 722

### **ATMS**

Provides for voice and data trunk facilities to be measured for satisfactory transmission performance.

### **ATM WAN Spare Processor**

Indicates whether or not an ATM WAN spare processor is part of the system. An ATM WAN spare processor acts as a PPN in the event of network failure, and can function as an SPE if the main PPN is not functional.

### **Attendant Vectoring**

Enables or disables Attendant Vectoring.

### **Audible Message Waiting**

Enables or disables audible message waiting.

### **Authorization Codes**

Enables or disables the use of Authorization Codes. Authorization Codes provide levels of calling privileges that override in-place restrictions. In addition to facilities access, authorization codes are used for unique identification for billing security purposes.

### **CAS Branch**

Enables or disables Centralized Attendant Service - Branch.

### **CAS Main**

Enables or disables multi-location customers served by separate switching vehicles to concentrate attendant positions at a single, main Avaya Communication Manager location. The main Avaya Communication Manager is served by an attendant queue that collects calls from all locations (main and branch). Each branch location switches all of its incoming calls to the centralized attendant positions over release link trunks (RLTs). The calls are then extended back to the requested extension at the branch server/switch over the same RLT. When the call is answered, the trunks to the main server are dropped and can be used for another call.

### **Change COR by FAC**

Provides certain users the ability to change the class of restriction of local extensions and local attendants via a telephone by using a feature access code (FAC).

### **Computer Telephony Adjunct Links**

Provides linkage between Avaya Communication Manager and adjuncts. Includes both the ASAI Link Core and ASAI Link Plus capabilities, plus the Phantom Calls and CTI Stations.

#### **Note:**

This field only applies to links administered as type adjlk.

### **Cvg Of Calls Redirected Off-net**

Provides continued monitoring for calls redirected to off-network (remote) coverage points. Uses call classification via call classifier circuit pack or ISDN trunk signaling.

### **DCS (Basic)**

Provides transparent operation of selected features across a Distributed Communications System (DCS). Users on one server running Communication Manager can use features

located on another server. Includes 4- and 5-digit uniform dialing and 1 to 4 digit steering. Does not support a 6/7-digit dial plan.

### ***DCS Call Coverage***

Provides DCS-based transparency of the call coverage feature across a DCS network of media servers or switches.

### ***DCS with Rerouting***

Provides for rerouting calls transferred among DCS nodes, enabling rerouting of the call for more effective use of facilities.

#### **Related topics:**

[Group Type](#) on page 860

[TSC Supplementary Service Protocol](#) on page 869

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

[Used for DCS](#) on page 1023

### ***Digital Loss Plan Modification***

Allows or disallows permission to customize the digital loss and digital tone plans.

### ***DS1 MSP***

Allows or disallows permission to administer values for the DS1 circuit pack without removing the related translations of all trunks from the trunk group.

### ***DS1 Echo Cancellation***

Removes perceivable echo from the system.

### **System parameters customer options: page 4**

#### ***Emergency Access to Attendant***

Provides for emergency calls to be placed to an attendant. These calls can be placed automatically by Avaya Communication Manager or dialed by users.

#### ***Enable 'dadmin' Login***

Provides business partners the ability to install, administer, and maintain Avaya servers and switches. The dadmin login has access to all the same commands as other logins with the exception of `Go` and `WP`. `Go` is used for `go tcm` and `go debug` as well as `go server`. `WP` is for writing memory.

#### ***Enhanced Conferencing***

Enables or disables the use of Meet-me Conference, Expanded Meet-me Conference , Selective Conference Party Display, Drop, Mute, and the No Hold Conference features.

#### ***Enhanced EC500***

Indicates if Extension to Cellular is enabled. EC500 refers to the Extension to Cellular feature.

#### ***Enterprise Survivable Server***

Identifies the server is an Enterprise Survivable Server (ESS).

**ESS Administration**

Indicates if administration of Enterprise Survivable Servers (ESS) is enabled.

**Extended Cvg/Fwd Admin**

Enables or disables Extended Coverage and Forwarding Administration.

**External Device Alarm Admin**

Provides for analog line ports to be used for external alarm interfaces. Allows identification of port location, adjunct associated with port location, and the alarm level to report.

**Enterprise Wide Licensing**

Enterprise Wide Licensing. See an Avaya representative for more information.

**Five Port Networks Max Per MCC**

Allows system administrator to create five port networks in a multi-carrier cabinet. Available only for duplex server Multi-Connect.

**Flexible Billing**

Provides an internationally accepted standard interface for end-to-end digital connectivity. Used with a T1 interface and supports twenty-three 64-KBPS voice or data B-Channels and one 64-Kbps signaling D Channel for total bandwidth of 1.544 Mbps.

**Forced Entry of Account Codes**

Allows system administration to force account users to enter account codes based on user or trunk class of restriction, or by an option on the Toll Analysis table. FEAC provides an easy method of allocating the costs of specific calls to the correct project, department, and so on.

**Global Call Classification**

Provides call classification outside of North America. Listens for tones and classifies tones detected. Required for Call Coverage Off Net and Outgoing Call Management.

**Hospitality (Basic)**

Provides access to basic features including: Attendant Crisis Alert, Attendant Room Status, Automatic Wakeup, Custom Selection of VIP DID Numbers, Do Not Disturb, Names Registration, Single-Digit Dialing, and Mixed Station Numbering.

**Hospitality (G3V3 Enhancements)**

Software required for Property Management System and Automatic Wakeup. Property Management System Interface activates Forward PMS Messages to INTUITY Lodging and PMS Protocol Mode (transmit in ASCII mode).

 **Note:**

Standard hospitality features are included in basic system software.

**IP Attendant Consoles**

Controls permission to administer the IP Attendant Console.

**IP Stations**

Controls permission to administer H.323 and/or SoftPhone stations. Must be enabled for IP telephones.

**IP Trunks**

Controls permission to administer H.323 trunks. Must be enabled for IP trunks.

**ISDN-BRI Trunks**

Provides the capability to add ISDN-BRI trunks to Communication Manager.

**Related topics:**

[Facility Type](#) on page 812

[Service/Feature](#) on page 849

[Group Type](#) on page 860

[TSC Supplementary Service Protocol](#) on page 869

[DCS with Rerouting](#) on page 945

[ISDN-PRI](#) on page 947

[ISDN-PRI](#) on page 947

[Used for DCS](#) on page 1023

**ISDN Feature Plus**

Provides ISDN Feature Plus signaling.

**ISDN-PRI**

Provides Integrated Services Digital Network (ISDN-PRI) software for either a switching-hardware platform migration only or a switching-hardware platform migration in combination with a software release upgrade. Also provides signaling support for H.323 signaling. Must be enabled for IP trunks.

**Related topics:**

[Facility Type](#) on page 812

[Service/Feature](#) on page 849

[Group Type](#) on page 860

[TSC Supplementary Service Protocol](#) on page 869

[DCS with Rerouting](#) on page 945

[ISDN-BRI Trunks](#) on page 947

[ISDN-BRI Trunks](#) on page 947

[Used for DCS](#) on page 1023

**ISDN/SIP Network Call Redirection**

Redirects an incoming ISDN/SIP call from a server running Avaya Communication Manager to another PSTN endpoint. It is used in call centers with Best Service Routing and Lookahead Interflow.

**Local Survivable Processor**

Indicates that the server is a Survivable Remote Server (Local Survivable Processor). The Survivable Remote Server is configured to provide standby call processing in case the primary media server is unavailable.

**Malicious Call Trace**

Provides the ability to retrieve certain information related to a malicious call.

**Mode Code for Centralized Voice Mail**

Provides the ability to share a Voice Mail System (VMS) among several servers/ switches using the Mode Code - Voice Mail System Interface.

**Multifrequency Signaling**

Provides for multi-frequency signaling between Communication Manager and the local telephone company central office.

**Multimedia Appl. Server Interface (MASI)**

Allows users of the Multimedia Communications Exchange (MMCX) to take advantage of certain Avaya Communication Manager telephony features.

**Multimedia Call Handling (Basic)**

Allows administration of desktop video-conferencing systems as data modules associated with Avaya Communication Manager voice stations in a multimedia complex. Users can dial one number to reach either endpoint (voice or data) in the complex. Also provides support for IP SoftPhones.

**Multimedia Call Handling (Enhanced)**

Allows a multifunction telephone to control a multimedia call like a standard voice call.

**Multimedia IP SIP Trunking**

Extends applicability of the H.323 video station licensing/control to all non-IP Softphones.

**System parameters customer options: page 5**

**Multinational Locations**

Provides the ability to use a single Enterprise Communication Server (ECS) with stations, port networks, remote offices, or gateways in multiple countries. Allows administration of location parameters such as companding, loss plans, and tone generation per location, instead of system-wide.

**Multiple Level Precedence and Preemption**

Multiple Level Precedence and Preemption (MLPP) provides users the ability to assign levels of importance to callers, and when activated, to give higher-priority routing to individual calls based on the level assigned to the caller.

**Multiple Locations**

Allows numbering plans and time zone and daylight savings plans that are specific for each cabinet in a port network.

**Personal Station Access (PSA)**

Provides basic telecommuting package capability for Personal Station Access.

**PNC Duplication**

Indicates whether or not Port Network Connectivity (PNC) Duplication can be enabled. This feature provides non-standard reliability levels (high, critical, or ATM PNC Network Duplication).

**Port Network Support**

| Valid Entry | Usage  |
|-------------|--|
| y           | The server is operating as a stand-alone Internal Communications Controller (ICC). |
| n           | Traditional Avaya port networks are in use.  |

**Posted Messages**

Supports the ability for users to post messages, selected from among a set of as many as 30 (15 fixed, 15 administrable), and shown on display telephones.

**Private Networking**

Indicates upgrading of PNA or ETN software RTU purchased with earlier systems.

**Processor and System MSP**

Allows for maintenance of the processor and system circuit packs.

**Processor Ethernet**

Indicates if the Ethernet card resident in the processor cabinet is used by the Communication Manager Call Processing software in place of a C-LAN card (located in a port network). Appears only on S8300D, S8510, and S8800 Media Servers. The Processor Ethernet interface is always enabled for duplex media servers.

**Remote Office**

Allows administration of a remote office.

**Restrict Call Forward Off Net**

Allows the system to monitor the disposition of an off-call and, if it detects busy, bring the call back for further processing, including call coverage.

**Secondary Data Module**

Provides the ability to use any data module as a secondary data module.

**Station and Trunk MSP**

Allows for maintenance of the station and trunk circuit packs.

**Station as Virtual Extension**

Allows multiple virtual extensions to be mapped to a single physical analog telephone. A specific ringing pattern can be administered for each virtual extension. Useful in environments such as college dormitories, where three occupants can have three different extensions for one physical telephone.

**System Management Data Transfer**

Indicates Communication Manager is accessible by network administration.

**Tenant Partitioning**

Provides for partitioning of attendant groups and/or stations and trunk groups. Typically this is used for multiple tenants in a building or multiple departments within a company or organization.

### ***Terminal Trans. Init. (TTI)***

Allows administrators of Terminal Translation Initialization (TTI) to merge an station administered with X in the **Port** field, to a valid port by dialing a system-wide TTI security code and the extension from a terminal connected to that port.

### ***Time of Day Routing***

Provides AAR and ARS routing of calls based on the time of day and day of the week to take advantage of lower calling rates during specific times.

#### **Related topics:**

[Time of Day Chart](#) on page 485

### ***TN2501 VAL Maximum Capacity***

Allows up to 60 minutes storage capacity per pack and multiple integrated announcement circuit packs. This is the Enhanced offer.

### ***Uniform Dialing Plan***

Enables or disables three- to seven-digit Uniform Dial Plan (UDP) and one- to seven-digit steering. Also allows use of Extended Trunk Access and Extension Number Portability features.

### ***Usage Allocation Enhancements***

Provides for assigning ISDN-PRI or ISDN-BRI Services/Features for Usage Allocation Plans.

### ***Wideband Switching***

Provides wideband data software for switching video or high-speed data. DSO channels can be aggregated up to the capacity of the span. Wideband supports H0, H11, and H12 standards, where applicable, as well as customer-defined data rates.

### ***Wireless***

Provides right to use for certain wireless applications.

### **System parameters customer options: page 6**

#### ***ACD***

Provides the software required for the Call Center Basic, Plus, Deluxe, and Elite features for the number of agents specified. Automatic Call Distribution (ACD) automatically distributes incoming calls to specified splits or skills.

#### ***BCMS (Basic)***

Provides real-time and historical reports about agent, ACD split, Vector Directory Number (VDN) and trunk group activity.

#### ***BCMS/VuStats Service Level***

Provides for hunt groups or Vector Directory Numbers (VDNs) with an acceptable service level. An acceptable service level defines the number of seconds within which a call must be answered to be considered acceptable.

**Business Advocate**

Enables or disables Avaya Business Advocate. Business Advocate establishes different levels of service for different types of calls. For example, a company may decide that a premium customer gets faster service than other types of customers.

**Call Center Release**

The call center release installed on the system.

**Call Work Codes**

Allows agents to enter digits for an ACD call to record customer-defined events such as account codes or social security numbers.

**DTMF Feedback Signals For VRU**

Provides support for the use of C and D Tones to voice response units (VRUs).

**Dynamic Advocate**

Enables or disables the Dynamic Advocate feature. While Business Advocate assigns reserve agents and sets overload thresholds to determine when those reserve agents get engaged, the Dynamic Advocate feature, also known as Dynamic Threshold Adjustment, takes this a step further. Dynamic Advocate automatically adjusts the thresholds as needed to help maintain defined service levels.

**EAS-PHD**

Increases the number of skills an agent can log in to from 4 to 20. Increases the number of agent skill preference levels from 2 to 16.

**Expert Agent Selection (EAS)**

Enables or disables skills-based routing of calls to the best-qualified agent.

**Forced ACD Calls**

See Multiple Call Handling.

**Least Occupied Agent**

Allows call center calls to be routed to the agent who has been the least busy, regardless of when the agent last answered a call.

**Lookahead Interflow (LAI)**

Provides Look-Ahead Interflow to balance the load of ACD calls across multiple locations.

**Multiple Call Handling (Forced)**

Forces an agent to be interrupted with an additional ACD call while active on an ACD call. Splits or skills can be one forced, one per skill, or many forced.

**Multiple Call Handling (On Request)**

Allows agents to request additional calls when active on a call.

**PASTE (Display PBX Data on Phone)**

Provides an interface between the display of a DCP telephone set and PC-based applications.

### **Reason Codes**

Allows agents to enter a numeric code that describes their reason for entering the AUX work state or for logging out of the system.

### **Service Level Maximizer**

Allows an administrator to define a service level whereby X% of calls are answered in Y seconds. When Service Level Maximizer (SLM) is active, the software verifies that inbound calls are matched with agents in a way that ensures that the administered service level is met.

### **Service Observing (Basic)**

Allows a specified user to observe an in-progress call on a listen-only or listen-and-talk basis.

### **Service Observing (Remote/By FAC)**

Allows users to service observe calls from a remote location or a local station using this feature's access codes.

### **Service Observing (VDNs)**

Provides the option of observing and/or monitoring another user's Vector Directory Number (VDN).

### **Timed ACW**

Places an auto-in agent in ACW for an administered length of time after completion of the currently active ACD call.

### **Vectoring (ANI/II-Digits Routing)**

Provides for ANI and II-Digits vector routing used to make vector routing decisions based on caller identity and the originating line.

### **Vectoring (Basic)**

Provides basic call vectoring capability.

#### **Related topics:**

[Basic](#) on page 466

### **Vectoring (Best Service Routing)**

Enables or disables the Best Service Routing feature. Through special vector commands, Best Service Routing allows the system to compare splits or skills at local and remote locations and queue a call to the resource that will give the caller the best service.

### **Vectoring (CINFO)**

Enables or disables the Caller Information Forwarding (CINFO) feature that allows the collection of caller-entered digits (ced) and customer database provided digits (cdpd) for a call from the network.

#### **Related topics:**

[CINFO](#) on page 466

### **Vectoring (G3V4 Advanced Routing)**

Provides for Rolling Average Speed of Answer Routing, Expected Wait Time Routing, and VDN Calls Routing.

**Vectoring (G3V4 Enhanced)**

Allows the use of enhanced comparators, wildcards in digit strings for matching on collected digits and ANI or II-digits, use of Vector Routing Tables, multiple audio/music sources for use with wait-time command and priority level with the oldest-call-wait conditional.

**Vectoring (Holidays)**

Indicates if the Holiday Vectoring feature is enabled or disabled that simplifies vector writing for holidays.

**Vectoring (Prompting)**

Allows flexible handling of incoming calls based on information collected from the calling party or from an ISDN-PRI message.

**System parameters customer options: page 7****Logged-In ACD Agents**

The total number of ACD agents that can be logged in simultaneously.

The limit applies to ACD agents on ACD and EAS calls. Auto-Available Split (AAS) agent ports are counted when they are assigned. AAS split or skill members are also counted. If the port for an AAS split/skill member is logged out, (for example, when a ringing call is redirected) the logged-in agent count is not updated. These counts are updated only during administration.

**Logged-In Advocate Agents**

The total number of Business Advocate Agents logged in simultaneously. The number of logged-in Business Advocate agents counts towards the total number of logged-in ACD agents.

**Logged-In IP Softphone Agents**

The total number of IP Softphone agents that can be logged-in simultaneously.

**VDN of Origin Announcement**

Provides a short voice message to an agent indicating the city of origin of the caller or the service requested by the caller based on the VDN used to process the call.

**VDN Return Destination**

Allows an incoming trunk call to be placed back in vector processing after all parties, except the originator, drop.

**VuStats**

Puts call center statistics on agents, splits or skills, Vector Directory Numbers (VDNs), and trunk groups on telephone displays.

**VuStats (G3V4 Enhanced)**

Provides G3V4 VuStats enhancements including historical data and thresholds.

**System parameters customer options: page 8 (ASAI FEATURES)****Agent States**

Provides proprietary information used by Avaya applications. For more information, contact an Avaya technical support representative.



**Note:**

This field applies only to links administered as type adjlk.

***CTI Stations***

Enables or disables any application using a link of Type ASAI that uses a CTI station to receive calls.

***Phantom Calls***

Indicates if phantom calls are enabled. This field only applies to links administered as type ASAI.

**System parameters customer options: page 8 (QSIG OPTIONAL FEATURES)**

***Basic Call Setup***

Provides basic QSIG services: basic connectivity and calling line ID number. Either ISDN-PRI or ISDN-BRI Trunks must be enabled for the system.

**Related topics:**

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

***Basic Supplementary Services***

Provides the following QSIG Supplementary Services:

- Name ID
- Transit Capabilities; that is, the ability to tandem QSIG information elements
- Support of Notification Information Elements for interworking between QSIG and non-QSIG tandemed connections
- Call Forwarding (Diversion) by forward switching. No reroute capabilities are provided
- Call Transfer by join. No path replacement capabilities are provided.
- Call Completion (also known as Automatic Callback)

Either ISDN-PRI or ISDN-BRI Trunks must be enabled for the system.

**Related topics:**

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

***Centralized Attendant***

Allows all attendants in one location to serve users in multi locations. All signaling is done over QSIG ISDN lines.

**Interworking with DCS**

Allows the following features to work between a user on a DCS-enabled media server or switch in a network and a QSIG-enabled media server or switch:

- Calling/Called/Busy/Connected Name
- Voice Mail/Message Waiting
- Leave Word Calling

**Supplementary Services with Rerouting**

Provides the following QSIG Supplementary Services:

- Transit Capabilities; that is, the ability to tandem QSIG information elements.
- Support of Notification Information Elements for interworking between QSIG and non-QSIG tandemed connections.
- Call Forwarding (Diversion) by forward switching. In addition, reroute capabilities are provided.
- Call Transfer by join. In addition, path replacement capabilities are provided.

**Transfer Into QSIG Voice Mail**

Allows transfer directly into the voice-mail box on the voice-mail system when a QSIG link connects Avaya Communication Manager and the voice-mail system.

**Value Added (VALU)**

Provides additional QSIG functionality, including the ability to send and display calling party information during call alerting.

**System parameters customer options: page 9 (MAXIMUM IP REGISTRATIONS BY PRODUCT ID) Limit**

| Valid Entry  | Usage  |
|--------------|--|
| 1000<br>5000 | Maximum number of IP registrations allowed, depending on server configuration. |

**Product ID**

Identifies the product using the IP (internet protocol) registration.

These are just a few examples of valid Product IDs. The valid Product IDs for a system are controlled by the license file.

| Product ID example | Description                  |
|--------------------|------------------------------|
| Avaya_IR           | Interactive Response product |
| IP_Agent           | IP Agents                    |
| IP_eCons           | SoftConsole IP attendant     |
| IP_Phone           | IP Telephones                |

| Product ID example | Description              |
|--------------------|--------------------------|
| IP_ROMax<br>R300   | Remote Office telephones |
| IP_Soft            | IP Softphones            |

**Rel**

| Valid Entry      | Usage                              |
|------------------|------------------------------------|
| 0 to 99<br>blank | Release number of the IP endpoint. |

## System parameters - Duplication

Use the System Parameters Duplication screen to enable PNC or IPSI duplication.

Example command: `change system-parameters duplication`

### Enable Operation of IPSI Duplication

Enables or disables IPSI duplication.

### Enable Operation of PNC Duplication

Enables or disables PNC duplication. Available only if PNC Duplication is enabled for the system.

#### Related topics:

[PNC Duplication](#) on page 948

## System parameters maintenance

This screen is described in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431.

## System Parameters Media Gateway Automatic Recovery Rule

This screen defines rules for returning a fragmented network, where a number of H.248 Media Gateways are being serviced by one or more Survivable Remote Server (Local Survivable Processors) automatically to the primary media server. The system displays a different warning message or time window grid depending on the option selected for the **Migrate H.248 MG to primary** field.

In the time window grid, an x or X can be specified for each hour. Leave blank to disable. This method helps with overlapping time issues between days of the week. There is no limit on intervals.

For more information on Auto Fallback for H.248 Gateways, see *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

Example command: `change system-parameters mg-recovery-rule n`, where *n* is the assigned recovery rule number.

### Migrate H.248 MG to primary

Indicates auto-fallback preferences.

| Valid Entry                   | Usage  |
|-------------------------------|--|
| immediately                   | The first media gateway registration that comes from the media gateway is honored, regardless of call count or time of day. This is the default.   |
| 0-active calls                | The first media gateway registration reporting 0 active calls is honored.  |
| time-day-window               | A valid registration message received during any part of this interval is honored. When this option is selected the system displays a grid for defining desired hours or days for the time window.   |
| time-window-OR-0-active-calls | A valid registration is accepted anytime, when a 0 active call count is reported or if a valid registration with any call count is received during the specified time/day intervals. When this option is selected the system displays a grid for defining desired hours or days for the time window. |

### Minimum time of network stability

| Valid Entry | Usage  |
|-------------|--|
| 3 to 15     | Administers the time interval for stability in the H.248 link before auto-fallback is attempted. Default is 3. |

### Recovery Rule Number

The number of the recovery rule up to the server maximum.

### Rule Name

The name for the recovery rule in alpha-numeric characters. The recovery rule is an aid for associating rules with media gateways.

## System parameters OCM call classification

Administers the country tone characteristics for Outbound Call Management (OCM) applications. It is not required for United States OCM applications. This screen defines the busy tone and cadence and can be administered with up to four on and off steps, which is four valid cycles to determine busy tone.

Use a minimum of two on and off steps to determine a valid busy tone. If the cadence is administered with one on and off step, any time the classifier hears the cadence it is considered BTD signal.

Available only if **Global Call Classification** is enabled for the system, or when **Enable Busy Tone Disconnect for Analog loop-start Trunks** is enabled for the system.

Example command: `change system-parameters ocm-call-classification`

**Related topics:**

[Enable Busy Tone Disconnect for Analog Loop-start Trunks](#) on page 938

[Global Call Classification](#) on page 946

**System parameters OCM call classification: page 1**

***Cadence Classification After Answer***

| Valid Entry | Usage   |
|-------------|---|
| y           | Old classifier detects live voice with or without AMD. These modes detect call progress tone cadence. If you upgrade the Communication Manager software, by default the classifier uses the old modes. If you do a new installation of the Communication Manager software, by default the classifier uses the no-cadence call classification modes. |
| n           | No-cadence call classification modes detect live voice with or without AMD whenever Communication Manager receives a connect or answer supervision message from an outbound trunk. These modes do not detect any call progress tone cadence.  |

***Global Classifier Adjustment (dB)***

| Valid Entry | Usage   |
|-------------|---|
| 0 to 15     | Specifies the dB loss adjustment. where 0 is the least adjustment, and 15 is the most adjustment. |

***USA Default Algorithm***

Enables or disables the use of the default United States tone detection.

***USA SIT Algorithm***

| Valid Entry | Usage   |
|-------------|---|
| y           | Uses the United States (SIT) tone characteristics for SIT tone detection.   |
| n           | The system treats tones with the administered tone name intercept as if they were SIT VACANT, and treats tones with the administered tone name information as if they were SIT UNKNOWN. |

**System parameters OCM call classification: page 2**

***Cadence Step***

Identifies the number of each tone cadence step and indicates whether the tone is on or off during this cadence step.

***Duration Maximum***

| Valid Entry | Usage   |
|-------------|---|
| 75 to 6375  | The upper limit in milliseconds of the tone duration in increments of 25. |

**Duration Minimum**

| Valid Entry | Usage  |
|-------------|--|
| 75 to 6375  | The lower limit in milliseconds (msec) of the tone duration in increments of 25. |

**Instance**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 8      | The number distinguishes tones that have the same name but more than one definition of silence and tone-on characteristics. |

**Tone Continuous**

| Valid Entry | Usage                            |
|-------------|----------------------------------|
| y           | Indicates a continuous tone.     |
| n           | Indicates a non-continuous tone. |

**Tone Name**

| Valid Entry   | Usage   |
|---|---|
| busy<br>information<br>intercept<br>reorder<br>ringback | The name of the tone. Busy is required when <b>Busy Tone Disconnect for Analog Loop-start Trunks</b> is enabled or <b>Global Call Classification</b> is disabled for the system. Required for tone definition outside of the U.S. and Canada. |

**Related topics:**

[Enable Busy Tone Disconnect for Analog Loop-start Trunks](#) on page 938

[Global Call Classification](#) on page 946

**System Parameters Port Networks**

These screens assign port networks to communities and specify recovery rules for port networks to return to the main server.

Example command: `change system-parameters port-networks`

**System parameters port networks: page 1****Community**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 64     | The Network Community number associated with this port network. |

| Valid Entry | Usage   |
|-------------|---|
|             |  <b>Note:</b><br>If the port network is administered in the system, the default community is 1 and administrable with a value between 1 and 64. If the port network is not administered in the system, the community value is 1 and not administrable. |

**PN**

| Valid Entry | Usage                      |
|-------------|----------------------------|
| 1 to 64     | Displays the port network. |

**System parameters port networks: page 2**

**Auto Return**

The Auto Return functionality is used to schedule a day and time for all port networks to return to the control of the main server after a failover occurs. The schedule can be set up to seven days prior the its activation.

| Valid Entry  | Usage   |
|--------------|---|
| y            | Enables the Auto Return feature. The port networks can automatically return to the main server after the value set in the <b>IPSI Connection up time</b> expires.       |
| n            | Disables the Auto Return feature. The port networks cannot automatically return to the control of the main server.  |
| s(scheduled) | Enables the Auto Return feature. A day and time also needs to be administered to schedule a day and time to return the port networks to the control of the main server. |

**Day**

| Valid Entry           | Usage  |
|-----------------------|--|
| Monday through Sunday | The day of the week the port networks return to the control of the main server if Auto Return is administered on a schedule. |

**IPSI Connection up time**

| Valid Entry | Usage  |
|-------------|--|
| 3 to 120    | The number of minutes that the IP Server Interface (IPSI) waits to return to the main server after communication with the main server is restored. |

**No Service Time Out Interval**

| Valid Entry | Usage  |
|-------------|--|
| 3 to 15     | The time in minutes that the IP Server Interfaces (IPSIs) wait before requesting service from the highest Enterprise Survivable Server (ESS) on its priority list. Default is 5 minutes. |

**PN Cold Reset Delay Timer (sec)**

| Valid Entry | Usage  |
|-------------|--|
| 60 to 120   | Time in seconds before a PN cold reset occurs. This value is retained after an upgrade event. Default is 60 seconds. |

**Time**

| Valid Entry    | Usage   |
|----------------|---|
| 00:00 to 23:59 | The time of day the port networks return to the control of the main server if Auto Return is administered on a schedule. This field uses a 24-hour military format. |

**System Parameters - SCCAN**

Example command: `change system-parameters sccan`

**Announcement**

The extension of the announcement played during call hand-in or handout.

**H1 Handover**

The primary handover extension called to facilitate handover of a cellular call to the WAN or WLAN. Depending on whether the user is entering or exiting the Enterprise space, Communication Manager replaces the active call with the new call made using the hand-off H1 or H2 number.

**H2 Handover**

A secondary handover extension used when no acknowledgement is received from the H1 Handover number.

**MM (WSM) Route Pattern**

A route pattern number that is SCCAN-enabled. Partition route pattern indexes, RHNPA indexes, deny, or nodes are not allowed. If this field is left blank, the feature is turned off. Blank is the default.

## Special Digit Conversion

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows a user to call a cellular telephone number and get the same treatment as calling an extension that is running Communication Manager. ARS checks the dialed string to determine if the dialed string is a SCCAN telephone number. If the number is a SCCAN telephone number, the cellular telephone number is replaced with the extension number that the cellular telephone is mapped to. |
| n           | The feature is turned off. This is the default.  |

## Telecommuting Access

Administers the extension which allows remote users to use the Telecommuting Access feature.

Example command: `change telecommuting-access`

### Telecommuting Access Extension

An extension that allows only remote access to the Telecommuting Access feature. This extension must consist of one to 13 digits that conforms to the system dial plan and is not assigned to any other system object.

## Tenant

This screen defines tenants to the system. If your server running Communication Manager uses tenant partitioning, see *Tenant Partitioning in Avaya Aura™ Communication Manager Feature Description and Implementation, 555-245-205*.

Example command: `change tenant n`, where *n* is the tenant partitioning number.

### Tenant: page 1

#### Attendant Group

| Valid Entry | Usage                                       |
|-------------|---|
| 1 to 128    | The attendant group assigned to the tenant. |

#### Attendant Vectoring VDN

Assigns the VDN extension for Attendant Vectoring to a console. Available only if Attendant Vectoring is enabled for the system and Tenant Partitioning is disabled.

#### Related topics:

[Attendant Vectoring](#) on page 944

[Tenant Partitioning](#) on page 949

**COS Group**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 100    | The Class of Service (COS) group assigned to the tenant. Available only if Tenant Partitioning is enabled for the system. |

**Related topics:**

[Tenant Partitioning](#) on page 949

**Ext Alert Port (TAAS)**

The Trunk Answer Any Station (TAAS) alert port assigned to this tenant, if any. The port type and the object type must be consistent. The port can be assigned to only one tenant.

| Valid Entry                                 | Usage  |
|---|--|
| <i>A valid port address</i> or X<br>1 to 64 | First and second characters are the cabinet number |
| A to E                                      | Third character is the carrier                     |
| 0 to 20                                     | Fourth and fifth character are the slot number     |
| 01 to 04 (Analog TIE trunks)<br>01 to 31    | Six and seventh characters are the circuit number  |
| 1 to 250                                    | Gateway  |

**Ext Alert (TAAS) Extension**

The extension of the external alert TAAS extension. A system installer can then use the Terminal Translation Initialization (TTI) feature from a telephone plugged into any port to assign this extension number to that port. Doing so makes that port the external alert TAAS port.

Available only if **Ext Alert Port (TAAS)** is administered without hardware.

**Related topics:**

[Ext Alert Port \(TAAS\)](#) on page 963

**Music Source**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 20     | The music or tone source for this tenant partition. |

**Night Destination**

The night service station extension, if night service is wanted for this tenant.

**Tenant**

Displays the tenant number.

**Tenant Description**

A description of the tenant that consists of up to 40 alpha-numeric characters.

***DISTINCTIVE AUDIBLE ALERTING***

**Attendant Originated Calls**

Indicates which type of ringing applies to attendant-originated calls.

Available only if Tenant Partitioning is *not* enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| internal    | Internal ringing applies to attendant-originated calls.                      |
| external    | External ringing applies to attendant-originated calls. Default is external. |
| priority    | Priority ringing applies to attendant-originated calls.                      |

**Related topics:**

[Tenant Partitioning](#) on page 949

**Distinctive Audible Alerting (Internal, External, Priority)**

The number of rings for Internal, External, and Priority calls. For virtual stations, this applies to the mapped-to physical telephone. This is also known as Distinctive Ringing. Defaults are as follows:

1. Internal calls
2. External and attendant calls
3. Priority calls



**Note:**

SIP Enablement Services (SES) messaging includes the ring types internal, external, intercom, auto-callback, hold recall, transfer recall, or priority. In Communication Manager, types intercom, auto-callback, hold recall, and transfer recall are treated as priority.

| Valid Entry | Usage   |
|-------------|---|
| 1           | 1 burst, meaning one burst of ringing signal per period   |
| 2           | 2 bursts, meaning two bursts of ringing signal per period |
| 3           | 3 bursts, meaning two bursts of ringing signal per period |

**Tenant: page 2**

This screen is used to enable additional tenant-to-tenant calling permissions.

***Calling permissions***

Establishes or blocks calling permission between the tenant being administered and any other tenant. The system default allows each tenant to call only itself and Tenant 1.

***Tenant***

Displays the tenant number.

## Terminal Parameters

Administers system-level parameters and audio levels for the 603 CALLMASTER telephones and the 4600-series, 6400-series, 8403, 8405B, 8405B+, 8405D, 8405D+, 8410B, 8410D, 8411B, 8411D, 8434D, and 2420/2410 telephones. Only authorized Avaya personnel can administer this screen.

 **Note:**

With the Multinational Locations feature enabled, terminal parameters can be administered per location, rather than system-wide.

Example command: `change terminal-parameters`

### Base Parameter Set

Determines which default set of telephone options and levels will be used. This field corresponds to the country codes.

#### Related topics:

[Country options table](#) on page 935

### Customize Parameters

Allows or disallows permission for the administrator to change one or more of the default parameters.

### ADJUNCT LEVELS

#### *Touch Tone Sidetone (dB)*

Determines the touchtone volume fed back from the telephone when a user presses a button.

#### *Voice Receive (dB)*

Determines the volume of voice inbound to the adjunct.

#### *Voice Sidetone (dB)*

Determines the volume of voice fed back from the handset voice microphone to the user's ear.

#### *Voice Transmit (dB)*

Determines the volume of voice outbound from the adjunct.

### OPTIONS

#### *Display Mode*

Determines how the # and ~ characters appear on the telephone's display.

| Valid Entry | Usage  |
|-------------|--|
| 1           | The # and ~ do not change.   |
| 2           | The telephone displays a # as a British pound sterling symbol and a ~ as a straight overbar. |

**DLI Voltage Level**

Determines whether DCP Line Voltage used by the telephones is forced high, forced low, or allowed to automatically adjust.

**Handset Expander Enabled**

Determines whether or not the telephone reduces background noise on the handset.

**Volume for DCP Types**

Determines what volume adjustments are retained. Allows the DCP telephone volume to be adjusted while the call is in-progress.

| Valid Entry                              | Usage  |
|--|--|
| default speaker, handset unchangeable    | The speaker resets to the default settings while the adjusted handset setting is retained. |
| default settings used to begin each call | No adjusted handset and speaker settings are retained.                                     |
| retain handset and speaker between calls | The adjusted handset and speaker settings are retained                                     |
| retain speaker, handset unchangeable     | Only the adjusted speaker setting is retained.   |

**Volume for IP Types**

Determines what volume adjustments are retained. Allows the IP telephone volume to be adjusted while the call is in progress.



**Note:**

Avaya recommends that values for PRIMARY LEVELS or BUILT-IN SPEAKER LEVELS are not changed.

| Valid Entry                              | Usage  |
|--|--|
| default speaker, handset unchangeable    | The speaker resets to the default settings while the adjusted handset setting is retained. |
| default settings used to begin each call | No adjusted handset and speaker settings are retained                                      |
| retain handset and speaker between calls | The adjusted handset and speaker settings are retained                                     |

| Valid Entry                                | Usage   |
|--|---|
| retain speaker,<br>handset<br>unchangeable | Only the adjusted speaker setting is retained |

**Touch Tone Transmit (dB)**

Determines the touchtone volume fed outbound from the telephone.

**Voice Receive (dB)**

Determines the volume of voice inbound to the adjunct.

**Voice Transmit (dB)**

Determines the volume of voice outbound from the adjunct.

**PRIMARY LEVELS**

The system displays the default setting from the Base Parameter Set for all fields. Also, these fields all require the same input; valid entries are from -44.0 db through +14.0 db in 0.5 increments. For example, -44.0, -43.5, -43.0 and so on.

**Touch Tone Sidetone (dB)**

Determines the touchtone volume fed back from the telephone when a user presses a button.

**Touch Tone Transmit (dB)**

Determines the touchtone volume fed outbound from the telephone.

**Voice Receive (dB)**

Determines the volume of voice inbound to the adjunct.

**Voice Sidetone (dB)**

Determines the volume of voice fed back from the handset voice microphone to the user's ear.

**Voice Transmit (dB)**

Determines the volume of voice outbound from the adjunct.

**Terminating Extension Group**

Defines a Terminating Extension Group (TEG). Any telephone can be assigned as a TEG member; however, only a multi-appearance telephone can be assigned a TEG button with associated status lamp. The TEG button allows the telephone user to select a TEG call appearance for answering or for bridging onto an existing call.

The TEG members are assigned on an extension number basis. Call reception restrictions applicable to the group are specified by the group class of restriction (COR). The group COR takes precedence over an individual member's COR. The members could all be termination restricted but still receive calls if the group is not restricted.

An extension number can be assigned to more than one TEG but can have only one appearance of each group.

Example command: `change term-ext-group n`, where *n* is the assigned group number.

**AUDIX Name**

The name of the AUDIX machine. Must be the same name as the IP Node name and administered *after* the IP Node is configured.

**Related topics:**

[IP Node Names](#) on page 700

**COR**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 995    | The class of restriction (COR) number that reflects the desired restrictions. |

**Coverage Path**

The call coverage path number for this group. A TEG cannot serve as a coverage point; however, calls to a TEG can redirect to coverage.

| Valid Entry | Usage             |
|-------------|-------------------|
| 1 to 9999   | Path number       |
| t1 to t999  | Time of day table |
| blank       | Not administered  |

**Group Extension**

The extension of the terminating extension group. The extension can consist of one to seven digits and cannot be a Vector Directory Number (VDN). This field cannot be left blank.

**Group Name**

The name used to identify the terminating extension group.

**Group Number**

Displays the terminating extension group number.

**ISDN Caller Disp**

Specifies whether the TEG group name or member name (member of TEG where call terminated) is sent to the originating user. Required if **ISDN-PRI** or **ISDN-BRI Trunks** are enabled for the system.

| Valid Entry | Usage                   |
|-------------|-------------------------|
| grp-name    | TEG group name is sent. |
| mbr-name    | Member name is sent.    |
| blank       | Not administered.       |

**Related topics:**

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

**LWC Reception**

Indicates where Leave Word Calling (LWC) messages are stored.

| Valid Entry | Usage   |
|-------------|---|
| audix       | LWC messages are stored on the voice messaging system.                          |
| none        | LWC messages are not be stored.   |
| spe         | LWC messages are stored in the system or on the switch processor element (spe). |

**Related topics:**

[AUDIX Name](#) on page 662

**Security Code**

The four-digit security code (password) for the Demand Print messages feature.

**TN**

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

**GROUP MEMBER ASSIGNMENTS*****Ext***

The extension number of one to seven digits assigned to a group number. The extension cannot be a Vector Directory Number (VDN).

***Name***

Displays the name assigned to the group number.

**TFTP Server**

The Trivial File Transfer Protocol screen allows specification of the TFTP server that Avaya Communication Manager uses to get download files.

Example command: `change tftp-server`

**Filename in Memory**

Displays the name of the file currently in Communication Manager memory.

**File Size**

Displays the number of bytes transferred.

**File Status**

Displays the download status as Download In Progress, Download Failed, File Not Found, or Download Completed.

**File to Retrieve**

The name of the file to retrieve using up to 32 alphanumeric, case sensitive, characters for identification.

**Local Node Name**

A previously-administered local node name. The node must be assigned to a CLAN IP interface or procr (processor CLAN).

| Valid Entry | Usage                                  |
|-------------|--|
| 1 to 15     | The node name.                         |
| procr       | Processor CLAN for S8300/S87XX Servers |

**Related topics:**

[Name](#) on page 700

**TFTP Server Node Name**

A previously-administered TFTP server node name from 1 to 15 characters.

**Related topics:**

[Name](#) on page 700

**TFTP Server Port**

| Valid Entry | Usage                               |
|-------------|-------------------------------------|
| 1 to 64500  | The number for the remote TCP port. |

**Time of Day Coverage Table**

This screen allows administration of up to five different coverage paths, associated with five different time ranges, for each day of the week. Only one coverage path can be in effect at any one time.

Example command: `change coverage time-of-day n`, where *n* is the assigned time of day coverage table.

**Act Time**

| Valid Entry  | Usage  |
|--------------|--|
| 00:01– 23:59 | Specifies the activation time of the associated coverage path. Information must be entered in 24-hour time format.<br>If there are time gaps in the table, there will be no coverage path in effect during those periods. The first activation time for a day is set to 00:00 and cannot be changed. Activation times for a day must be in ascending order from left to right. |

## CVG Path

| Valid Entry        | Usage                     |
|--------------------|---------------------------|
| 1 to 9999<br>blank | The coverage path number. |

## Time of Day Coverage Table

Displays the Time of Day Coverage Table number.

## Time of Day Routing Plan

This screen is used to set up Time of Day Routing Plans.

- AAR and ARS calls can be routed based on the time of day each call is made.
- Up to eight Time of Day Routing Plans can be designed, each scheduled to change up to six times a day for each day in the week.
- The Time of Day Routing Plan PGN# is matched with the **PGN#** field on the Partition Routing Table for the correct route pattern.

Available only if **Automatic Route Selection (ARS)** or **Private Networking, AAR/ARS Partitioning**, and **Time of Day Routing** are enabled for the system.

Example command: `change time-of-day n`, where *n* is the time of day routing plans.

### Related topics:

[PGN 1 \(through PGN 8\)](#) on page 816

[ARS](#) on page 942

[Private Networking](#) on page 949

[Time of Day Routing](#) on page 950

## Act Time

| Valid Entry    | Usage   |
|----------------|---|
| 00:00 to 23:59 | Specifies the time of day the route pattern, identified by PGN#, begins. Time is represented using a 24 hour clock. List times for the same day in increasing order. There must be at least one entry for each day. |

## PGN #

The route pattern for the activation time listed. The PGN must match a previously-administered PGN and route pattern on the Partition Routing Table. There must be at least one entry for each day.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 8      | The route pattern range when SA9050 is not active. |
| 1 to 32     | The route pattern range when SA9050 is active.     |

### Time of Day Routing Plan

Displays the Time of Day Routing Plan number.

### Time of Day Station Lock Table

This screen administers the ability to lock stations automatically by a time of day schedule.

Example command: `change tod-station-lock n`, where *n* is the assigned time of day station lock table number.

#### Begin Time

| Valid Entry    | Usage  |
|----------------|--|
| 00:00 to 23:59 | When the time of day station lock interval begins for each day of the week. Time is represented using a 24-hour clock. |

#### End Time

| Valid Entry    | Usage  |
|----------------|--|
| 00:00 to 23:59 | When the time of day station lock interval ends for each day of the week. Time is represented using a 24-hour clock. |

#### INTERVAL 1, 2, 3

Three separate time of day station lock intervals can be administered. The system imposes validation of overlapping intervals or invalid blank entries.

#### Manual Unlock allowed

Indicates whether or not the user can manually unlock the TOD-locked station using either a **sta-lock** button or a Feature Access Code followed by an SSC.

#### Table Active

Activates or deactivates time of day lock for all stations associated with this table.

### Toll Analysis

This screen associates dialed strings to the system's Restricted Call List (RCL), Unrestricted Call List (UCL), and Toll List. Users can be forced to dial an account code if you associate dialed strings with CDR Forced Entry of Account Codes.

To maximize system security, Avaya recommends that toll calling areas be restricted as much as possible through the use of the **RCL** (Restricted Call List) and **Toll List** fields on this screen.

 **Note:**

The Toll List field on this screen does not interact with or relate to the ARS Toll Table.

Example command: `change toll n`, where *n* is the dialed digits.

**CDR FEAC**

| Valid Entry | Usage  |
|-------------|--|
| x           | Requires an account code from a call whose facility COR requires a Forced Entry of Account Code. |

**Dialed String**

Dialed numbers are matched to the dialed string entry that most closely matches the dialed number. For example, if 297-1234 is dialed and the table has dialed string entries of 297-1 and 297-123, the match is on the 297-123 entry.

An exact match is made on a user-dialed number and dialed string entries with wildcard characters and an equal number of digits. For example, if 424 is dialed, and there is a 424 entry and an X24 entry, the match is on the 424 entry.

Accepts up to 18 digits that the call-processing server analyzes. Also accepts x and X wildcard characters.

**Location**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 250    | (Depending on your server configuration, see <i>Avaya Aura™ Communication Manager System Capacities Table</i> , 03-300511.) The location of the endpoint that is dialing the digits. Available only if <b>ARS</b> and <b>Multiple Locations</b> are enabled for the system. See the Location sections in <i>Avaya Aura™ Communication Manager Feature Description and Implementation</i> , 555-245-205, for the other ways, and for a list of features that use location. |
| all         | Indicates that this Toll Analysis Table is the default for all locations.   |

**Related topics:**

[ARS](#) on page 942

[Multiple Locations](#) on page 948

**Max**

The maximum number of user-dialed digits the system collects to match to the dialed string.

**Min**

The minimum number of user-dialed digits the system collects to match to the dialed string.

**Percent Full**

| Value    | Comments  |
|----------|---|
| 0 to 100 | The percentage of system memory resources that have been used by the table. |

**RCL**

| Valid Entry | Usage  |
|-------------|--|
| x           | Assigns the Dialed String to the Restricted Call List (RCL). All entries marked with x and their associated dialed strings are referred to as the System's Restricted Call List. The RCL can be assigned to any COR. |

**Toll List**

| Valid Entry | Usage                                       |
|-------------|---|
| x           | Assigns the Dialed String to the Toll List. |

| Dialed String | Minimum | Maximum | Toll List |
|---------------|---------|---------|-----------|
| 0             | 1       | 23      | X         |
| 1             | 4       | 23      | X         |
| 20            | 10      | 10      | X         |
| 21            | 10      | 10      | X         |
| 30            | 10      | 10      | X         |
| 31            | 10      | 10      | X         |
| 40            | 10      | 10      | X         |
| 41            | 10      | 10      | X         |
| 50            | 10      | 10      | X         |
| 51            | 10      | 10      | X         |
| 60            | 10      | 10      | X         |
| 70            | 10      | 10      | X         |
| 71            | 10      | 10      | X         |
| 80            | 10      | 10      | X         |
| 81            | 10      | 10      | X         |
| 90            | 10      | 10      | X         |
| 91            | 10      | 10      | X         |

**Unrestricted Call List**

| Valid Entry | Usage   |
|-------------|---|
| x           | Assigns the dialed string to one of the system's Unrestricted Call Lists (UCL). |

## Tone Generation

This screen administers the tone characteristics that parties on a call hear under various circumstances.

 **Note:**

With the Multinational Locations feature enabled, tone generation can be administered per location, rather than system-wide.

Example command: `change tone-generation`

### Tone Generation: page 1 440Hz PBX-dial Tone

| Valid Entry | Usage  |
|-------------|--|
| y           | The switch primary dial tone is changed to a continuous 440Hz-17 tone. |
| n           | A customized tone defaults to the <b>Base Tone Generation Set</b> .    |

**Related topics:**

[Base Tone Generator Set](#) on page 975

### 440Hz Secondary-dial Tone

| Valid Entry | Usage  |
|-------------|--|
| y           | The secondary local telephone company central office dial tone is changed to a continuous 440Hz-17 tone. |
| n           | A customized tone defaults to the <b>Base Tone Generation Set</b> .                                      |

**Related topics:**

[Base Tone Generator Set](#) on page 975

### Base Tone Generator Set

| Valid Entry | Usage   |
|-------------|---|
| 1 to 25     | The country code that identifies the base tone generation set to be used. |

**Related topics:**

[Country options table](#) on page 935

### Tone generation: page 2 (TONE GENERATION CUSTOMIZED TONES page) Cadence Step

Displays the number of each tone cadence step.

**Duration (msec)**

| Valid Entry | Usage   |
|-------------|---|
| 50 to 12750 | The duration of this step in the tone sequence. Values are in increments of 50. |

**Step**

The number of the cadence step for this `goto` command.

**Tone (Frequency/Level)**

Available only if **Tone/Frequency Level** is a `goto` command.

| Valid Entry   | Usage   |
|---|---|
| silence   | No tone. A final step of silence with an infinite duration will be added internally to any tone sequence that does not end in a <code>goto</code> . |
| goto  | Repeats all or part of the sequence, beginning at the specified cadence step.   |
| 350/-17.25<br>350+425/-4.0<br>350+440/-13.75<br>375+425/-15.0<br>404/-11.0<br>404/-16.0<br>404+425/-11.0<br>404+450/-11.0<br>425/-4.0<br>425/-11.0<br>425/-17.25<br>440/-17.25<br>440+480/-19.0<br>450/-10<br>480/-17.25<br>480+620/-24.0<br>525/-11.0<br>620/-17.25<br>697/-8.5<br>770/-8.5<br>852/-8.5<br>941/-8.5<br>1000/0.0<br>1000/+3.0<br>1004/0.0<br>1004/-16.0<br>1209/-7.5<br>1336/-7.5<br>1400/-11.0<br>1477/-7.5<br>1633/-7.5 | Specifies the frequency and level of the tone.  |

| Valid Entry  | Usage |
|--|-------|
| 2025/-12.1<br>2100/-12.1<br>2225/-12.1<br>2804/-16.0 |       |

### Tone Name

| Valid Entry   | Usage  |
|---|--|
| 1-call-wait<br>2-call-wait<br>3-call-wait<br>busy<br>busy-verify<br>call-wait-<br>ringback<br>conference<br>confirmation<br>disable-dial<br>hold<br>hold-recall<br>immed-ringback<br>intercept<br>intrusion<br>mnr/rec-<br>warning<br>PBX-dial<br>recall-dial<br>recall-dont-ans<br>redirect<br>reorder<br>rep-confirmation<br>reset-shift<br>ringback<br>secondary-dial<br>special-dial<br>whisper-page<br>zip | Indicates which of the individually administrable tones is modified. |

## Trunk Group

### Trunk Group

Sets basic characteristics for every type of trunk group and assigns ports to the group. Many fields are dependent on the settings of other fields and only appear when certain values are entered in other fields on the screen. For example, the entry in **Group Type** might significantly change the content and appearance of the Trunk Group screen.



**Note:**

For descriptions of the screens and fields that are unique to ISDN trunks, see *ISDN Trunk Group*.

Example command: `add trunk-group n`, where *n* is the trunk group number.

**Trunk Group: page 1**

**Analog Gain**

Reduces the strength of incoming signals on TN2199 ports if users regularly experience echo, distortion, or unpleasantly loud volume.

Available only if the country code is 15 and the **Trunk Type (in/out)** value is 2-wire-ac, 2-wire-dc, or 3-wire.

| Valid Entry | Usage  |
|-------------|--|
| a           | Reduces the incoming signal by -3dB.   |
| b           | Reduces the incoming signal by -6dB.   |
| c           | Reduces the incoming signal by -8dB.   |
| none        | No reduction. This setting should not be changed unless the trunk group sound quality is unacceptable. |

**Related topics:**

[Country](#) on page 822

[Trunk Type \(in/out\)](#) on page 991

**Auth Code**

If enabled, users are required to tandem a call through an AAR or ARS route pattern. The code will be required even if the facility restriction level of the incoming trunk group is normally sufficient to send the call out over the route pattern. This field affects the level of security for tandemed outgoing calls.

Available only for incoming or two-way trunk groups and if **Authorization Codes** are enabled for the system.

**Related topics:**

[Direction](#) on page 724

[Authorization Codes](#) on page 944

**BCC**

Generalized Route Selection uses the Bearer Capability Class (BCC) to select the appropriate facilities for routing voice and data calls. Far-end tandem servers/switches use the BCC to select outgoing routing facilities with equivalent BCC classes. The **BCC** entry is used to select the appropriate facilities for incoming ISDN calls. Communication Manager compares the **BCC** entry to the value of the Bearer Capability information element for the incoming call and routes the call over appropriate facilities.

Available only if all of the following conditions are true:

- **ISDN-BRI Trunks** or **ISDN-PRI** are enabled for the system.
- The trunk group type is access, co, fx, tandem, tie, or wats.
- The **Comm Type** is data, avd, or rbavd.

| Valid Entry | Usage  |
|-------------|--|
| 0           | Voice and voice-grade data                                     |
| 1           | 56 kbps synchronous data transmitted with robbed-bit signaling |
| 2           | Less than 19.2 kbps synchronous or asynchronous data           |
| 4           | 64 kbps data on unrestricted channels                          |

#### Related topics:

[Group Type](#) on page 725

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

[Comm Type](#) on page 980

#### Busy Threshold

| Valid Entry | Usage  |
|-------------|--|
| 1 to 255    | The number of trunks that must be busy to alert attendants to control access to outgoing and two-way trunk groups during periods of high use. When the threshold is reached and the warning lamp for that trunk group lights, the attendant can activate trunk group control: internal callers who dial out using a trunk access code are connected to the attendant. Calls handled by AAR and ARS route patterns go out normally. |

#### CDR Reports

| Valid Entry    | Usage  |
|----------------|--|
| y              | All outgoing calls on this trunk group generate call detail records. If <b>Record Outgoing Calls Only</b> is disabled for CDR, incoming calls on this trunk group also generate call detail records.   |
| n              | Calls over this trunk group do not generate call detail records.   |
| r (ring-intvl) | CDR records are generated for both incoming and outgoing calls. In addition, the following ringing interval CDR records are generated: <ul style="list-style-type: none"> <li>• <b>Abandoned calls:</b> The system creates a record with a condition code of "H" indicating the time until the call was abandoned.</li> <li>• <b>Answered calls:</b> The system creates a record with a condition code of "G" indicating the interval from start of ring to answer.</li> <li>• <b>Calls to busy stations:</b> The system creates a record with a condition code of "I" indicating a recorded interval of 0.</li> </ul> |

**Related topics:**

[Record Outgoing Calls Only](#) on page 474

**CESID I Digits Sent**

For emergency 911 service, Communication Manager might send Caller's Emergency Service Identification (CESID) information to the local telephone company central office or E911 tandem server or switch. This digit string is part of the E911 signaling protocol. Determine the correct entry for this field by talking to the E911 provider. Accepts from one to three digits.

Available only for a cama trunk group.

**Related topics:**

[Group Type](#) on page 725

**Comm Type**

Indicates whether the trunk group carries voice, data, or both.



**Note:**

**Comm Types** of avd, rbavd, and data require trunk member ports on a DS1 circuit pack.

| Valid Entry | Usage  |
|-------------|--|
| avd         | For applications that mix voice and Digital Communication Protocol data, such as video conferencing applications. The receiving end server discriminates voice calls from data calls and directs each to an appropriate endpoint. Neither originating nor terminating ends insert a modem pool for any calls. The <b>Signaling Mode</b> for the DS1 circuit pack must be set to either common-chan or CAS signaling. |
| data        | All calls across the trunk group originate and terminate at Communication Manager digital data endpoints. Public networks don't support data: supported by Avaya's DCP protocol, this entry is used almost exclusively for the data trunk group supporting DCS signaling channels. The <b>Signaling Mode</b> for the DS1 circuit pack must be set to either robbed-bit or common-chan.                               |
| rbavd       | For digital trunk groups that carry voice and data with robbed-bit signaling. The <b>Signaling Mode</b> for the DS1 circuit pack must be set to robbed-bit unless mixed mode signaling is allowed on the DS1 circuit pack. In that case, the <b>Signaling Mode</b> must be isdn-ext or isdn-pri.   |
| voice       | For trunk groups that carry only voice traffic and voice-grade data (that is, data transmitted by modem). Analog trunk groups must use voice.  |

**Related topics:**

[Signaling Mode](#) on page 550

## COR

| Valid Entry | Usage  |
|-------------|--|
| 0 to 995    | The Class of Restriction (COR) for the trunk group. Classes of restriction control access to trunk groups, including trunk-to-trunk transfers. Decisions regarding the use of Class of Restriction (COR) and Facility Restriction Levels (FRLs) should be made with an understanding of their implications for allowing or denying calls when AAR/ARS/WCR route patterns are accessed. |

**Tip:**

Remember that FRLs are assigned to classes of restriction. Even if two trunk groups have classes of restriction that allow a connection, different facility restriction levels might prevent operations such as off-net call forwarding or outgoing calls by remote access users.

## CO Type

Available only if the country code is 14. Used only by trunk group members administered on a TN464D vintage 2 or later DS1 circuit pack.

| Valid Entry       | Usage  |
|-------------------|--|
| analog<br>digital | Specifies whether the trunk group is connected to analog or digital facilities at the local telephone company central office (CO). |

**Related topics:**

[Country](#) on page 822

## Country

The country code that corresponds to the protocol used by the local telephone company central office (CO) where the trunk group terminates.

Available only for trunk groups that connect Communication Manager to a CO in the public network — CO, DID, DIOD, FX, and WATS trunk groups.

**Caution:**

Customers should not attempt to administer this field. Please contact your Avaya technical support representative for assistance.

| Valid Entry            | Usage  |
|------------------------|--|
| 1 to 25, except for 19 | For a list of country codes, see the <i>Country code table</i> .                                     |
| 11                     | Communication Manager is administered for Public Network Call Priority (Call Retention and Re-ring). |
| 14                     |  |
| 15                     | Communication Manager is administered for Public Network Call Priority (Intrusion and Re-ring).      |

| Valid Entry | Usage   |
|-------------|---|
| 18          | Communication Manager is administered for Public Network Call Priority (Mode of Release Control, Forced Disconnect, and Re-ring). |
| 23          | If the trunk <b>Group Type</b> is either CO or DID, Communication Manager is administered for Block Collect Calls.                |

**Related topics:**

[Trunk Gain](#) on page 826

[Trunk Termination](#) on page 827

[Country options table](#) on page 935

**Dial Access**

Controls whether users can route outgoing calls through an outgoing or two-way trunk group by dialing its trunk access code. Allowing dial access does not interfere with the operation of AAR/ARS.



**Security alert:**

Calls dialed with a trunk access code over WATS trunks bypass AAR/ARS and are not restricted by facility restriction levels. For security, leave this field disabled unless dial access is needed to test the trunk group.

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows users to access the trunk group by dialing its access code.   |
| n           | Does not allow users to access the trunk group by dialing its access code. Attendants can still select this trunk group with a <b>Trunk Group Select</b> button. |

**Digit Absorption List**

| Valid Entry     | Usage   |
|-----------------|---|
| 0 to 4<br>blank | Assigns a digit absorption list, when used, to a trunk group that terminates at a local telephone company central office. |



**Note:**

In a DCS network, DCS features that use the **remote-tgs** button (on telephones at a remote end) do not work when the incoming trunk group at your end deletes or inserts digits on incoming calls. If you need to manipulate digits in a DCS network (for example, to insert an AAR feature access code), do it on the outgoing side based on the routing pattern.

**Direction**

The direction of the traffic on this trunk group.

Available for all trunk groups except DID and CPE.

| Valid Entry | Usage  |
|-------------|--|
| incoming    | Traffic on this trunk group is incoming.   |
| outgoing    | Traffic on this trunk group is outgoing  |
| two-way     | Traffic on this trunk group is incoming and outgoing. Required for <b>Network Call Redirection</b> . |

**Related topics:**

[Answer Supervision Timeout](#) on page 733

[Disconnect Supervision-Out](#) on page 735

[Receive Answer Supervision](#) on page 825

**Group Name**

A unique name that provides information about the trunk group. Accepts up to 27 characters.

This field should contain names that identify the vendor and function of the trunk group rather than the group type (DID, WATS).

**Note:**

Supported by Unicode language display for the 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones. Unicode is also an option for the 2420J telephone when the **Display Character Set** is katakana. For more information on the 2420J, see *2420 Digital Telephone User's Guide*.

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Related topics:**

[Display Character Set](#) on page 938

**Group Number**

The trunk group number.

**Note:**

For trunk groups connecting two servers in Distributed Communication System networks, assign the same group number on both servers.

**Group Type**

The type of trunk group. The fields that are displayed and available might change according to the trunk group type selected.

| Valid Entry | Usage  |
|-------------|--|
| Access      | Used to connect satellite servers to the main switch in Electronic Tandem Networks (ETN). Access trunks do not carry traveling class marks (TCM) and thus allow satellite callers unrestricted access to out-dial trunks on the main server. This entry allows Inband ANI. |

| Valid Entry | Usage   |
|-------------|---|
| APLT        | Advanced Private Line Termination (APLT) trunks. Used in private networks. This entry allows Inband ANI.  |
| CAMA        | Used to route emergency calls to the local community's Enhanced 911 systems.  |
| CO          | Typically used to connect Communication Manager to the local telephone company central office, but can also connect adjuncts such as external paging systems and data modules.  |
| CPE         | Used to connect adjuncts, such as paging systems and announcement or music sources, to the server running Communication Manager.  |
| DID         | Used to direct callers directly to individuals within an organization without going through an attendant or some other central point. This entry allows Inband ANI.   |
| DIOD        | Two-way trunks that are used to transmit dialed digits in both directions. In North America, tie trunks are used for applications that require two-way transmission of dialed digits. This entry allows Inband ANI.   |
| DMI-BOS     | Digital Multiplexed Interface - Bit-Oriented Signaling (DMI-BOS) trunks allow communication with systems using DMI-BOS protocol. This entry also allows Inband ANI.   |
| FX          | A local telephone company central office (CO) trunk that connects the server running Communication Manager directly to a CO outside the local exchange area. Used to reduce long-distance charges if the organization averages a high volume of long-distance calls to a specific area code.  |
| ISDN        | <p>Used when digital trunks are needed that can integrate voice, data, and video signals and provide the bandwidth needed for applications such as high-speed data transfer and video conferencing. ISDN trunks can also efficiently combine multiple services on one trunk group. Also used for <b>Network Call Transfer</b>.</p> <p> <b>Note:</b><br/>Available only if <b>ISDN-PRI</b>, <b>ISDN-BRI Trunks</b>, or both have been enabled for the system.</p> |
| RLT         | Used with Centralized Attendant Service in a private network.   |
| SIP         | <p>Used to connect a server running Communication Manager to a SIP Enablement Services (SES) home server, or to connect two Communication Manager servers.</p> <p> <b>Note:</b><br/>The Automatic CallBack, Priority Calling, and Whisper Page features do not work correctly if each of the call's parties is using a SIP endpoint administered on and managed by a different instance of Communication Manager.</p>  |
| Tandem      | Used to connect tandem nodes in a private network. This entry allows Inband ANI.  |

| Valid Entry | Usage   |
|-------------|---|
| Tie         | Used to connect a server running Communication Manager to a local telephone company central office or to another server or switch in a private network. Tie trunks transmit dialed digits with both outgoing and incoming calls. This entry also allows Inband ANI.   |
| WATS        | Used to reduce long-distance bills when your organization regularly places many calls to a specific geographical area in North America. Outgoing WATS service allows calls to certain areas ("WATS band") for a flat monthly charge. Incoming WATS trunks allow toll-free calling to customers and employees. |

**Related topics:**

- [Local Country Code](#) on page 605
- [International Access Code](#) on page 605
- [Carrier Medium](#) on page 722
- [Supplementary Service Protocol](#) on page 737
- [SBS](#) on page 744
- [Path Replacement](#) on page 750
- [Call Still Held](#) on page 821
- [ISDN-BRI Trunks](#) on page 947
- [ISDN-PR1](#) on page 947

**Incoming Destination**

Sets the destination for all incoming calls on trunk groups such as CO, FX, and WATS that must terminate at a single destination. The destination entered here is also the default night service destination. Available only for incoming or two-way trunk groups.

| Valid Entry                   | Usage   |
|-------------------------------|---|
| <i>Valid extension number</i> | <p>Calls go to this extension number. You can enter any type of extension, though typically the extension entered here identifies a VDN, a voice response unit, or a voice messaging system. Night service overrides this setting when it is active.</p> <p> <b>Note:</b></p> <p>When entering a Multi-Location Dial Plan shortened extension in a field designed for announcement extensions, certain administration end validations that are normally performed on announcement extensions are not done, and resultant warnings or submittal denials do not occur. The shortened extensions also do not appear in any display or list that shows announcement extensions. Extra care should be taken to administer the correct type of announcement for the application if assigning shortened extensions.</p> |
| attd                          | Calls go to the attendant and are recorded as Listed Directory Number (LDN) calls on call detail records.   |
| blank                         | Leave this field blank if <b>Trunk Type (in/out)</b> is not administered as auto/<br>....   |

**Related topics:**

- [Direction](#) on page 724
- [Trunk Type](#) on page 826
- [Night Service](#) on page 986

ITC

Determines the line coding the Generalized Route Selection feature uses for comparison to select appropriate routes for voice and data calls.

Available only when the **Comm Type** is data, avd, or rbavd and a **BCC** value is administered.

| Valid Entry    | Usage   |
|----------------|---|
| rest(stricted) | Restricted trunks use ami-basic or ami-zcs line coding and can carry only restricted calls.   |
| unre(stricted) | Unrestricted trunks use b8zs, hdb3, or cmi line coding and can carry restricted or unrestricted calls. A trunk group with an unrestricted ITC can have only unrestricted trunks as members. |

**Related topics:**

- [Comm Type](#) on page 980

Night Service

Sets the destination for incoming calls when **Night Service** is operating. If a night service destination is administered for an individual trunk that is a member of this group, that entry overrides the group destination for that trunk. CPE, DID, and DIOD trunk groups do not support night service.

 **Tip:**

Whenever possible, use a night service destination on your switch; otherwise, some features do not function correctly over a DCS network.

| Valid Entry                        | Usage   |
|------------------------------------|---|
| An extension number (can be a VDN) | The extension of your night service destination.<br><br> <b>Note:</b><br>When entering a Multi-Location Dial Plan shortened extension in a field designed for announcement extensions, certain administration end validations that are normally performed on announcement extensions are not done, and resultant warnings or submittal denials do not occur. The shortened extensions also do not appear in any display or list that shows announcement extensions. Extra care should be taken to administer the correct type of announcement for the application if assigning shortened extensions. |
| attd                               | Calls go to the attendant and are recorded as Listed Directory Number (LDN) calls on call detail records.   |
| blank                              | Leave this field blank if <b>Trunk Type (in/out)</b> is not administered as auto/<br>....   |

**Related topics:**

[Trunk Type \(in/out\)](#) on page 991

**Number of Members**

Available only for sip trunk groups.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 255    | The number of SIP Enablement Services (SES) trunks that are members of the trunk group. All members of an SES trunk group will have the same characteristics. |

**Related topics:**

[Group Type](#) on page 725

**Outgoing Display**

Allows display telephones to show the name and number of the trunk group used for an outgoing call before the call is connected.

| Valid Entry | Usage                                     |
|-------------|---|
| y           | Displays the trunk group name and number. |
| n           | Displays the digits the caller dials.     |

**Prefix-1**

If enabled, the prefix “1” is added to the beginning of the digit string for outgoing calls. Use this field for outgoing and two-way trunk groups handling long distance service. Do not enable for trunk groups in AAR or ARS route patterns.

Available only for CO, FX, and DIOD trunk groups.

**Protocol Type**

The type of line signaling protocol used by the local telephone company central office for DID and DIOD trunk groups.

Available only if the **Country** code is 15. Used only by trunk group members administered on a TN2199 or TN464D vintage 3 or later circuit pack.

| Valid Entry | Usage   |
|-------------|---|
| inloc       | Incoming local. Only the inloc protocol provides ANI. |
| intol       | Incoming toll.  |

**Related topics:**

[Country](#) on page 822

[Country options table](#) on page 935

**Queue Length**

Available only for outgoing or two-way trunk groups.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 100    | The number of outgoing calls that can wait in queue when all trunks in a trunk group are busy. Calls wait in queue in the order in which they were made. If a queue is administered, a caller hears a confirmation tone when no trunk is available for the outgoing call. The caller can then hang up and wait; when a trunk becomes available, Communication Manager calls the extension that placed the original call. Communication Manager remembers the number the caller dialed and automatically completes the call. |
| 0           | Callers receive a busy signal when no trunks are available. Use for DCS trunks.   |

**Related topics:**

[Direction](#) on page 724

Service Type

The service for which this trunk group is dedicated. In addition to the predefined services or features listed as valid entries, any previously administered user-defined Network Facility **Facility Type** of 0 (feature) or 1 (service) is allowed.

| Valid Entry | Usage   |
|-------------|---|
| access      | A tie trunk giving access to an Electronic Tandem Network.  |
| accunet     | ACCUNET Switched Digital Service — part of ACI (AT&T Communications ISDN) phase 2.  |
| cbc         | Call-by-Call service — provides different dial plans for different services on an ISDN trunk group. Indicates this trunk group is used by the Call-By-Call Service Selection feature. |
| dmi-mos     | Digital multiplexed interface — message-oriented signaling.   |
| i800        | International 800 Service — allows a subscriber to receive international calls without a charge to the call originating party.  |
| inwats      | INWATS — provides OUTWATS-like pricing and service for incoming calls.  |
| lds         | Long-Distance Service — part of ACI (AT&T Communications ISDN) phase 2.   |
| megacom     | MEGACOM Service — an AT&T communications service that provides unbanded long-distance services using special access (switch to 4ESS switch) from an AT&T communications node.         |
| mega800     | MEGACOM 800 Service — an AT&T communications service that provides unbanded 800 service using special access (4ESS switch to switch) from an AT&T communications node.                |
| multiquest  | AT&T MULTIQUEST Telecommunications Service — dial 700 service. A terminating-user's service that supports interactive voice service   |

| Valid Entry  | Usage   |
|--------------|---|
|              | between callers at switched-access locations and service provides directly connected to the AT&T Switched Network (ASN).  |
| operator     | Network Operator — provides access to the network operator.   |
| outwats-bnd  | OUTWATS Band — WATS is a voice-grade service providing both voice and low speed data transmission capabilities from the user location to defined service areas referred to as bands; the widest band is 5.  |
| public-ntwrk | Public network calls — It is the equivalent of CO (outgoing), DID, or DIOD trunk groups. If Service Type is public-ntwrk, <b>Dial Access</b> can be enabled.  |
| sddn         | Software Defined Data Network — provides a virtual private line connectivity via the AT&T switched network (4ESS switches). Services include voice, data, and video applications. These services complement the SDN service. Do not use for DCS with Rerouting. |
| sdn          | Software Defined Network (SDN) — an AT&T communications offering that provides a virtual private network using the public switched network. SDN can carry voice and data between customer locations as well as off-net locations.                               |
| sub-operator | Presubscribed Common Carrier Operator — provides access to the presubscribed common carrier operator.   |
| tandem       | Tandem tie trunks integral to an ET.  |
| tie          | Tie trunks — general purpose.   |
| wats-max-bnd | Maximum Banded Wats — a WATS-like offering for which a user's calls are billed at the highest WATS band subscribed to by users.   |

**Related topics:**

[Facility Type](#) on page 812

## Signaling Group

Available only for sip trunk groups.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 650    | The number of the SIP Enablement Services (SES) signaling group associated with this trunk group. |

**Related topics:**

[Group Type](#) on page 725

[Group Number](#) on page 860

## TAC

The trunk access code (TAC) that must be dialed to access the trunk group. A different TAC must be assigned to each trunk group. CDR reports use the TAC to identify each trunk group.

## Managing inventory

The characters “\*” and “# ” can be used as the first character in a TAC. Accepts a one- to four-digit number.

### TN

| Valid Entry | Usage  |
|-------------|--|
| 1 to 100    | A tenant partition number assigned to this trunk group.<br> <b>Tip:</b><br>If an unassigned tenant partition number is used, the system accepts the entry but calls cannot go to the trunk group. |

### Toll Restricted

If enabled, restricts toll-restricted users from using a trunk access code to make restricted outgoing calls over this trunk group.

### Trunk Flash

Enables or disables multifunction telephones to access local telephone company central office (CO) customized services that are provided by servers at the far-end or CO. These CO customized services are electronic features, such as conference and transfer, that are accessed by a sequence of flash signal and dial signals from the Communication Manager telephone on an active trunk call.

### Trunk Signaling Type

Controls the signaling used by members in private network trunk groups, mainly in Italy, Brazil, and Hungary. This field also controls the signaling used by members in public network digital trunk groups.

Available only for access, aplt, rlt, tandem, or tie trunk groups.

E&M trunks in Italy, Brazil, and Hungary can use either continuous or discontinuous signaling. Each entry specifies a set of signals and available timers used in the process of setting up and releasing connections. The type of signaling must match the signaling type administered on the far-end server. Use these values only when all trunk group members are assigned to ports on a TN464F, TN2464, or TN2140 circuit pack.

| Valid Entry | Usage         |
|-------------|---------------|
| cont        | Continuous    |
| dis         | Discontinuous |

The following entries are for tie trunks in Main-Satellite/Tributary networks. Use these values only when all trunk group members are assigned to a TN497 circuit pack.

| Valid Entry | Usage  |
|-------------|--|
| tgu         | For outgoing trunks, tgu at the main server running Communication Manager administers a tie trunk group connected to a satellite server. (This same group should be administered as tge at the satellite.) |

| Valid Entry | Usage  |
|-------------|--|
| tge         | For incoming trunks, tge at a satellite server administers a tie trunk group connected to the main server running Communication Manager. (This same group should be administered as tgu at the main server.) |
| tgi         | For internal trunks, tgi administers a two-way tie trunk group between two satellites or between the main server and a satellite. (This trunk group should be administered as tgi on both servers.)          |

DIOD trunks support pulsed and continuous E&M signaling in Brazil and discontinuous E&M signaling in Hungary. The following entries are for DIOD trunks. Use these values only when all trunk group members are assigned to a TN464F (or later version) or TN2464 circuit pack.

| Valid Entry | Usage                         |
|-------------|-------------------------------|
| cont        | Continuous E&M signaling.     |
| pulsed      | Pulsed E&M signaling.         |
| discont     | Discontinuous E&M signaling.  |
| blank       | Leave blank for R2 signaling. |

#### Related topics:

[Group Type](#) on page 725

#### Trunk Type (in/out)

Controls the seizure and start-dial signaling used on this trunk group. Settings might differ for incoming and outgoing trunks.

| Valid Entry | Usage  |
|-------------|--|
| auto        | Used for immediate connection to a single preset destination (incoming local telephone company central office trunks, for example). No digits are sent, because all calls terminate at the same place.   |
| cont        | Continuous signaling is used with Italian E&M tie trunks. The server/switch seizes a trunk by sending a continuous seizure signal for at least the duration specified by the Incoming Seizure Timer.   |
| delay       | The sending switch does not send digits until it receives a delay dial signal (an off-hook signal followed by an on-hook signal) from the far-end switch, indicating that it is ready to receive the digits.   |
| disc        | Discontinuous signaling is used with Italian tie trunks that use E&M signaling. The Avaya server can seize a trunk by sending a single, short signal for the duration specified by the <b>Normal Outgoing Seize Send</b> value. However, with the Three-Way Seizure option, the calling end can also send routing information to the called end by sending one or a series of brief seizure signals. |
| wink        | The sending server or switch does not send digits until it receives a wink start (momentary off-hook) signal from the far-end server or switch, indicating that it is ready to receive the digits.   |

| Valid Entry                      | Usage   |
|----------------------------------|---|
| immed                            | The sending server or switch sends digits without waiting for a signal from the far-end server or switch.   |
| 2-wire-ac<br>2-wire-dc<br>3-wire | Used with local telephone company central office (CO) trunks in Russia. Select the type of connection to the CO. Check with the network service provider for the type of connection. To use these entries, the <b>Country</b> code must be 15 and the CO trunks must use ports on a TN2199 circuit board. |



**Tip:**

When incoming trunks use the setting immed/immed, the far-end server seizes the trunk and sends digits without waiting for acknowledgment from the receiving end. When traffic is heavy, the receiving server or switch might not immediately attach a Touch Tone Receiver to a call and therefore lose digits. Use wink-start trunks or increase the dial-guard timer value on the far-end server or switch to avoid this problem.

**Related topics:**

[Country](#) on page 822

[Normal Outgoing Seize Send \(msec\)](#) on page 1028

Version

Adjusts the signaling on multi-country local telephone company central office (CO) trunk circuit packs. Entries adjust signaling characteristics on these circuit packs to match the signaling characteristics of the public network in a specific country.

Available only for CO, FX, and WATS trunk groups when the **Country** code is 5, 16, or 23.

If the **Country** code is 5, this field controls only TN2147 ports.

| Valid Entry | Usage   |
|-------------|---|
| a           | Uses standard signaling for the Netherlands public network.   |
| b           | Uses country 1 (U.S.) signaling. This value is appropriate if Communication Manager is connected to a CO using an Ericcson AXE-10 switch. |

If the **Country** code is 16 or 23, this field sets the input impedance value and only controls TN465C (vintage 2 or later) ports.

| Valid Entry | Usage  |
|-------------|--|
| a           | Sets input impedance to 600 Ohms.                                      |
| b           | Sets input impedance to 900 Ohms. This value is appropriate in Brazil. |

**Related topics:**

[Country](#) on page 822

**Trunk Group: page 2****Administer Timers**

Enables or disables administration of timers on this trunk group. The default for the ISDN trunk group type is disabled. All other trunk group types are enabled by default.

Available for all trunk group types *except* cpe, h.323, and sip.

**Related topics:**

[Group Type](#) on page 725

**Analog Loss Group**

Determines which administered two-party row in the loss plan applies to this trunk group if the call is carried over an analog signaling port in the trunk group.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 17     | The index into the loss plan and tone plan. If values are administered other than in between 6 and 10 or 15 and 17, a warning message displays stating that the loss group may not be appropriate for this trunk group. |

**Answer Supervision Timeout**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 250    | The number of seconds Communication Manager waits before it acts as though answer supervision has been received from the far-end. During a cut-through operation, timing begins after each outgoing digit is sent and timing ceases after the far-end sends answer supervision. On senderized operation, the timer begins after the last digit collected is sent. |

 **Note:**

This field's setting does not override answer supervision sent from the network or from DS1 port circuit timers.

**Related topics:**

[Administer Timers](#) on page 733

[Receive Answer Supervision](#) on page 825

**Auto Guard**

Enables or disables Auto Guard, which prevents repeated seizures of a defective trunk. Communication Manager does a maintenance busy-out on these trunks. This field controls ports only on TN438B, TN465B, and TN2147 circuit packs. TN438B ports have hardware support for detecting a defective trunk. TN465B and TN2147 ports consider a trunk defective if no dial tone is detected on an outgoing call, and the **Outpulse Without Tone** feature is disabled for the system.

Available only for co or fx trunk groups.

**Related topics:**

[Outputpulse Without Tone](#) on page 607

[Group Type](#) on page 725

Bit Rate

Available when the **Comm Type** is avd or rbavd. Also available if the **Comm Type** is data, but only if **ISDN-PRI** is enabled for the system.

| Valid Entry                                  | Usage                                      |
|--|--|
| 300<br>1200<br>2400<br>4600<br>9600<br>19200 | The baud rate to be used by pooled modems. |

**Related topics:**

[ISDN-PRI](#) on page 947

[Comm Type](#) on page 980

Call Still Held

If enabled, the system prevents glare by extending the Incoming Glare Guard timer and delaying an outgoing seizure of a trunk for at least 140 seconds after it is released from an incoming call. This field is used when the receiving end media server or switch initiates the disconnection of incoming calls. This field affects only TN438B, TN465B, and TN2147 ports and is used primarily when the **Country** code is 2.

Available only for co or fx trunk groups.

**Related topics:**

[Group Type](#) on page 725

Cut-Through

Available only if the **Outgoing Dial Type** field is rotary or tone.



**Security alert:**

Enabling this field reduces the ability to prevent toll fraud.

| Valid Entry | Usage  |
|-------------|--|
| y           | Users get dial tone directly from the far end of the trunk. If you set the <b>Cut-Through</b> field to y, some administered restrictions are bypassed.       |
| n           | Users receive switch dial tone. Instead of digits being sent to the central office, they are collected, and sent all at once when the user finishes dialing. |

**Related topics:**

[Outgoing Dial Type](#) on page 824

## Cyclical Hunt

Controls the starting point Communication Manager uses to search for an available trunk when a call is sent to the trunk group. Cyclical hunts can be enabled or disabled at any time, however, all the trunks in the group must be idle or busied out.

Available only for two-way loop-start trunks.

| Valid Entry | Usage  |
|-------------|--|
| y           | Communication Manager starts its search from the last trunk seized. This method is faster, and thus better suited for high-traffic trunk groups. |
| n           | Communication Manager starts each search at member 1 (the first trunk administered as a group member).   |

### Related topics:

[Direction](#) on page 724

[Trunk Type](#) on page 826

## Delay Call Setup When Accessed Via IGAR

Appears when the **Group Type** field is isdn or sip. If a user in one network region accesses an ISDN or SIP trunk in another network region through IGAR, the **Delay Call Setup When Accessed Via IGAR** field determines whether the IGAR trunk and the outgoing trunk are initiated in sequence or parallel.

| Valid Entry | Usage   |
|-------------|---|
| y           | The outgoing trunk call waits until the IGAR trunk call is active.  |
| n           | The two trunk calls are set up in parallel. The default value is n. |

## Dial Detection

Indicates whether digit pulses are detected by observing the A-wire (default) or the B-wire only. Applies only to TN2199 ports. The **Country** code must be 15.

### Related topics:

[Country](#) on page 822

## Digital Loss Group

| Valid Entry | Usage  |
|-------------|--|
| 1 to 19     | Determines which administered two-party row in the loss plan applies to this trunk group if the call is carried over a digital signaling port in the trunk group. If values other than 18 or between 11 and 15 are administered, a warning message displays stating that the loss group may not be appropriate for this trunk group. |

## Digits

If the **Digit Treatment** is absorption, this field specifies how many digits are deleted. If the **Digit Treatment** is insertion, this field identifies the specific digits that are added.

| Valid Entry                       | Usage   |
|-----------------------------------|---|
| 1 to 5                            | The number of digits to be deleted (absorbed).                              |
| Up to 4 digits, including * and # | The actual digits to be added (inserted).                                   |
| blank                             | This field can be blank only if <b>Digit Treatment</b> is not administered. |

**Related topics:**

[Digit Treatment](#) on page 996

Digit Treatment

Modifies an incoming digit string by adding or deleting digits. This is required if the number of digits received does not match the dial plan.

Requires administration of the **Digits** to add or delete.

| Valid Entry | Usage  |
|-------------|--|
| absorption  | Deletes digits, starting at the beginning of the string. |
| insertion   | Adds digits, starting at the beginning of the string.    |
| blank       | The incoming digit string is not changed.                |

**Related topics:**

[Digits](#) on page 995

Disconnect Supervision-In

Indicates whether Communication Manager receives disconnect supervision for incoming calls over this trunk group.

Available only for incoming or two-way trunk groups.

| Valid Entry | Usage   |
|-------------|---|
| y           | Allows trunk-to-trunk transfers involving trunks in this group. The far-end server or switch sends a release signal when the calling party releases an incoming call, and the far-end server or switch is responsible for releasing the trunk. Enhances Network Call Redirection. |
| n           | The far-end server or switch does not provide a release signal, the hardware cannot recognize a release signal, or timers are preferred for disconnect supervision on incoming calls. Prevents trunk-to-trunk transfers involving trunks in this group.                           |

 **Caution:**

In general, U.S. local telephone company central offices provide disconnect supervision for incoming calls but not for outgoing calls. Public networks in most other countries do not provide disconnect supervision for incoming or outgoing calls. Check with the network services provider.

**Related topics:**

[Direction](#) on page 724

[Trunk Direction](#) on page 825

**Disconnect Supervision-Out**

Indicates whether Communication Manager receives disconnect supervision for outgoing calls over this trunk group. Available for outgoing or two-way trunk groups.

| Valid Entry | Usage   |
|-------------|---|
| y           | Allows trunk-to-trunk transfers involving trunks in this group. The far-end sends a release signal when the called party releases an outgoing call, and the far-end is responsible for releasing the trunk. Enhances Network Call Redirection. Available only if <b>Answer Supervision Timeout</b> is 0 and <b>Receive Answer Supervision</b> is enabled. |
| n           | The far-end server or switch does not provide a release signal, the hardware cannot recognize a release signal, or timers are preferred for disconnect supervision on outgoing calls. Prevents trunk-to-trunk transfers involving trunks in this group.   |

**Caution:**

Verify that the far-end server or switch provides answer supervision and disconnect supervision. Most public networks do not provide disconnect supervision over analog trunks. Check with the network services provider.

**Related topics:**

[Direction](#) on page 724

[Answer Supervision Timeout](#) on page 733

[Receive Answer Supervision](#) on page 825

**Disconnect Timing (msec)**

| Valid Entry                              | Usage   |
|--|---|
| 140 to 2550 ms<br>in increments of<br>10 | Specifies the minimum time in milliseconds that the local telephone company central office or far-end server requires to recognize that this server has disconnected from a call. This timer does not affect ports on a circuit pack that uses the administrable Incoming Disconnect and Outgoing Disconnect timers. Settings on those two timers override this field.<br><br>The default of 500 is an industry standard and should not be changed. If this field is set too high, the server or switch does not disconnect sometimes when it should; too low, and it disconnects when it should not. |

**Disconnect Type**

Indicates which side or user controls the disconnect. A refers to the calling party, and B refers to the called party.

## Managing inventory

Available only if the **Country** code is 15 and the **Trunk Type** is 2-wire-ac, 2-wire-dc, or 3-wire. Applies only to the TN2199 port.

| Valid Entry | Usage                                 |
|-------------|---------------------------------------|
| AandB       | Both parties control the disconnect.  |
| AorB        | Either party controls the disconnect. |

### Related topics:

[Country](#) on page 822

[Trunk Type](#) on page 826

## Drop Treatment

| Valid Entry                  | Usage  |
|------------------------------|--|
| intercept<br>busy<br>silence | Determines what the calling party hears when the called party terminates an incoming call. For security reasons, it is better to apply a tone; silence can provide an opening for hackers. Applies only to DID trunks. |

### \* Note:

In Italy, **Drop Treatment** must be administered as intercept for all DID trunk groups.

## Duplex

Available if the **Comm Type** is avd or rbavd. Also available if the **Comm Type** is data, but only if **ISDN-PRI** is enabled for the system.

### \* Note:

Even if the trunk group supports full-duplex transmission, other equipment in a circuit might not.

| Valid Entry | Usage   |
|-------------|---|
| full        | Allows simultaneous two-way transmission, which is most efficient. Recommended in most cases. |
| half        | Supports only one transmission direction at a time.   |

### Related topics:

[ISDN-PRI](#) on page 947

[Comm Type](#) on page 980

## End-to-End Signaling

Available only for a cpe (customer-provided equipment) trunk group.

| Valid Entry                      | Usage  |
|----------------------------------|--|
| 60 to 360 ms in increments of 10 | The duration of the touch tone signal sent to auxiliary equipment. Equipment such as paging equipment and music sources might be |

| Valid Entry | Usage  |
|-------------|--|
|             | connected to Communication Manager by auxiliary trunks. Communication Manager might send DTMF signals (touch tones) to these devices. This field sets the duration of these tones. |

**Related topics:**

[Group Type](#) on page 725

## Expected Digits

| Valid Entry | Usage   |
|-------------|---|
| 1 to 18     | The number of digits that the far-end server sends for an incoming connection. If the end is absorbing digits on this trunk group, the entry in this field must be larger than the value administered for the number of digits to be absorbed.  |
| blank       | Required if <b>Digit Treatment</b> is insert and <b>Digits</b> is a feature access code (for example, AAR or ARS) followed by digits. In this case, the number of digits expected are set on the AAR and ARS Digit Analysis Table and AAR and ARS Digit Conversion Table. If left blank, digit absorption cannot be administered. |

**Related topics:**

[Digits](#) on page 995

[Digit Treatment](#) on page 996

## Extended Loop Range

Available only for a DID trunk group. This field is used only with the TN459A circuit pack.

| Valid Entry | Usage  |
|-------------|--|
| y           | The distance between the local telephone company central office (CO) and the server is greater than the required distance. |
| n           | The distance between the CO and the server is not greater than the required distance.                                      |

## Format

Specifies the encoding of Numbering Plan Indicator for identification purposes in the Calling Number and/or Connected Number IEs, and in the QSIG Party Number.

Available only if **Send Calling Number** or r or the **Send Connected Number** is enabled or restricted.

| Valid Entry | Usage  |
|-------------|--|
| public      | Indicates that the number plan according to CCITT Recommendation E. 164 is used. |
| unknown     | Indicates the <b>Numbering Plan Indicator</b> is unknown.                        |

| Valid Entry | Usage  |
|-------------|--|
| private     | Indicates the <b>Numbering Plan Indicator</b> is PNP.  |
| unk-pvt     | Determines the type of number from the private numbering format, but the <b>Numbering Plan Indicator</b> is unknown. |

**Related topics:**

[Send Calling Number](#) on page 745

[Send Connected Number](#) on page 746

Group Type

Displays the type of trunk group.

**Related topics:**

[Group Type](#) on page 725

[ISDN-BRI Trunks](#) on page 947

[ISDN-PR1](#) on page 947

Incoming Calling Number - Delete

Available only for incoming or two-way trunk groups.

| Valid Entry             | Usage   |
|-------------------------|---|
| 1 to 15<br>all<br>blank | The number of digits, if any, to delete from the calling party number for all incoming calls on this trunk group. |

**Related topics:**

[Direction](#) on page 724

Incoming Calling Number - Format

The TON/NPI encoding applied to CPN information modified by the CLI Prefix feature. This encoding does not apply to calls originating locally.

If this field is blank, Communication Manager passes on the encoding received in the incoming setup message. If the incoming setup message did not contain CPN information and digits are added, the outgoing message will contain these digits. If a numbering format is not administered in this case, the value defaults to pub-unk. If the numbering format is administered as unknown, the trunk group is modified to unk-unk encoding of the TON/NPI. Therefore, this field also must contain a value other than unknown.

The values for this field map to the Type of Numbering (TON) and Numbering Plan Identifier (NPI) values shown below.

| Valid Entry | Type of Numbering (TON) | Numbering Plan Identifier (NPI) |
|-------------|-------------------------|---------------------------------|
| blank       | incoming TON unmodified | incoming NPI unmodified         |

| Valid Entry | Type of Numbering (TON) | Numbering Plan Identifier (NPI) |
|-------------|-------------------------|---------------------------------|
| natl-pub    | national(2)             | E.164(1)                        |
| intl-pub    | international(1)        | E.164(1)                        |
| locl-pub    | local/subscriber(4)     | E.164(1)                        |
| pub-unk     | unknown(0)              | E.164(1)                        |
| lev0-pvt    | local(4)                | Private Numbering Plan - PNP(9) |
| lev1-pvt    | Regional Level 1(2)     | Private Numbering Plan - PNP(9) |
| lev2-pvt    | Regional Level 2(1)     | Private Numbering Plan - PNP(9) |
| unk-unk     | unknown(0)              | unknown(0)                      |

**Related topics:**

[Numbering Format](#) on page 742

[Format](#) on page 999

**Incoming Calling Number - Insert**

| Valid Entry            | Usage  |
|------------------------|--|
| 0 to 9<br>all<br>blank | Up to 15 digits added to the beginning of the digit string of incoming calls when the calling party is a member of this trunk group. |

**Incoming Dial Tone**

Indicates whether or not the server running Communication Manager gives dial tone in response to far-end seizures of the trunk group.

| Valid Entry | Usage  |
|-------------|--|
| y           | Used if the incoming trunk group transmits digits. For example, this option is used for two-way, dial-repeating tie trunks that users select by dialing a trunk access code. |
| n           | Used for trunks that are not sending digits, such as tandem or incoming local telephone company central office trunks.   |

**Incoming Dial Type**

Indicates the type of pulses required on an incoming trunk group. This value should match what the local telephone company central office provides.

Available for Access, APLT, DID, DIOD, DMI-BOS, FX, RLT, Tandem, or WATS trunk groups. Also available for tie trunk groups when the **Trunk Signaling Type** is blank, cont, or dis.

| Valid Entry | Usage  |
|-------------|--|
| tone        | Used for Dual Tone Multifrequency (DTMF) addressing, also known as "touchtone" in the U.S. Allows the trunk group to support both DTMF and |

## Managing inventory

| Valid Entry | Usage   |
|-------------|---|
|             | rotary signals. Used for the Inband ANI feature. Also used for pulsed and continuous E&M signaling in Brazil and for discontinuous E&M signaling in Hungary.  |
| rotary      | Allows only the dial pulse addressing method used by non-touch tone telephones. Though the tone entry supports rotary dialing as well, it is inefficient to reserve touch tone registers for calls that do not use DTMF.  |
| mf          | Used if a <b>Trunk Signaling Type</b> is not administered. Available only if <b>Multifrequency Signaling</b> is enabled for the system. Not available if this trunk is used for DCS. Required for pulsed and continuous E&M signaling in Brazil and for discontinuous E&M signaling in Hungary. |

### Related topics:

[Group Type](#) on page 725

## Incoming Rotary Timeout (sec)

| Valid Entry      | Usage   |
|------------------|---|
| 5 to 99<br>blank | Sets the maximum time to wait to receive all incoming digits from the far-end switch. |

### Related topics:

[Incoming Dial Type](#) on page 1001

## Line Length

Available only for trunk groups with a **Trunk Signaling Type** of tge, tgi, or tgu.

| Valid Entry   | Usage            |
|---------------|------------------|
| short<br>long | The line length. |

### Related topics:

[Group Type](#) on page 725

[Trunk Signaling Type](#) on page 990

## Outgoing Dial Type

Sets the method used to transmit digits for an outgoing call. Usually, this method should match what the local telephone company central office provides.

DIOD trunks support pulsed and continuous E&M signaling in Brazil and discontinuous E&M signaling in Hungary.

Available for Access, APLT, CO, DIOD, DMI-BOS, FX, RLT, and WATS trunk groups. Also available for Tie trunk groups when the **Trunk Signaling Type** is blank, cont, or dis.

| Valid Entry | Usage  |
|-------------|--|
| tone        | Uses Dual Tone Multifrequency (DTMF) addressing, also known as “touchtone” in the U.S. Allows the trunk group to support both DTMF and rotary signals. For pulsed and continuous E&M signaling in Brazil and for discontinuous E&M signaling in Hungary, use tone or mf.   |
| rotary      | Allows only the dial pulse addressing method used by non-touch tone telephones. For example, this value is appropriate for an internal full touch tone system and for a connection to a local telephone company central office that only supports rotary dialing.  |
| r1mf        | For CAMA trunk groups. It is the only outgoing dial type allowed on CAMA trunk groups. Allows Russian MF Packet Signaling on outgoing trunks. Russian MF Packet Signaling carries calling party number and dialed number information.<br>Available only for co trunk groups.   |
| mf          | Used if a <b>Trunk Signaling Type</b> is not administered. For pulsed and continuous E&M signaling in Brazil and for discontinuous E&M signaling in Hungary, use tone or mf.<br>Available only if Multifrequency Signaling is enabled for the system. Not available if this trunk is used for DCS.                     |
| automatic   | For tie trunks if the <b>Trunk Signaling Type</b> is not administered. This provides “cut-through” operation to outgoing callers who dial a trunk access code, connecting them directly to local telephone company central office dial tone and bypassing any toll restrictions administered on Communication Manager. |

**Related topics:**

[Group Type](#) on page 725

[Multifrequency Signaling](#) on page 948

[Trunk Signaling Type](#) on page 990

## Preferred Minimum Session Refresh Interval (sec)

Available only for sip trunk groups that do not support SCCAN calls.

| Valid Entry | Usage  |
|-------------|--|
| 90 to 1800  | Sets the session refresh timer value of an SES session for non-SCCAN applications. The timer starts once an SES session is established. Communication Manager then sends a session refresh request as a Re-INVITE or UPDATE after every timer interval. If a session refresh request is not received before the interval passes, the session terminates. Default is 600 seconds. |

**Related topics:**

[Group Type](#) on page 725

[SCCAN](#) on page 1004

## Receive Answer Supervision

If enabled, the network provides answer supervision. For Outbound Call Management applications, use for trunks supporting network answer supervision. For trunks that do not

receive a real answer, this field determines when the CallVisor Adjunct-Switch Application Interface (ASAI) connect event is sent.

**Related topics:**

[Administer Timers](#) on page 733

[Answer Supervision Timeout](#) on page 733

Receive Release Ack

If enabled, Communication Manager receives a release acknowledgment in response to a forward or backward release signal. Available only if the **Trunk Signaling Type** is cont or dis. Only applies to TN2140 ports (used for Italian and Hungarian tie trunks).

**Related topics:**

[Trunk Signaling Type](#) on page 990

Redirect on OPTIM failure

| Valid Entry               | Usage   |
|---------------------------|---|
| 250 to 32000 milliseconds | Determines how long to wait for OPTIM to intercede before the call is redirected. Redirect on OPTIM failure is sometimes known as ROOF. |

SCCAN

If enabled, this trunk group provides support for incoming SCCAN calls. Available only for sip type trunk groups when **Enhanced EC500** is enabled for the system.

**Related topics:**

[Group Type](#) on page 725

[Enhanced EC500](#) on page 945

Send Answer Supervision

If enabled, Communication Manager signals the calling server when an incoming call is answered. Available only if the **Trunk Signaling Type** is cont or dis. The field applies only to TN2140 ports. Available only for incoming or two-way trunks.

**Related topics:**

[Direction](#) on page 724

[Trunk Signaling Type](#) on page 990

Send Release Ack

Indicates whether a release acknowledgment is sent in response to a forward or backward release signal. Available only if the **Trunk Signaling Type** is cont or dis. This field applies only to TN2140 ports (used for Italian and Hungarian tie trunks).

**Related topics:**

[Trunk Signaling Type](#) on page 990

Sig Bit Inversion

Indicates which bits in bit-oriented signaling should be inverted, if any. For trunk ports on TN2242 and TN464B and later circuit packs, this field inverts the A- and B-bits as necessary

so that the far-end server or switch can understand seizure and release signals from Communication Manager. If the far-end server, such as a local telephone company central office, on this trunk group interprets the A- and B-bits differently from the default, invert one or both bits — to change “1” to “0” and vice-versa in the A-bit.

| Valid Entry           | Usage                                      |
|-----------------------|--|
| A<br>B<br>A&B<br>none | For the TN464B and later circuit packs.    |
| A and none            | For the Japanese 2Mbit trunk circuit pack. |

**Related topics:**

[Country Protocol](#) on page 539

Supplementary Service Protocol

Available only for ISDN trunk groups.

| Valid Entry | Usage  |
|-------------|--|
| a           | Allows ASAI Flexible Billing. AT&T, Telcordia Technologies, Nortel. When the <b>Country</b> code for the DS1 circuit pack is 1A, SSA selects AT&T custom supplementary services. When the <b>Country</b> code for the DS1 circuit pack is 1B, SSA selects Telcordia Technologies Supplementary Services. When the <b>Country</b> code for the DS1 circuit pack is 1C, SSA selects Nortel Proprietary Supplementary Services. |
| b           | QSIG; also used for SBS signaling trunk groups when full QSIG functionality is needed.   |
| c           | ETSI; used for Network Call Deflection.  |
| d           | ECMA QSIG  |
| e           | Allows ASAI Flexible Billing. Allows DCS with rerouting when the trunk is used for DCS and <b>DCS with Rerouting</b> is enabled.   |
| f           | Feature Plus   |
| g           | ANSI. Available only if <b>ISDN-PRI</b> or <b>ISDN-BRI Trunks</b> is enabled for the system, or the trunk is used for DCS. Used for Network Call Transfer.   |

**Related topics:**

[Country Protocol](#) on page 539

[DCS with Rerouting](#) on page 945

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

[Used for DCS](#) on page 1023

### Synchronization

Available only if the **Group Type** is :

- dmi-bos or isdn
- access, co, fx, tandem, tie, or wats; and the **Comm Type** is avd or rbavd
- access, co, fx, tandem, tie, or wats; the **Comm Type** is data; and **ISDN-PRI** or **ISDN-BRI Trunks** is enabled for the system

 **Caution:**

Do not change this field without the assistance of Avaya or your network service provider.

| Valid Entry   | Usage   |
|---------------|---|
| async<br>sync | Determines whether the trunk group uses synchronous or asynchronous communications. |

**Related topics:**

[Group Type](#) on page 725

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

[Comm Type](#) on page 980

### Trunk Gain

Specifies the amplification applied to the trunks in this group. With the values administered for **Trunk Termination** and **Country** code, the value in this field also determines the input and trans-hybrid balance impedance for TN465B, TN2146, TN2147, and TN2184 ports. All other CO and DID circuit packs are set automatically to high.

| Valid Entry | Usage   |
|-------------|---|
| high        | Used if users complain of low volume.         |
| low         | Used if users complain of squeal or feedback. |

**Related topics:**

[Country](#) on page 822

[Trunk Termination](#) on page 827

### Trunk Hunt

Defines the trunk hunt search order. Communication Manager performs a trunk hunt when searching for available channels within a facility in an ISDN trunk group. The search can be administered per ISDN-PRI trunk group, but it infers the direction of search within all ISDN-PRI facilities (or portions of those facilities) administered within the trunk group.

| Valid Entry | Usage  |
|-------------|--|
| ascend      | Enables a linear trunk hunt search from the lowest to highest numbered channels. All trunks within an ISDN trunk group are selected without regard to the order in which trunks are administered within the trunk group.   |
| cyclical    | Enables a circular trunk hunt based on the sequence the trunks were administered within the trunk group. When using ISDN-BRI interfaces, only cyclical is allowed. The cyclical option cannot be set if the trunk group using ISDN-PRI interfaces is to be used for Wideband operations. |
| descend     | Enables a linear trunk hunt search from the highest to lowest numbered channels. All trunks within an ISDN trunk group are selected without regard to the order in which trunks are administered within the trunk group.   |

**Related topics:**

[Wideband Support](#) on page 748

**Trunk Termination**

Adjusts the impedance of the trunk group for optimal transmission quality.

| Valid Entry | Usage   |
|-------------|---|
| 600ohm      | The distance to the local telephone company central office (CO) or to the server at the other end of the trunk is less than 3,000 feet. |
| rc          | The distance to the CO or to the server at the other end of the trunk is more than 3,000 feet.  |

**Trunk Type**

Controls the seizure and start-dial signaling used on this trunk group. Entries in this field vary according to the function of the trunk group and must match the corresponding setting on the far-end server or switch.

Available only for CO, DID, FX, and WATS trunk groups.

| Valid Entry  | Usage   |
|--------------|---|
| ground-start | Use ground-start signaling for two-way trunks whenever possible. Ground-start signaling avoids glare and provides answer supervision from the far end.  |
| loop-start   | In general, loop-start signaling is used only for one-way trunks. Loop-start signaling is susceptible to glare and does not provide answer supervision. |

| Valid Entry  | Usage   |
|--|---|
| auto/auto<br>auto/delay<br>auto/immed<br>auto/wink | The term before the slash tells Communication Manager how and when it receives incoming digits. The term after the slash tells Communication Manager how and when it should send outgoing digits. <ul style="list-style-type: none"> <li>• auto — Used for immediate connection to a single preset destination (incoming central office trunks, for example). No digits are sent, because all calls terminate at the same place.</li> <li>• delay — The sending server running Communication Manager does not send digits until it receives a delay dial signal (an off-hook signal followed by an on-hook signal) from the far-end server or switch, indicating that it is ready to receive the digits.</li> <li>• immed — The sending server running Communication Manager sends digits without waiting for a signal from the far-end server or switch.</li> <li>• wink — The sending server running Communication Manager does not send digits until it receives a wink start (momentary off-hook) signal from the far-end server or switch, indicating that it is ready to receive the digits.</li> </ul> |
| 2-wire-ac<br>2-wire-dc<br>3-wire                   | These entries are used with local telephone company central office (CO) trunks in Russia. The specific CO should match one of these values. Available only if the <b>Country</b> code is 15 and the CO trunks use ports on a TN2199 circuit board.  |

**Related topics:**

[Country](#) on page 822

Unicode Name

Used to determine whether to send Name1 (legacy name) or Name2 (Unicode name). The value for this field is only examined for calls to SIP Enablement Services (SES) stations over an SES trunk group. Available only for sip trunk groups.

 **Note:**

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

| Valid Entry | Usage  |
|-------------|--|
| y           | Uses the Unicode name.   |
| n           | Uses the name as specified on the station form.<br><br> <b>Note:</b><br>Any non-ASCII characters in the name may not appear correctly on a SIP phone. |
| auto        | The choice to use the station name or the Unicode name is automatically determined based on the called phone's capability and the user's preference.   |

**Related topics:**

[Group Type](#) on page 725

**Wink Timer (msec)**

Sets the wink timer as follows:

- Sets the maximum duration of the wink signal (wait-for-wink-to-end) when **Trunk Type (in/out)** is administered as .../wink.
- Sets the maximum interval after trunk seizure for the wink to begin (wait-for-wink-to-start) when **Trunk Type (in/out)** is administered as .../delay.

Requirements for the United States domestic network specify that the wink signal for wink-start trunks must begin within 5 seconds after a trunk is seized. For trunks with a delay-dial start, the wink must not last longer than 5 seconds. While some circuit packs are hard-coded to allow the full 5 seconds in both cases, other circuit packs allow you reduce the allowed start time and duration, thus reducing the window in which glare can occur.

Available only for wink-type trunks.

**Related topics:**

[Trunk Type \(in/out\)](#) on page 991

**Trunk Group: page 3****Caution:**

Customers: Do not change fields on this page without assistance from Avaya or your network service provider.

**Abandoned Call Search**

Indicates whether this trunk group conducts an Abandoned Call Search to identify ghost calls. Abandoned Call Search is designed to work with analog ground-start local telephone company central office (CO) trunks that do not provide disconnect supervision. The CO must support Abandoned Call Search for the feature to work properly. If the CO provides disconnect supervision, the Abandoned Call Search feature is not needed.

Available only for ground-start type trunks.

**Related topics:**

[Trunk Type](#) on page 826

**ACA Assignment**

Indicates whether Automatic Circuit Assurance (ACA) measurements are taken for this trunk group.

**Charge Conversion**

Available only for outgoing or two-way CO, DIOD, FX, and WATS trunk groups.

| Valid Entry    | Usage  |
|----------------|--|
| 1 to 64<br>500 | Communication Manager multiplies the number of charge units by the value of this field and displays it as a currency amount. Without a value in this field, Communication Manager displays the number of charge units without converting it to currency. |

**Related topics:**

[Direction](#) on page 724

[Trunk Direction](#) on page 825

Charge Type

Text string used to describe charges related to a telephone call. These words or characters appear on telephone displays after the charge amount. Typically uses either the currency symbol or the charge type, but not both. Accepts up to seven characters. Embedded spaces count as characters.

Available only for outgoing or two-way CO, DIOD, FX, and WATS trunk groups.

**Related topics:**

[Direction](#) on page 724

Connected to CO

Enables or disables overlap sending to a local telephone company central office (CO).

Available only for tie trunk groups.

**Related topics:**

[Group Type](#) on page 725

Currency Symbol

The symbol that appears on telephone displays before the charge amount. Accepts from one to three characters. Leading and embedded spaces count as characters.

Available only for outgoing or two-way CO, DIOD, FX, and WATS trunk groups.

**Related topics:**

[Direction](#) on page 724

[Trunk Direction](#) on page 825

Data Restriction

Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Cannot be assigned if **Auto Answer** is administered as all or acd. If enabled, whisper page to this station is denied.

**Related topics:**

[Auto Answer](#) on page 61

## Decimal Point

The appropriate representation for a decimal point as it appears on telephone displays. Available only with outgoing or two-way CO, DIOD, FX, and WATS trunk groups.

### **Note:**

If the received charge contains no decimals, no decimal point is displayed (that is, the administered decimal point is ignored for charge information received with no decimals). On a QSIG trunk group, unlike other trunk groups, the **Decimal Point** field does not drive whether a decimal point appears on the calling display. Instead, it tells what symbol should be displayed if the QSIG AOC received has a 1/10 or 1/100 or 1/1000 Multiplier.

| Valid Entry | Usage   |
|-------------|---|
| comma       | If the received charge contains decimals, the charge is displayed at the calling endpoint's display with a comma as the decimal point. Divides the charge value by 100.                       |
| period      | This is the default. If the received charge contains decimals, the charge is displayed at the calling endpoint's display with a period as the decimal point. Divides the charge value by 100. |
| none        | No decimal point is displayed.  |

### **Related topics:**

[Charge Advice](#) on page 723

[Direction](#) on page 724

[Trunk Direction](#) on page 825

## DS1 Echo Cancellation

Enables or disables echo cancellation on a per port basis. If enabled, reduces voice call echo.

### **Note:**

Changes to the DS1 Echo Cancellation field do not take effect until one of the following occurs:

- Port is busied-out or released.
- Trunk group is busied-out or released.
- SAT command test trunk group is performed.
- Periodic maintenance runs.

## DSN Term

Enables or disables the trunk group as a DSN termination telephone. The default is disabled.

## Format

Specifies the encoding of Numbering Plan Indicator for identification purposes in the Calling Number and/or Connected Number IEs, and in the QSIG Party Number.

Available only if **Send Calling Number** or **r** or the **Send Connected Number** is enabled or restricted.

| Valid Entry | Usage  |
|-------------|--|
| public      | Indicates that the number plan according to CCITT Recommendation E.164 is used.                                      |
| unknown     | Indicates the <b>Numbering Plan Indicator</b> is unknown.  |
| private     | Indicates the <b>Numbering Plan Indicator</b> is PNP.  |
| unk-pvt     | Determines the type of number from the private numbering format, but the <b>Numbering Plan Indicator</b> is unknown. |

**Related topics:**

[Send Calling Number](#) on page 745

[Send Connected Number](#) on page 746

Glare Handling

Determines the reaction of Communication Manager to glare.

The following circuit packs can detect glare:

- TN767 (all releases)
- TN760C (or later releases)
- TN464C (or later releases)

Available only for two-way trunks when the outgoing side of the **Trunk Type** is either .../wink or .../delay.

| Valid Entry | Usage   |
|-------------|---|
| control     | Communication Manager seizes the trunk and proceeds with call setup. The other switch finds another trunk.          |
| backoff     | The other server or switch seizes the trunk and proceeds with call setup. The server or switch finds another trunk. |
| none        | Not administered.   |

**Related topics:**

[Direction](#) on page 724

[Trunk Type](#) on page 826

Hold/Unhold Notifications

If enabled, hold and unhold messages are sent over the isdn trunk when a user places a call on hold/unhold. Default is enabled.

Available only for isdn trunk groups.

**Related topics:**

[Group Type](#) on page 725

## Incoming Tone (DTMF) ANI

Digits received through Automatic Number Identification (ANI) are printed on a CDR record, passed to the INTUITY AUDIX and ASAI interfaces, and displayed on the telephone (and on tandem calls if the outgoing trunk requires ANI). Then the digits are sent to the outgoing trunk.

Available only if the **Incoming Dial Type** is tone.

| Valid Entry | Usage  |
|-------------|--|
| *ANI*DNIS*  | If 555-3800 calls extension 81120, the trunk group receives *55538000*81120*. The telephone displays Call from 555-3800. |
| ANI*DNIS*   | If 555-3800 calls extension 81120, the trunk group receives 55538000*81120*. The telephone displays Call from 555-3800.  |
| no          | Not administered.  |

**Related topics:**

[Incoming Dial Type](#) on page 1001

## Internal Alert

Indicates if internal ringing and coverage is used for incoming calls.

## Long Holding Time (hours)

Available only if Automatic Circuit Assurance measurements are taken for the trunk group.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 10     | The number of hours that the system considers a long holding time. A value of 0 indicates that the system does not consider long holding calls. |

**Related topics:**

[ACA Assignment](#) on page 738

## Maintenance Tests

Enables or disables hourly maintenance tests on this trunk group.

Available only for aplt, isdn, sip, or tie trunk groups.

**Related topics:**

[Group Type](#) on page 725

## Measured

Indicates if the system transmits data for this trunk group to the Call Management System.

| Valid Entry | Usage   |
|-------------|---|
| internal    | Sends the data to the Basic Call Management System (BCMS), the VuStats data display, or both.<br>Available only if <b>BCMS (Basic)</b> or <b>VuStats</b> is enabled for the system. |
| external    | Sends the data to the CMS.  |

## Managing inventory

| Valid Entry | Usage   |
|-------------|---|
| both        | Collects data internally and sends it to the CMS.<br>Available only if <b>BCMS (Basic)</b> or <b>VuStats</b> is enabled for the system. |
| none        | Trunk group measurement reports are not required.   |

### Related topics:

[BCMS \(Basic\)](#) on page 950

[VuStats](#) on page 953

## MF Tariff Free

If enabled, Communication Manager generates an MFC Tariff-Free Backward Signal during call setup instead of the “free” signal. This aids local telephone company central office billing.

Available only for Access, APLT, DID, DIOD, DMI-BOS, and Tandem trunk groups when the **Incoming Dial Type** is mf or for tie trunk groups when the **Trunk Signaling Type** is blank, cont, or dis, and the **Incoming Dial Type** is mf.

### Related topics:

[Group Type](#) on page 725

[Trunk Signaling Type](#) on page 990

[Incoming Dial Type](#) on page 1001

## Modify Tandem Calling Number

Appears when the **Group Type** field is sip. Available with outgoing or two-way trunks.

| Valid Entry      | Usage   |
|------------------|---|
| natl-intl-prefix | Adds the national or international prefixes from the Feature Related System Parameters screen when the calling party number is appropriate. |
| tandem-cpn-form  | Modifies the calling party number IE in the previously administered format specified for the Tandem Calling Party Number.                   |
| no               | Does not modify the calling party number.   |

### Related topics:

[Modify Tandem Calling Number](#) on page 742

## Network Call Redirection

| Valid Entry     | Usage   |
|-----------------|---|
| deflect         | Allows Network Call Deflection.                           |
| ANSI-transfer   | Allows Network Call Transfer for MCI DEX 600 ISDN trunks. |
| Nortel-transfer | Allows Network Call Transfer for MCI DMS 250 switches.    |

| Valid Entry    | Usage   |
|----------------|---|
| telcordia-tbct | Allows Network Call Transfer for Lucent 5ESS or Nortel DMS100 switches. |

### Outgoing ANI

The digit string sent in place of normal ANI. Overrides the normal ANI if this trunk group is used for an outgoing call with ANI. The ANI is sent exactly as administered, except for the normal truncation to seven digits for Russian ANI. This ANI override works both for calls originated in Communication Manager and calls tandemed through it. Accepts up to 15 digits.

Available only for CO, DIOD, FX, and WATS trunk groups.

### Path Replacement Method

Available only if the **Group Type** is ISDN, the **Supplementary Service Protocol** is b or e, and **Supplementary Services with Rerouting** or **DCS with Rerouting** is enabled for the system. Not available if **Path Replacement with Retention** is enabled.

| Valid Entry       | Usage  |
|-------------------|--|
| always            | Use any QSIG (SSB) trunk group as the replacement trunk group. A new call is always originated, even when the original trunk group is determined to be the replacement trunk group.  |
| BR (better route) | Route pattern preferences help determine trunk group path replacement. The original trunk group is retained if <b>Path Replacement with Retention</b> is enabled. Path replacement fails (and the original trunk group is retained) if <b>Path Replacement with Retention</b> is disabled. |

### Related topics:

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

[Path Replacement with Retention](#) on page 750

[DCS with Rerouting](#) on page 945

[Supplementary Services with Rerouting](#) on page 955

### Path Replacement with Retention

Available only if the **Group Type** is ISDN, the **Supplementary Service Protocol** is b or e, and **Supplementary Services with Rerouting** or **DCS with Rerouting** is enabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| y           | Retains the original trunk group.  |
| n           | Allows path replacement according to settings for the <b>Path Replacement Method</b> . |

### Related topics:

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 737

## Managing inventory

[DCS with Rerouting](#) on page 945

[Supplementary Services with Rerouting](#) on page 955

## PBX ID

| Valid Entry      | Usage   |
|------------------|---|
| 1 to 63<br>blank | Identifies the remote switch in the network with which the trunk communicates on a DCS signaling link. Available only for trunks that are used for DCS. |

### Related topics:

[Used for DCS](#) on page 1023

## Per Call CPN Blocking Code

## Per Call CPN Unblocking Code

## Precedence Incoming

Available only when the trunk group is a DSN termination telephone and the trunk group type is tie.

| Valid Entry | Usage   |
|-------------|---|
| digit       | Precedence level for dual-tone multifrequency (DTMF) or tone trunks is received as digits (rotary pulses).    |
| dtmf (a-d)  | Precedence level for dual-tone multifrequency (DTMF) or tone trunks is received as DTMF signals (touchtones). |

### Related topics:

[Group Type](#) on page 725

[DSN Term](#) on page 741

## Precedence Outgoing

Available only when the trunk group is a DSN termination telephone and the trunk group type is tie.

| Valid Entry | Usage   |
|-------------|---|
| digit       | Precedence level for dual-tone multifrequency (DTMF) or tone trunks is sent as digits (rotary pulses).    |
| dtmf (a-d)  | Precedence level for dual-tone multifrequency (DTMF) or tone trunks is sent as DTMF signals (touchtones). |

## R2 MFC Signaling

Available only if:

- **Multinational Locations** is enabled for the system
- **Outgoing Dial Type** is mf

- **Incoming Dial Type** or **Outgoing Dial Type** is rotary
- **Country** code is 15 (Russia)

| Valid Entry | Usage  |
|-------------|--|
| 1 to 8      | The MFC signaling parameters set used by this trunk group. |

**Related topics:**

[Country](#) on page 822

[Outgoing Dial Type](#) on page 824

[Multinational Locations](#) on page 948

[Incoming Dial Type](#) on page 1001

**Receive Analog Incoming Call ID**

Enables or disables the collection of incoming call ID information on analog trunks. Fifteen characters of name and number information associated with an incoming call (ICLID, or incoming call line identification information) is stored and displays.

Available for CO, DID, and DIOD trunk groups when **Analog Trunk Incoming Call ID** is enabled. The trunk must be incoming or two-way.

| Valid Entry | Usage   |
|-------------|---|
| Bellcore    | Collects ICLID information in the U.S.  |
| NTT         | Collects ICLID information in Japan.  |
| disabled    | Stops the collection of ICLID information on analog trunks.                                       |
| V23–Bell    | For Telcordia Technologies protocol with V.23 modem tones. Used in Bahrain and similar countries. |

**Related topics:**

[Direction](#) on page 724

[Analog Trunk Incoming Call ID](#) on page 942

**Replace Unavailable Numbers**

If enabled, replaces unavailable numbers with administrable strings for incoming and outgoing calls assigned to the specified trunk group. Applies to BRI/PRI, H.323, and SIP Enablement Services (SES) trunks. Also applies to analog trunks if **Analog Trunk Incoming Call ID** is enabled for the system and **Receive Analog Incoming Call ID** for the trunk is set to any value except disabled.

Available only if the group type is isdn or sip.

**Related topics:**

[Group Type](#) on page 725

[Analog Trunk Incoming Call ID](#) on page 942

[Receive Analog Incoming Call ID](#) on page 1017

### Request Category

Indicates if Communication Manager should request a call category from the local telephone company central office (CO).

Available only if the **Country** code is 15 and MF shuttle signaling is enabled.

#### Related topics:

[Country](#) on page 822

[Shuttle](#) on page 1022

### Seize When Maintenance Busy

Indicates whether this server generates an outgoing seizure when a trunk in this trunk group is maintenance busied and whether the far-end server or switch is administered to do likewise. This supports the Electronic Tandem Network Busyout feature, which is intended to prevent a far-end server or switch from reporting problems with a trunk that has been removed from service. This field does not affect the behavior of the far-end server or switch. It controls the behavior of your server and defines the expected far-end behavior.

This field only affects ports on TN760C (or later release), TN767, and TN464C (or later release) circuit packs. For DIOD trunks using TN464F (or later release) or TN2464 circuit packs, available only for diod trunk groups when the **Trunk Signaling Type** is pulsed, cont, or dis.

| Valid Entry | Usage   |
|-------------|---|
| near-end    | Communication Manager generates an outgoing seizure when a trunk is maintenance busied, but the far-end server or switch does not. The seizure is maintained until the maintenance busyout is released. |
| far-end     | The far-end server or switch generates an outgoing seizure when a trunk is maintenance busied, but this server running Communication Manager does not.  |
| both-ends   | Both this server running Communication Manager and the far-end server or switch generate an outgoing seizure when a trunk is maintenance busied.  |

If a server generates an outgoing seizure when a trunk is busied out, the seizure will probably cause alarms at the far-end server or switch, perhaps leading to a far-end maintenance busy out, unless the far-end server or switch is administered to expect this behavior.

If the administered value of this field is either far-end or both-ends, any abnormally long incoming seizure (including failure to drop from a completed call) is assumed to be the result of a far-end maintenance busy condition. This assumption might be incorrect, since the abnormally long seizure might actually be due to failure of the trunk circuit.

#### Related topics:

[Group Type](#) on page 725

[Trunk Signaling Type](#) on page 990

**Send Called/Busy/Connected Number**

Specifies if the dialed number, whether called (ringing), busy (busy tone), or connected (answered) is sent on incoming or tandemed ISDN calls.

Available only if **QSIG Value-Added** is enabled for the trunk group.

| Valid Entry | Usage   |
|-------------|---|
| y           | The dialed number is sent on incoming or tandemed ISDN calls. This field must be enabled in order for the Calling Party Number of an incoming ISDN call to display at the transferred-to station after a QSIG transfer operation. If enabled, the Numbering - Public/Unknown Format is accessed to construct the actual number sent, or the Numbering - Private Format is used. |
| n           | Disables the sending of the dialed number on incoming or tandemed ISDN calls.   |
| r           | Restricted. The connected number is sent "presentation restricted".   |

**Related topics:**

[QSIG Value-Added](#) on page 751

[Numbering-Private Format](#) on page 813

[Numbering — Public/Unknown Format](#) on page 814

**Send Calling Number**

Specifies whether the calling party's number is sent on outgoing or tandemed ISDN calls.

**Note:**

The Numbering - Public/Unknown Format can override the Send Calling Number administration

| Valid Entry | Usage  |
|-------------|--|
| y           | The calling party's number is sent on outgoing or tandemed ISDN calls. If enabled, the Numbering - Public/Unknown Format is accessed to construct the actual number sent, or the Numbering - Private Format is used. |
| n           | Disables the sending of the calling party's number on outgoing or tandemed ISDN calls. If disabled, an incoming number is not tandemed out again. This applies to all Supplementary Service Protocols.               |
| r           | Restricted. The calling number is sent "presentation restricted". If set to restricted, an incoming number is marked restricted when it is tandemed out again. This applies to all Supplementary Service Protocols.  |

**Related topics:**

[Number Format](#) on page 721

[Numbering-Private Format](#) on page 813

[Numbering — Public/Unknown Format](#) on page 814

Send Connected Number

Specifies if the connected party's number is sent on incoming or tandemed ISDN calls.

Available only if **QSIG Value-Added** is disabled for the trunk group.

| Valid Entry | Usage   |
|-------------|---|
| y           | The connected party's number is sent on outgoing or tandemed ISDN calls. If enabled, the Numbering - Public/Unknown Format is accessed to construct the actual number sent, or the Numbering - Private Format is used. This field must be enabled for the Calling Party Number of an incoming ISDN call to display at the transferred-to station after a QSIG transfer operation. |
| n           | Disables the sending of the connected party's number on outgoing or tandemed ISDN calls. If disabled, an incoming number is not tandemed out again. This applies to all Supplementary Service Protocols.  |
| r           | Restricted. The connected number is sent "presentation restricted". If this field is set to r, an incoming number is marked restricted when it is tandemed out again. This applies to all Supplementary Service Protocols.  |

 **Note:**

The AT&T Switched Network Protocol does not support restricted displays of connected numbers. Therefore, if you administer the 1a country-protocol/ protocol-version combination for the DS1 Circuit Pack, you should not administer the Send Connected Number as restricted, as this causes display problems. The Numbering - Public/Unknown Format overrides the Send Connected Number administration for any administrable block of extensions.

**Related topics:**

[QSIG Value-Added](#) on page 751

[Numbering-Private Format](#) on page 813

[Numbering — Public/Unknown Format](#) on page 814

Send EMU Visitor CPN

Controls which calling party identification (extension of the primary telephone or extension of the visited telephone) is used when a call is made from a visited telephone. There are areas where public network trunks disallow a call if the calling party information is invalid. In this case, there can be instances where the extension of the primary telephone is considered invalid and the extension of the visited telephone must be used.

| Valid Entry | Usage  |
|-------------|--|
| y           | Sends calling party identification information on the extension of the EMU user's telephone. |
| n           | Sends calling party identification information on the primary telephone.                     |

## Send Name

Specifies whether the calling, connected, called, or busy party's administered name is sent to the network on outgoing or incoming calls. Available only for isdn or sip trunk groups.

| Valid Entry    | Usage  |
|----------------|--|
| y              | When the <b>Supplementary Service Protocol</b> is e (DCS with Rerouting), only values of y and n are permitted.  |
| n              | When the <b>Supplementary Service Protocol</b> is e (DCS with Rerouting), only values of y and n are permitted.  |
| r (restricted) | The calling/connected name will be sent by Communication Manager, but will be marked "presentation restricted". This value is valid only if the <b>Supplementary Service Protocol</b> is a (national supplementary service), b (for called/busy only), or d for the QSIG Global Networking Supplementary Service Protocol. |

 **Note:**

If name information is not administered for the calling station or the connected, called, or busy station; the system sends the extension number instead of the name.

**Related topics:**

[Group Type](#) on page 725

[Supplementary Service Protocol](#) on page 1005

## Short Holding Threshold

Available only if Automatic Circuit Assurance measurements are taken for this trunk group.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 30     | The number of times the system will record a short holding call before alerting an attendant to the possibility of a faulty trunk.<br>If 0 is entered, no short holding calls are recorded. |

**Related topics:**

[ACA Assignment](#) on page 738

## Short Holding Time (seconds)

Available only if Automatic Circuit Assurance measurements are taken for this trunk group.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 160    | The length of time that the system considers as being a short holding time.<br>If 0 is entered, the system does not consider short holding calls. |

**Related topics:**

[ACA Assignment](#) on page 738

## Managing inventory

### Show ANSWERED BY on Display

Available only for isdn pri/bri and sip trunk groups.

| Valid Entry | Usage  |
|-------------|--|
| y           | The words “ANSWERED BY” display in addition to the connected telephone number on calls over this trunk. This is the default.<br> <b>Note:</b><br>Based on display language settings for stations, “ANSWERED BY” is translated into and displayed in the appropriate language. |
| n           | Only the connected telephone number displays. This might be preferred when outgoing calls are over a trunk that might be redirected.   |

### Shuttle

Enables or disables MF shuttle signaling. It can be administered on TN464D (or later release) or TN2199 circuit packs.

Available only for co, fx, or wats trunk groups, with a **Country** code of 15, when the **Outgoing Dial Type** is rotary.

#### Related topics:

[Group Type](#) on page 725

[Country](#) on page 822

[Outgoing Dial Type](#) on page 824

### Signaling Group

The signaling group number.

### Start B Signal

Indicates which B-signal should be used to start a call. The value administered in this field must be coordinated with the local telephone company central office.

Available only when the **Country** code is 15 and MF shuttle signaling is enabled.

| Valid Entry | Usage  |
|-------------|--|
| 1           | Start calls with signal B1 (first digit).    |
| 2           | Start calls with signal B2 (next digit).     |
| 3           | Start calls with signal B3 (previous digit). |

#### Related topics:

[Country](#) on page 822

[Shuttle](#) on page 1022

### Start Position

Available only when the **Country** code is 15 and MF shuttle signaling is enabled.

| Valid Entry | Usage  |
|-------------|--|
| 1 to 9      | Indicates which digit in the digit string is considered to be the “previously sent” digit. The value administered in this field must be coordinated with the local telephone company central office. |

**Related topics:**

[Country](#) on page 822

[Shuttle](#) on page 1022

**Suppress # Outpulsing**

Indicates whether or not to suppress the final “#” in cases where the system would normally outpulse it. Used if end-to-end signaling begins with (and includes) “#”. This field should be enabled when the local telephone company central office or any other facility treats “#” as an error.

**Time (sec) to Drop Call on No Answer**

Available only for co or diod trunk groups when the **Outgoing Dial Type** is mf, or for co, diod, fx, or wats trunk groups when the **Country** code is 15.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 1200   | The duration in seconds that Communication Manager should wait for outgoing calls to be answered. If the call is not answered in the specified number of seconds, the call drops.<br>If 0 is entered, the timer is not set and no calls drop. |

**Related topics:**

[Group Type](#) on page 725

[Country](#) on page 822

[Outgoing Dial Type](#) on page 824

**Used for DCS**

If enabled, this trunk group sends and receive messages on a DCS signaling link.

 **Note:**

This field cannot be enabled if the trunk group number is greater than 255 or if the Trunk Access code is more than 3 digits long.

**Related topics:**

[Group Type](#) on page 860

[TSC Supplementary Service Protocol](#) on page 869

[DCS with Rerouting](#) on page 945

[ISDN-BRI Trunks](#) on page 947

[ISDN-PRI](#) on page 947

**Used Only for Paging**

Indicates whether or not this trunk is used only for paging. Default is disabled.

Available only for wats trunk groups when **Port Network Support** is disabled for the system.

**Related topics:**

[Group Type](#) on page 725

[Port Network Support](#) on page 949

Voice Paging Timeout (sec)

Available only if the trunk is used only for paging.

| Valid Entry | Usage   |
|-------------|---|
| 10 to 6000  | The number of seconds before a paged trunk call drops. Default is 10. |

**Related topics:**

[Used Only for Paging](#) on page 1023

Wideband Support

 **Note:**

This feature is not supported on the DS1 interfaces on H.248 gateways (G700/G350).

Enables or disables wideband switching on this trunk group. Only trunk members from TN464C or later circuit packs can use wideband switching.

Available only if **Wideband Switching** is enabled for the system.

 **Note:**

Wideband trunk calls are treated as a single trunk call when Automatic Circuit Assurance (ACA) measurements are taken. This way, if an ACA referral call is generated (for short or long holding time), the wideband call only triggers a single referral call using the lowest B-channel trunk member associated with the wideband channel.

**Related topics:**

[Wideband Switching](#) on page 950

**Administrable Timers**

This screen might not appear for all trunk group types.

 **Caution:**

Customers: Do not change fields on this page without assistance from Avaya or your network service provider.

**Answer Send (msec)**

Available only for incoming or two-way trunk groups when the **Trunk Type** is dis. Only TN2140 and TN2199 ports receive this timer.

| Valid Entry                    | Usage                                    |
|--------------------------------|--|
| 10 to 2550 in increments of 10 | The duration of the answer signal pulse. |

**Related topics:**

[Direction](#) on page 724

[Trunk Type](#) on page 826

***Busy Tone Disconnect***

If enabled, Communication Manager recognizes a busy tone signal as a disconnect on this trunk group.

Available only if **Enable Busy Tone Disconnect for Analog loop-start Trunks** is enabled for the system country options.

**Related topics:**

[Enable Busy Tone Disconnect for Analog Loop-start Trunks](#) on page 938

***Cama Outgoing Dial Guard (msec)***

Available only for cama trunk groups (the trunk group type used for emergency 911 service).

| Valid Entry                    | Usage  |
|--------------------------------|--|
| 25 to 6375 in increments of 25 | Minimum interval between the seizure acknowledgment on the receiving server or switch and the outpulsing of digits by this server. |

**Related topics:**

[Group Type](#) on page 725

***Cama Wink Start Time (msec)***

Available only for cama trunk groups.

| Valid Entry                    | Usage   |
|--------------------------------|---|
| 20 to 5100 in increments of 20 | The duration (the wait-for-wink-to-end time) for a wink-start CAMA trunk. The wink must begin before the Outgoing Seizure Response timer expires. |

**Related topics:**

[Group Type](#) on page 725

***Disconnect Signal Error (sec)***

Available only for ground-start trunk groups.

| Valid Entry                 | Usage  |
|-----------------------------|--|
| 1 to 255 in increments of 1 | The maximum interval that Communication Manager waits to receive a disconnect signal from the far-end after the local party (a telephone or tie trunk) goes on-hook. If the timer expires, Communication Manager assumes a disconnect failure. |

**Flash Length (msec)**

| Valid Entry                    | Usage  |
|--------------------------------|--|
| 10 to 2550 in increments of 10 | The duration of a flash signal generated toward the local telephone company central office. This timer is sent to TN436B, TN459B, TN464C (or later), TN465B (or later), TN753 (if <b>Country</b> code is 23), TN2146, TN2147, TN2184, and TN2199 circuit boards. |

**Glare**

Available only for two-way or outgoing trunk groups when the **Trunk Type** is cont. Only TN2140 ports receive this timer.

| Valid Entry                   | Usage   |
|-------------------------------|---|
| 40 to 100 in increments of 10 | The minimum acceptable interval between the moment your server running Communication Manager sends an outgoing seizure and the moment it receives a seizure acknowledgment. If acknowledgment is received before the timer expires, glare is assumed. |

**Related topics:**

[Direction](#) on page 724

[Trunk Type](#) on page 826

**Incoming Dial Guard (msec)**

| Valid Entry                    | Usage  |
|--------------------------------|--|
| 10 to 2550 in increments of 10 | The minimum acceptable interval between the detection of an incoming seizure and the acceptance of the first digit. Communication Manager does not accept digits before this timer expires. This timer is never sent to TN429 ports. |

**Incoming Disconnect (msec)**

Available only for incoming or two-way trunk groups when the **Trunk Type** is blank or cont.

| Valid Entry                    | Usage  |
|--------------------------------|--|
| 50 to 2550 in increments of 10 | The minimum valid duration of a disconnect signal for an incoming call. Communication Manager does not recognize shorter disconnect signals. This field cannot be blank. For Brazil pulsed E&M signaling, use 600. |

**Related topics:**

[Direction](#) on page 724

[Trunk Type](#) on page 826

**Incoming Disconnect Send (msec)**

Available only for incoming or two-way trunk groups when the **Trunk Type** is dis. Only TN2140 ports receive this timer.

| Valid Entry                      | Usage  |
|----------------------------------|--|
| 500 to 1200 in increments of 100 | The duration of the backward release signal the server running Communication Manager sends at the end of an incoming call. |

**Related topics:**

[Direction](#) on page 724

[Trunk Type](#) on page 826

***Incoming Glare Guard (msec)***

Available only for two-way trunk groups.

| Valid Entry                       | Usage   |
|-----------------------------------|---|
| 100 to 25500 in increments of 100 | The minimum interval that must elapse between a trunk's release from an incoming call and its seizure for an outgoing call. This delay gives the far-end time to release all equipment after the trunk is released. This field cannot be blank. |

**Related topics:**

[Direction](#) on page 724

***Incoming Incomplete Dial Alarm (sec)***

| Valid Entry                 | Usage  |
|-----------------------------|--|
| 1 to 255 in increments of 1 | The maximum acceptable interval between an incoming seizure and receipt of all digits. Intervals greater than this limit generate an inline error. Only the TN436 (all), TN459 (all), TN464C (or later), TN767, TN2140, TN2146, TN2184, TN2199, and TN2242 circuit packs use this timer. |

***Incoming Partial Dial (sec)***

Available only if the **Incoming Dial Type** is rotary. This timer is never sent to TN429 ports.

| Valid Entry                 | Usage  |
|-----------------------------|--|
| 5 to 255 in increments of 1 | The maximum time allowed between incoming rotary digits. |

**Related topics:**

[Incoming Dial Type](#) on page 1001

***Incoming Seizure (msec)***

Available only for incoming or two-way trunk groups, and, when applicable, the **Trunk Type** is cont. Only TN429, TN438 (any release), TN 447, TN464C (or later), TN465 (any release), TN767, TN2138, TN2140, TN2147, TN2184, and TN2199 ports receive this timer. For DID trunks, only TN2199 and TN429D (or later) receive this timer.

| Valid Entry                    | Usage   |
|--------------------------------|---|
| 20 to 2550 in increments of 10 | The duration of the shortest incoming seizure signal the server running Communication Manager can recognize. For ICLID, set this field to 120. The field cannot be blank. |

**Related topics:**

[Direction](#) on page 724

[Trunk Type](#) on page 826

**Normal Outgoing Seize Send (msec)**

Available only for two-way or outgoing trunk groups when the **Trunk Type** is dis. Only TN2140 ports receive this timer.

| Valid Entry                   | Usage  |
|-------------------------------|--|
| 10 to 990 in increments of 10 | The duration of the signal the server running Communication Manager sends for an outgoing seizure. |

**Related topics:**

[Direction](#) on page 724

[Trunk Type](#) on page 826

**Outgoing Dial Guard (msec)**

| Valid Entry                       | Usage  |
|-----------------------------------|--|
| 100 to 25500 in increments of 100 | The minimum interval between seizure acknowledgment of a trunk and the outpulsing of digits. For trunks that do not provide seizure acknowledgment, the timer specifies the minimum time between seizure and the outpulsing of digits. Any digit the caller dials after lifting the receiver, but before the timer expires, is not outpulsed until the timer expires.<br>This field cannot be blank. |

**Outgoing Disconnect (msec)**

| Valid Entry                    | Usage  |
|--------------------------------|--|
| 50 to 2550 in increments of 10 | The minimum valid duration of a disconnect signal for an outgoing call. Communication Manager does not recognize shorter disconnect signals. This timer begins timing when a disconnect signal is detected on an outgoing call and resets when the signal is no longer detected. If the timer expires, the trunk drops.<br>This field cannot be blank. For Brazil pulsed E&M signaling, use 600. |

**Outgoing Disconnect Send (msec)**

Available only for two-way or outgoing trunk groups when the **Trunk Type** is dis. Only TN2140 ports receive this timer.

| Valid Entry                      | Usage   |
|----------------------------------|---|
| 100 to 9900 in increments of 100 | The duration of the forward release signal the server running Communication Manager sends at the end of outgoing calls. |

**Related topics:**

[Direction](#) on page 724

[Trunk Type](#) on page 826

**Outgoing End of Dial (sec)**

Available for outgoing or two-way trunk groups when the network does not provide answer supervision.

| Valid Entry                 | Usage   |
|-----------------------------|---|
| 1 to 254 in increments of 1 | <p>The maximum time Communication Manager waits to receive answer supervision for outgoing calls on the ports controlled by firmware timers. Controls firmware answer supervision timers on circuit packs that have them.</p> <p>During a cut-through operation, timing begins after Communication Manager sends each outgoing digit and ceases when answer supervision is received. If the timer expires, Communication Manager acts as if it has received answer supervision. On senderized operation, the timer begins after the switch sends the last digit collected. The timer ceases when answer supervision is received. If the timer expires, Communication Manager acts as if it has received answer supervision.</p> <p>For Brazil pulsed E&amp;M signaling, use 40.</p> |

**Related topics:**

[Direction](#) on page 724

[Receive Answer Supervision](#) on page 825

**Outgoing Glare Guard (msec)**

Available only for outgoing and two-way trunk groups.

| Valid Entry                       | Usage   |
|-----------------------------------|---|
| 100 to 25500 in increments of 100 | The minimum interval that must elapse between a trunk's release from an outgoing call and its seizure for another outgoing call. This delay gives the far-end time to release all equipment after the outgoing trunk is released. This field cannot be blank. |

**Related topics:**

[Direction](#) on page 724

**Outgoing Last Digit (sec)**

Available only for two-way or outgoing trunk groups when the **Trunk Type** is dis or cont. Only TN497 and TN2140 ports receive this timer.

| Valid Entry                | Usage  |
|----------------------------|--|
| 1 to 40 in increments of 1 | The maximum time that Communication Manager waits for the next digit dialed. After the timer expires, no more digits are accepted by the circuit pack. |

**Related topics:**

[Direction](#) on page 724

[Trunk Type](#) on page 826

**Outgoing Rotary Dial Interdigit (msec)**

Available only if:

- The trunk **Group Type** is access, aplt, co, diod, dmi-bos, fx, rlt, tandem, or wats, and the **Outgoing Dial Type** is rotary.
- The trunk **Group Type** is tie, the **Trunk Type** is blank, cont, or dis, and the **Outgoing Dial Type** is rotary.
- The trunk **Group Type** is tie, and the **Trunk Type** is tge, tgi, or tru.

| Valid Entry                     | Usage  |
|---------------------------------|--|
| 150 to 2550 in increments of 10 | The minimum time between outpulsed digits on outgoing rotary trunks. |

**Related topics:**

[Group Type](#) on page 725

[Outgoing Dial Type](#) on page 824

[Trunk Type](#) on page 826

**Outgoing Seizure (msec)**

Available only if the **Country** code is 15, for outgoing or two-way trunk groups, when the **Trunk Type** is 2-wire-ac, 2-wire-dc, or 3-wire. This timer is sent only to the TN2199 circuit pack.

| Valid Entry                    | Usage  |
|--------------------------------|--|
| 20 to 2550 in increments of 10 | The duration of the outgoing seizure signal. |

**Related topics:**

[Direction](#) on page 724

[Country](#) on page 822

[Trunk Type](#) on page 826

**Outgoing Seizure Response (sec)**

| Valid Entry                 | Usage   |
|-----------------------------|---|
| 1 to 255 in increments of 1 | The maximum interval that Communication Manager waits after sending a seizure signal to receive seizure acknowledgment from the far-end. If |

| Valid Entry | Usage   |
|-------------|---|
|             | the acknowledgment is not received in this time, a seizure failure response is uplinked. This timer is sent to the TN438B, TN439, TN447, TN458, TN464B (or later), TN465B (or later), TN767, TN2140, TN2147, TN2184, TN2199, and TN2242 circuit packs.<br>For Brazil pulsed E&M signaling, use 255. |

### ***Programmed Dial Pause (msec)***

| Valid Entry                       | Usage   |
|-----------------------------------|---|
| 100 to 25500 in increments of 100 | The exact duration of the pause used during abbreviated dialing, ARS outpulsing, and terminal dialing operations. This timer is administrable for all outgoing and two-way trunk groups. This timer works with the TN464B (or later), TN767, TN458, TN2140, and TN2242 tie circuit packs. All central office (CO) circuit packs that accept administrable timers accept this timer. |

### ***Release Ack Send (msec)***

Available only for incoming and two-way trunk groups when the **Trunk Type** is dis. Only TN2140 ports receive this timer.

| Valid Entry                      | Usage   |
|----------------------------------|---|
| 500 to 1200 in increments of 100 | The duration of the signal the server running Communication Manager sends for a forward release acknowledgment. After the server running Communication Manager receives a forward release signal, it must send a forward release acknowledgment signal. |

### **Related topics:**

[Direction](#) on page 724

[Trunk Type](#) on page 826

### ***Ringling Monitor (msec)***

| Valid Entry                       | Usage  |
|-----------------------------------|--|
| 200 to 51000 in increments of 200 | The minimum time Communication Manager requires to determine if a trunk disconnects. If the ringing signal disappears for a duration longer than the time specified in this field, Communication Manager assumes the call has been disconnected. This timer is sent to TN464C (or later), TN767, TN438 (all), TN447, TN465 (all), TN2138, TN2147, TN2184, and TN2199 CO circuit packs.<br>The field cannot be blank. |

### ***Seize Ack Delay (msec)***

Available only for incoming or two-way trunk groups if the **Trunk Type** is dis. Only TN2140 ports receive this timer.

| Valid Entry                   | Usage  |
|-------------------------------|--|
| 40 to 120 in increments of 10 | The maximum interval the server running Communication Manager waits after receipt of an incoming seizure to send seizure acknowledgment. |

**Related topics:**

[Direction](#) on page 724

[Trunk Type](#) on page 826

**Seize Ack Send (msec)**

Available only for incoming or two-way trunk groups if the **Trunk Type** is dis. Only TN2140 ports receive this timer.

| Valid Entry                   | Usage  |
|-------------------------------|--|
| 10 to 990 in increments of 10 | The duration of the seizure acknowledgment signal the server running Communication Manager sends in response to an incoming seizure. |

**Related topics:**

[Direction](#) on page 724

[Trunk Type](#) on page 826

**Send Incoming/Outgoing Disconnect Timers to TN465 Ports**

If enabled, the incoming disconnect and outgoing disconnect timer values are sent to the trunk group ports that are on a TN465 board. Available only for a co, fx, or wats trunk group.

**END TO END SIGNALING**

Pause (msec)

Available only if the **Trunk Type** is blank.

| Valid Entry                    | Usage   |
|--------------------------------|---|
| 20 to 2550 in increments of 10 | The interval (pause) between DTMF tones sent from a hybrid telephone. All CO, DIOD, and tie circuit packs that accept administrable timers accept this timer. However, this timer is sent only to the following circuit packs: TN464B (or later), TN767, TN436B, TN459B, TN2146, TN2199, and TN2242, and TN429 and TN2184 ports in a DID trunk group. |

**Related topics:**

[Trunk Type](#) on page 826

Tone (msec)

Available only if the **Trunk Type** is blank.

| Valid Entry                    | Usage   |
|--------------------------------|---|
| 20 to 2550 in increments of 10 | The duration of the DTMF tone sent when a button on a hybrid telephone is pressed. All CO, DIOD, and Tie circuit packs that accept administrable timers accept this timer. This timer is also sent to the following circuit |

| Valid Entry | Usage  |
|-------------|--|
|             | packs: TN464B (or later), TN767, TN436B, TN459B, TN2146, TN2199, TN429, TN2184 ports in a DID trunk group. |

**Related topics:**

[Trunk Type](#) on page 826

**OUTPULSING INFORMATION**

## Break (msec)

The duration of the break interval (the pulse duration) while the system is outpulsing digits using dial pulse signaling. The field cannot be blank.

| Valid Entry                 | Usage   |
|-----------------------------|---|
| 20 to 80 in increments of 5 | If the <b>PPS</b> (pulses per second) value is 10, the sum of the <b>Make (msec)</b> and <b>Break (msec)</b> values must equal 100. |
| 10 to 40 in increments of 5 | If the <b>PPS</b> (pulses per second) value is 20, the sum of the <b>Make (msec)</b> and <b>Break (msec)</b> values must equal 50.  |

**Related topics:**

[Make \(msec\)](#) on page 1034

[PPS](#) on page 1034

## Frequency

Identifies the Periodical Pulse Metering (PPM) pulse frequency, or frequencies, sent by the public network. Circuit packs can detect up to three different frequencies (12kHz, 16kHz, and 50Hz), plus two frequency combinations (50Hz/12kHz and 50Hz/16kHz). This field controls TN465B, TN2138, and TN2184 circuit packs. Available for outgoing or two-way trunk groups if **PPM** is enabled.

| Valid Entry | Usage   |
|-------------|---|
| 12k         | The TN465B (or later) and TN2184 can only detect 12k and 16kHz PPM. Therefore, if 12k is administered, the circuit pack will be set to detect 12kHz.    |
| 16k         | The TN465B (or later) and TN2184 can only detect 12k and 16kHz PPM. Therefore, if 16k is administered, the circuit pack will be set to detect 16kHz.    |
| 50          | The TN465B (or later) and TN2184 can only detect 12k and 16kHz PPM. Therefore, if 50 is administered, the circuit pack will be set to detect 16kHz.     |
| 50/12k      | The TN465B (or later) and TN2184 can only detect 12k and 16kHz PPM. Therefore, if 50/12k is administered, the circuit pack will be set to detect 12kHz. |

| Valid Entry | Usage   |
|-------------|---|
| 50/16k      | The TN465B (or later) and TN2184 can only detect 12k and 16kHz PPM. Therefore, if 50/16k is administered, the circuit pack will be set to detect 16kHz. |

**Related topics:**

[Direction](#) on page 724

[PPM](#) on page 1034

**Make (msec)**

The duration of the make interval (the pause between pulses) while the system is outpulsing digits using dial pulse signaling. The field cannot be blank.

| Valid Entry                 | Usage   |
|-----------------------------|---|
| 20 to 80 in increments of 5 | If the <b>PPS</b> (pulses per second) value is 10, the sum of the <b>Make (msec)</b> and <b>Break (msec)</b> values must equal 100. |
| 10 to 40 in increments of 5 | If the <b>PPS</b> (pulses per second) value is 20, the sum of the <b>Make (msec)</b> and <b>Break (msec)</b> values must equal 50.  |

**Related topics:**

[Break \(msec\)](#) on page 1033

[PPS](#) on page 1034

**PPM**

Determines if Periodical Pulse Metering (PPM) pulses should be collected from the public network to determine call cost. For CO, DIOD, FX, PCOL, and WATS trunks. Available only for outgoing or two-way trunk groups.

**Related topics:**

[Direction](#) on page 724

[Direction](#) on page 724

[Frequency](#) on page 1033

**PPS**

Available only for cama trunk groups.

| Valid Entry | Usage   |
|-------------|---|
| 10<br>20    | The rate (pulses per second) at which outgoing rotary pulses are sent over this trunk group.<br>The TN439, TN458, TN497, TN747Bv12 (or later), and TN767 circuit packs send rotary pulses at 10 pps only. |

**Related topics:**

[Break \(msec\)](#) on page 1033

[Make \(msec\)](#) on page 1034

**Trunk Group: ATMS Thresholds**

Available for outgoing or two-way trunk groups when **ATMS** is enabled for the system.

 **Caution:**

Customers: Do not change fields on this page without assistance from Avaya or your network service provider.

**Related topics:**

[Direction](#) on page 724

[ATMS](#) on page 944

**Far-End Test No**

The access number dialed to reach the terminating test line (TTL). Accepts up to 16 digits.

**Trunk Contact**

The name or telephone number of someone from the trunk vendor who can be contacted if there are problems with the trunks. Accepts up to 25 alphanumeric characters.

**Trunk Length**

This field is not required. Since noise on a trunk increases with the length of the trunk, however, this information might be useful.

| Valid Entry | Usage  |
|-------------|--|
| 0 to 4 k    | The length of the trunk group in kilometers. |
| 0 to 4 m    | The length of the trunk group in miles.      |

**Trunk Vendor**

The name of the vendor providing service over this trunk group that needs to be notified in the event of problems with the trunks in this trunk group. Accepts up to 22 alphanumeric characters.

**TTL Contact**

The name or telephone number of someone from the TTL vendor who can be contacted in the event of problems with the terminating test line. Accepts up to 25 alphanumeric characters.

**TTL Type**

Type of terminating test line (TTL) selected for testing trunks. The TTL type determines what ATMS tests can be completed and thus which threshold values need to be administered.

| Valid Entry | Usage  |
|-------------|--|
| 105-w-rl    | 105 with return loss. Full range of 18 measurements or some defaults for return loss used (56A). |
| 105-wo-rl   | 105 without return loss. Cannot return default values for far-end return loss.                   |
| high-lts    | High-level tone source. Sends a fixed sequence of tones at 0 dBm.                                |

| Valid Entry | Usage   |
|-------------|---|
| low-lts     | Low-level tone source. Sends a fixed sequence of tones at -16dBm.                   |
| 100         | 100 type. Up to 5 measurements that sends a 1004 Hz tone, then a quiet termination. |
| 102         | 102 type. One measurement that sends a 1004 Hz tone.                                |

**TTL Vendor**

The name of the vendor supplying the terminating test line (TTL). Accepts up to 22 alphanumeric characters.

**MARGINAL / UNACCEPTABLE**

Allow ATMS Busyout, Error Logging and Alarming

Enables or disables ATMS error logging and alarming.

Marginal Threshold --Dev - 404 Hz Loss

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9      | The maximum negative deviation of measured loss at 404 Hz from the 1004 Hz test tone noise level (in dB) allowed before reporting a trunk as out of tolerance. Smaller dB values are more restrictive. |

Marginal Threshold +Dev - 404 Hz Loss

| Valid Entry | Usage   |
|-------------|---|
| 0 to 9      | The maximum positive deviation of measured loss at 404 Hz from the 1004 Hz test tone loss level (in dB) allowed before reporting a trunk as out of tolerance. Smaller dB values are more restrictive. |

Marginal Threshold --Dev - 2804 Hz

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9      | The maximum negative deviation of measured loss at 2804 Hz from the 1004 Hz test tone loss level (in dB) allowed before reporting a trunk as out of tolerance. Smaller dB values are more restrictive. |

Marginal Threshold +Dev - 2804 Hz

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9      | The maximum positive deviation of measured loss at 2804 Hz from the 1004 Hz test tone loss level (in dB) allowed before reporting a trunk as out of tolerance. Smaller dB values are more restrictive. |

## Marginal Threshold - Max - 1004 Hz Loss

| Valid Entry | Usage   |
|-------------|---|
| 0 to 21     | The maximum signal loss allowed for a 1004 Hz test tone (in dB) before a trunk is reported as out of tolerance. A smaller dB value is more restrictive. |

## Marginal Threshold - Maximum C Message Noise

| Valid Entry | Usage   |
|-------------|---|
| 15 to 55    | The maximum C-message noise telephone as measured within the voice band frequency range (500 to 2500 Hz) allowed before reporting a trunk as out of tolerance. Smaller values are more restrictive. |

## Marginal Threshold - Maximum C Notched Noise

| Valid Entry | Usage  |
|-------------|--|
| 34 to 74    | The maximum C-notched signal dependent noise interference in dBmC allowed before reporting a trunk as out of tolerance. Smaller values are more restrictive. |

## Marginal Threshold - Min -1004 Hz Loss

| Valid Entry | Usage  |
|-------------|--|
| -2 to 21    | The minimum signal loss allowed for a 1004 Hz test tone (in dB) before a trunk is reported as out of tolerance. A larger dB value is more restrictive. |

## Marginal Threshold - Minimum ERL

| Valid Entry | Usage  |
|-------------|--|
| 0 to 40     | The minimum low-frequency echo return loss in dB allowed before reporting a trunk as out of tolerance. Larger values are more restrictive. |

## Marginal Threshold - Minimum SRL-HI

| Valid Entry | Usage  |
|-------------|--|
| 0 to 40     | The minimum high-frequency signaling return loss in dB allowed before reporting a trunk as out of tolerance. Larger values are more restrictive. |

## Marginal Threshold - Minimum SRL-LO

| Valid Entry | Usage   |
|-------------|---|
| 0 to 40     | The minimum low-frequency signaling return loss in dB allowed before reporting a trunk as out of tolerance. Larger values are more restrictive. |

Maximum Percentage of Trunks Which Can Be Removed From Service by ATMS

Available only if **Allow ATMS Busyout**, **Error Logging**, and **Alarming** are enabled.

| Valid Entry        | Usage  |
|--------------------|--|
| 0, 25, 50, 75, 100 | The highest percentage of trunks from the trunk group that can be removed from service at one time because of unacceptable transmission measurement results. |

**Related topics:**

[Allow ATMS Busyout, Error Logging and Alarming](#) on page 1036

Unacceptable Threshold --Dev - 404 Hz

| Valid Entry | Usage   |
|-------------|---|
| 0 to 9      | The maximum negative deviation of measured loss at 404 Hz from the 1004 Hz test tone loss level (in dB) allowed before reporting a trunk as unacceptable. Smaller dB values are more restrictive. |

Unacceptable Threshold --+Dev - 404 Hz

| Valid Entry | Usage   |
|-------------|---|
| 0 to 9      | The maximum positive deviation of measured loss at 404 Hz from the 1004 Hz test tone loss level (in dB) allowed before reporting a trunk as unacceptable. Smaller dB values are more restrictive. |

Unacceptable Threshold --Dev - 2804 Hz

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9      | The maximum negative deviation of measured loss at 2804 Hz from the 1004 Hz test tone loss level (in dB) allowed before reporting a trunk as unacceptable. Smaller dB values are more restrictive. |

Unacceptable Threshold --+Dev - 2804 Hz

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9      | The maximum positive deviation of measured loss at 2804 Hz from the 1004 Hz test tone loss level (in dB) allowed before reporting a trunk as unacceptable. Smaller dB values are more restrictive. |

Unacceptable Threshold - Max - 1004 Hz Loss

| Valid Entry | Usage   |
|-------------|---|
| 0 to 21     | The maximum signal loss allowed for a 1004 Hz test tone (in dB) before a trunk is reported as unacceptable. A smaller dB value is more restrictive. |

## Unacceptable Threshold - Maximum C Message Noise

| Valid Entry | Usage   |
|-------------|---|
| 15 to 55    | The maximum C-message noise interference in dBmC above reference noise terminating on a telephone as measured within the voice band frequency range (500 to 2500 Hz) allowed before reporting a trunk as unacceptable. Smaller values are more restrictive. |

## Unacceptable Threshold - Maximum C Notched Noise

| Valid Entry | Usage  |
|-------------|--|
| 34 to 74    | The maximum C-notched signal dependent noise interference in dBmC allowed before reporting a trunk as unacceptable. Smaller values are more restrictive. |

## Unacceptable Threshold - Min - 1004 Hz Loss

| Valid Entry | Usage  |
|-------------|--|
| -2 to 21    | The minimum signal loss allowed for a 1004 Hz test tone (in dB) before a trunk is reported as unacceptable. A larger dB value is more restrictive. |

## Unacceptable Threshold - Minimum ERL

| Valid Entry | Usage  |
|-------------|--|
| 0 to 40     | The minimum low-frequency echo return loss in dB allowed before reporting a trunk as unacceptable. Larger values are more restrictive. |

## Unacceptable Threshold - Minimum SRL-HI

| Valid Entry | Usage  |
|-------------|--|
| 0 to 40     | The minimum high-frequency signaling return loss in dB allowed before reporting a trunk as unacceptable. Larger values are more restrictive. |

## Unacceptable Threshold - Minimum SRL-LO

| Valid Entry | Usage   |
|-------------|---|
| 0 to 40     | The minimum low-frequency signaling return loss in dB allowed before reporting a trunk as unacceptable. Larger values are more restrictive. |

**Trunk Group: Group Member Assignments**

For SIP Enablement Services (SES) trunks, the group member-assignment pages are not individually administrable. The system automatically populates and displays these fields based on the number of members of SES trunk groups previously specified.

**Administered Members (min/max)**

The minimum and maximum member numbers that have been administered for this trunk group.

**Ans Delay**



**Caution:**

Customers should not attempt to administer this field. Please contact your Avaya technical support representative for assistance.

| Valid Entry                    | Usage   |
|--------------------------------|---|
| 20 to 5100 in increments of 20 | The length of time the server running Communication Manager waits before it sends answer supervision for incoming calls on tie trunks using the TN722A or later, TN760 (B, C, or D), TN767, TN464 (any suffix), TN437, TN439, TN458, or TN2140 circuit packs. |
| blank                          | Same as setting the field to zero.  |

**Code**

The type of circuit pack physically installed or logically administered at the location to which this member is assigned. If no circuit pack is installed or administered at the port address, the field is blank.

**Mode**

The signaling mode used on tie trunks with TN722A or later, TN760B or later, TN767, TN464 (any suffix), TN437, TN439, TN458, or TN2140 circuit packs. This entry must correspond to associated dip-switch settings on the circuit pack.



**Caution:**

Customers should not attempt to administer this field. Please contact your Avaya technical support representative for assistance.

| Valid Entry | Usage  |
|-------------|--|
| e&m         | For six-wire connections that pair two signaling wires with four voice wires. This configuration is used in the vast majority of systems in the United States. |
| simplex     | For four-wire connections that do not use an additional signaling pair. This configuration is very rare in the United States.                                  |

**Name**

The name of the trunk group member. The name should identify the trunk unambiguously. Accepts up to 10 characters.

**Example**

- The telephone number assigned to incoming trunks
- The Trunk Circuit Identification number assigned by the service provider

**Night**

The night service destination for this trunk group member if different from the night service destination administered for the trunk group. Incoming calls are routed to this destination when the system is placed in night service mode.

| Valid Entry              | Usage   |
|--------------------------|---|
| <i>A valid extension</i> | The extension of the night destination for the trunk.   |
| attd                     | Calls go to the attendant when night service is active. |
| blank                    | Not administered  |

**Related topics:**

[Night Service](#) on page 986

**Port**

| Valid Entry                              | Usage   |
|--|---|
| 1 to 64                                  | First and second characters are the cabinet number. |
| A to E                                   | Third character is the carrier.                     |
| 0 to 20                                  | Fourth and fifth characters are the slot number.    |
| 01 to 04 (Analog TIE trunks)<br>01 to 31 | Six and seventh characters are the circuit number.  |
| 1 to 250                                 | Gateway   |
| V1 to V9                                 | Module  |
| 01 to 31                                 | Circuit   |

**Sfx**

The model suffix for the type of circuit pack physically installed at the location to which this member is assigned. If no circuit pack is installed at the port address, the field is blank.

**Total Administered Members**

The total number of members administered in the trunk group.

**Type**
 **Caution:**

Customers should not attempt to administer this field. Please contact your Avaya technical support representative for assistance.

| Valid Entry        | Usage  |
|--------------------|--|
| t1-stan<br>t1-comp | Specifies the signaling type to be used with TN760B (or later release), TN722 (with any suffix), TN767, TN2140 (when the <b>Trunk Type</b> is cont), |

| Valid Entry      | Usage   |
|------------------|---|
| t5-rev<br>type-5 | TN437, TN439, TN464 with any suffix, or TN458 circuit packs. Available only if the <b>Trunk Type</b> is blank or cont.<br>t5-rev is allowed only for the TN760D vintage 10 or later. When <b>Type</b> is t5 rev, <b>Mode</b> must be e&m. |

**Related topics:**

[Trunk Type](#) on page 826

**Trunk Group: Protocol Variations**

Available only for sip trunk groups.

**Related topics:**

[Group Type](#) on page 725

***Always Use re-INVITE for Display Updates***

Appears only when the **Group Type** field is sip.

| Valid Entry | Usage  |
|-------------|--|
| y           | In SIP messages, Communication Manager sends re-invite message to display update.                      |
| n           | In SIP messages, Communication Manager sends update message to display update. The default value is n. |

***Convert 180 to 183 for Early Media***

Enables or disables the early media and direct media cut-through, When SDP answer is returned by Communication Manager in 18x some entities have a problem receiving the SDP in 180 Ringing message and require the use of 183 Session Progress message. The default value is n.

***Enable Q-SIP***

Appears only when the **Group Type** field is sip.

| Valid Entry | Usage  |
|-------------|--|
| y           | Enables the QSIG over SIP (Q-SIP) feature for the trunk group. If trunk members are already assigned to this trunk group, you must not change the value of <b>Enable Q-SIP</b> field. If you change the value of <b>Enable Q-SIP</b> field, the system displays an error message and prompts you to remove all assigned members before enabling Q-SIP. |
| n           | The QSIG over SIP feature for the trunk group is disabled. By default, the value is n.   |

***Mark Users as Phone***

Enables or disables the encoding of URIs in call control signaling messages originated at the gateway with the “user=phone” parameter. No subscription messages are encoded with the “user=phone” parameter, even when the field is set to y. Default is n.

 **Note:**

Do not change the default of n for this field unless you are sure that every recipient of SIP Enablement Services (SES) calls using this trunk can accept and properly interpret the optional “user=phone” parameter. Enterprise users without support for “user=phone” in their SIP Enablement Services (SES) endpoints will experience adverse effects, including rejected calls.

### **Network Call Redirection**

If enabled, Network Call Redirection (NCR) service is signaled over this trunk group. NCR only works on trunk groups connected to Service Providers that support NCR.

### **Prepend "+" to Calling Number**

If enabled, the calling party number in the header of the SIP message is prepended with a plus sign (+). Available only for sip trunk groups.

### **Related topics:**

[Group Type](#) on page 725

### **QSIG Reference Trunk Group**

Appears only when the **Group Type** field is sip and the **Enable Q-SIP** is set to y.

| Valid Entry | Usage   |
|-------------|---|
| 1 to 2000   | (For Avaya S8510 Server) Assigns a number for the QSIG trunk group. If trunk members are already assigned to this trunk group, you must not change the value of <b>QSIG Reference Trunk Group</b> field. If you change the value of this field, the system displays an error message and prompts you to remove all assigned members before enabling Q-SIP.  |
| 1 to 99     | (For Avaya S8300D Server) Assigns a number for the QSIG trunk group. If trunk members are already assigned to this trunk group, you must not change the value of <b>QSIG Reference Trunk Group</b> field. If you change the value of this field, the system displays an error message and prompts you to remove all assigned members before enabling Q-SIP. |
| blank       | No QSIG trunk group is assigned. By default, the value is blank.  |

### **Send Transferring Party Information**

Enables or disables sending the transferring party information on a transferred call. Default is disabled.

### **Telephone Event Payload Type**

| Valid Entry        | Usage   |
|--------------------|---|
| 96 to 127<br>blank | The default payload type offered by Communication Manager for SIP trunks. The payload type number encoding for originating (offering) the RFC 2833 RTP “telephone-event” payload format is based on the |

| Valid Entry | Usage  |
|-------------|--|
|             | administered number from this field. This value is used only for Communication Manager originations (outgoing offers). Default is 127. |

## Uniform Dial Plan Table

The **UDP** provides a common dial plan length — or a combination of extension lengths — that can be shared among a group of Avaya servers. Additionally, **UDP** can be used alone to provide uniform dialing between two or more private switching systems without ETN, DCS, or Main/Satellite/Tributary configurations.

Available only if **Uniform Dialing Plan** is enabled for the system.

Example command: `change uniform-dialplan n`, where *n* is the uniform dial plan length.

### Related topics:

[Uniform Dialing Plan](#) on page 950

### Conv

Enables or disables additional digit conversion.

### Del

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9      | The number of digits to delete before routing the call. This number must be less than or equal to the number of user dialed digits the system collects to match to the matching pattern. |

### Related topics:

[Len](#) on page 1045

### Insert Digits

The specific digits or number of administered location prefix digits inserted before routing the call.

| Valid Entry            | Usage   |
|------------------------|---|
| 0 to 9 (1 to 4 digits) | The digits that replace the deleted portion of the dialed number.   |
| Lx (1 to 5)            | The variable <i>x</i> represents a number of digits between 1 and 5. It is the number of leading digits taken from the administered location prefix. These digits are prepended to the dialed string. The value for <i>x</i> must be less than the number of digits in the location prefix. |
| blank                  | Leave this field blank to simply delete the digits.   |

**Related topics:**

[Locations](#) on page 770

**Len**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 18     | The number of user-dialed digits the system collects to match to this Matching Pattern. This number must be greater than or equal to the <b>Matching Pattern</b> value. The value 2 can be used only when <b>Insert Digits</b> contains an Lx value. |

**Related topics:**

[Insert Digits](#) on page 1044

[Matching Pattern](#) on page 1045

**Matching Pattern**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 9      | The number Communication Manager matches to dialed numbers. Accepts up to seven digits. |

**Net**

| Valid Entry              | Usage  |
|--------------------------|--|
| aar<br>ars<br>enp<br>ext | The server or switch network used to analyze the converted number. The converted digit-string is routed either as an extension number or through its converted AAR address, its converted ARS address, or its ENP node number.<br>For enp, the ENP node number must be administered, digit conversion must be disabled, and the <b>Insert Digits</b> must not be administered. |

**Related topics:**

[Conv](#) on page 1044

[Insert Digits](#) on page 1044

[Node Num](#) on page 1045

**Node Num**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 999    | The ENP (Extension Number Portability) Node Number. |

**Percent Full**

Displays the percentage (0 to 100) of the memory resources allocated for the uniform dial plan data that are currently being used.

## User Profile

This screen is described in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431. For more information on administering user profiles and logins, see AAA Services in *Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205.

## Variables for Vectors

This screen creates variables and defines the necessary parameters for each variable type. Specifies the variable type, the name to use for the variable, the size of the variable, how the variable gets set or assigned, and whether the variable is local or global. Up to 702 variables can be supported using A to Z and AA to ZZ rows.

Example command: `change variables`

### Assignment

A number to pre-assign to the variable. This field displays the current value for global values. Administration is optional. Available only when the type is value or collect G .

#### Related topics:

[Type](#) on page 1047

### Description

An identifying name or description of the vector variable. Administration is optional. Default is blank. Accepts up to 27 characters.

### Length

| Valid Entry | Usage   |
|-------------|---|
| 1 to 16     | The maximum number of digits from the data to assign to the variable. This field does not apply to the doy, dow, and tod variables. This entry is required for all types to which it applies. |

### Scope

| Valid Entry | Usage                          |
|-------------|--------------------------------|
| G           | The variable is used globally. |
| L           | The variable is used locally.  |

### Start

| Valid Entry | Usage   |
|-------------|---|
| 1 to 96     | Specifies the beginning character position of the data digits string to be used for assigning to the variable. The combination of the <b>Start</b> position |

| Valid Entry | Usage  |
|-------------|--|
|             | and maximum length of the digits string defines what is to be assigned to the variable. If the number of digits to be used is less than the maximum length specified, only that portion is assigned to the variable. |

**Type**

| Valid Entry  | Usage                     |
|--|---------------------------|
| ani<br>asaiuui<br>collect<br>dow<br>doy<br>stepcnt<br>tod<br>value<br>vdn<br>vdntime | The vector variable type. |

**VAC**

| Valid Entry     | Usage  |
|-----------------|--|
| 1 to 9<br>blank | The Vector Variable Feature Access Code (FAC) to use for changing the value. |

**Var**

| Valid Entry      | Usage   |
|------------------|---|
| A to Z, AA to ZZ | The letter identifying the row of a specific vector variable. |

**Vector Directory Number**

Defines vector directory numbers (VDN) for the Call Vectoring feature. A VDN is an extension number used to access a call vector. Each VDN is mapped to one call vector. VDNs are software extension numbers (that is, not assigned to physical equipment). A VDN is accessed through direct dial local telephone company central office trunks mapped to the VDN (incoming destination or night service extension), DID trunks, and LDN calls. The VDN can be Night Destination for LDN.

Example command: `add vdn n`, where *n* is the VDN extension number.

**Vector Directory Numbers: page 1**

**1st/2nd/3rd Skill**

This field follows VDN override rules when the system changes the “active” VDN for a call. Available only if **Expert Agent Selection (EAS)** is enabled for the system and **Meet-me Conferencing** is disabled.

| Valid Entry | Usage                                  |
|-------------|--|
| 1 to 999    | The skill number for each skill.       |
| blank       | Not administered. This is the default. |

**Related topics:**

[Expert Agent Selection \(EAS\)](#) on page 951

[Meet-me Conference](#) on page 1049

**Acceptable Service Level (sec)**

Available only if **BCMS/VuStats Service Level** is enabled for the system and the VDN is measured by BCMS.

| Valid Entry | Usage   |
|-------------|---|
| 0 to 9999   | The number of seconds within which calls to this VDN should be answered. This allows BCMS to report the percentage of calls that were answered within the specified time. |
| blank       | Not administered. This is the default.  |

**Related topics:**

[BCMS/VuStats Service Level](#) on page 950

[Measured](#) on page 1049

**Allow VDN Override**

Available only if **Meet-me Conferencing** is disabled for the system.

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows the system to change the routed-to VDN to the “active” VDN for a call. The “active” VDN is the VDN to be used for parameters associated with the call such as VDN name, skills, tenant number, BSR application, VDN variables, and so on. The field follows VDN override rules when the system changes the “active” VDN for a call. |
| n           | The routed-to VDN does not become the active VDN. The parameters of the original VDN are used. This is the default.  |

**Related topics:**

[Meet-me Conference](#) on page 1049

**Attendant Vectoring**

Indicates whether or not Attendant Vectoring is optioned on this VDN. Attendant Vectoring does not support Call Center features.

**Related topics:**

[Attendant Vectoring](#) on page 944

**COR**

| Valid Entry | Usage   |
|-------------|---|
| 0 to 995    | The class of restriction (COR) of the VDN consisting of a one- or two-digit number. This field cannot be blank. |

**Destination**

Specifies if the calls are routed using a Vector Number or Policy Routing Table.

**Extension**

The extension number of the VDN. The extension is a number that starts with a valid first digit and length as defined by the system's dial plan.

**Measured**

Enables measurement data collection for this VDN. Data can be collected for reporting by BCMS or the Call Management System. Available only if **Meet-me Conferencing** is disabled. **BCMS** must be enabled for the system for this field to be set to internal or both. In addition, the appropriate CMS release must be administered for the system if this field is external or both.

| Valid Entry | Usage   |
|-------------|---|
| internal    | Data is measured internally by BCMS.              |
| external    | Data is measured internally by CMS.               |
| both        | Data is measured internally by both BCMS and CMS. |
| none        | Data is not measured. This is the default.        |

**Related topics:**

[BCMS \(Basic\)](#) on page 950

[Meet-me Conference](#) on page 1049

**Meet-me Conference**

Enables or disables Meet-me Conferencing for this VDN. Determines if the VDN is a Meet-me Conference VDN.

**Note:**

If the VDN extension is part of your DID block, external users are able to access the conference VDN. If the VDN extension is not part of the DID block, only internal callers on the network (including DCS or QSIG) or remote access callers can access the conference VDN.

Available only if **Enhanced Conferencing** is enabled for the system. If **Enhanced Conferencing** is enabled, but no other vectoring options are enabled, only Meet-me Conference vectors can be assigned.

**Related topics:**

[Enhanced Conferencing](#) on page 945

**Name**

The name associated with the VDN. When **Meet-me Conferencing** is disabled, this field follows VDN override rules when the system changes the “active” VDN for a call. Accepts up to 27 alphanumeric characters.

The name might be truncated on agents’ displays depending on the application. When information is forwarded with an interflowed call, only the first 15 characters are sent.

 **Note:**

Supported by Unicode language display for the 4610SW, 4620SW, 4621SW, and 4622SW, Sage, Spark, and 9600-series Spice telephones. Unicode is also an option for the 2420J telephone when the **Display Character Set** is katakana. For more information on the 2420J, see *2420 Digital Telephone User's Guide*.

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, do not display correctly on a BRI station.

**Related topics:**

[Display Character Set](#) on page 938

[Meet-me Conference](#) on page 1049

**Number**

| Valid Entry | Usage  |
|-------------|--|
| 1 to 2000   | The number of the vector or the Policy Routing Table (PRT) to which the calls are allocated. |

**Service Objective**

This field has two uses:

- When **BCMS/VuStats Service Level** is enabled for the system
- When **Dynamic Advocate** is enabled for the system

| Valid Entry | Usage   |
|-------------|---|
| 1 to 9999   | For <b>BCMS/VuStats Service Level</b> , sets the number of seconds within which calls to this VDN should be answered. This allows BCMS to report the percentage of calls that were answered within the specified time. The VDN must be administered to be measured by BCMS. The default is blank. |

| Valid Entry | Usage   |
|-------------|---|
| 1 to 9999   | For <b>Dynamic Advocate</b> , enables the Dynamic Queue Position feature. This feature allows calls to be queued from multiple VDNs to a single skill, while maintaining different service objectives for those VDNs. Enter the service level, in seconds, that you want to achieve for the VDN. The default is 20. |

**Related topics:**

[BCMS/VuStats Service Level](#) on page 950

[Dynamic Advocate](#) on page 951

**TN**

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

**VDN of Origin Annc. Extension**

The extension number of the VDN of Origin announcement. A VDN of Origin announcement is a short recording that identifies something about the call originating from the VDN. The agent hears the recording just prior to the delivery of the call. This field follows VDN override rules when the system changes the “active” VDN for a call.

Available only if VDN of **Origin Announcement** is enabled for the system and **Meet-me Conferencing** is disabled.

**Related topics:**

[VDN of Origin Announcement](#) on page 953

[Meet-me Conference](#) on page 1049

**Vector Number**

An identifying number that specifies the call vector that is accessed through the VDN. This field cannot be blank.

**Vector Directory Number: page 2 (Meet-me Conference disabled)****Related topics:**

[Meet-me Conference](#) on page 1049

**AUDIX Name**

The name of the AUDIX machine if this VDN is associated with the AUDIX vector.

**BSR Application**

Available only if **Lookahead Interflow (LAI)** and **Vectoring (Best Service Routing)** are enabled for the system. When **Meet-me Conferencing** is disabled, this field follows VDN override rules when the system changes the “active” VDN for a call.

| Valid Entry       | Usage   |
|-------------------|---|
| 1 to 511<br>blank | A one- to three-digit number that specifies an application plan for the VDN when using multi-site Best Service Routing with this VDN. |

**Related topics:**

[Lookahead Interflow \(LAI\)](#) on page 951

[Vectoring \(Best Service Routing\)](#) on page 952

**BSR Available Agent Strategy**

Determines how Best Service Routing identifies the best split or skill to service a call in an agent surplus situation. Available only if **Vectoring (Best Service Routing)** is enabled for the system. When **Meet-me Conferencing** is disabled, this field follows VDN override rules when the system changes the “active” VDN for a call.

| Valid Entry | Usage   |
|-------------|---|
| 1st-found   | BSR uses the first selection for routing; that is, the current best selected from the previous consider commands.   |
| UCD-LOA     | The call is routed to the least occupied agent, without regard to skill level. Can be set only if <b>Least Occupied Agent (LOA)</b> or <b>Business Advocate</b> is enabled for the system.      |
| UCD-MIA     | The call is routed to the most idle agent, without regard to skill level. This type of call distribution ensures a high degree of equity in agent workloads even when call-handling times vary. |
| EAD-LOA     | The call is routed to the highest skill level agent with the lowest occupancy. Can be set only if <b>Least Occupied Agent (LOA)</b> or <b>Business Advocate</b> is enabled for the system.      |
| EAD-MIA     | The call is routed to the highest skill level, most idle agent. Can be set only if <b>Expert Agent Selection (EAS)</b> is enabled for the system.   |

**Related topics:**

[Business Advocate](#) on page 951

[Expert Agent Selection \(EAS\)](#) on page 951

[Least Occupied Agent](#) on page 951

[Vectoring \(Best Service Routing\)](#) on page 952

**BSR Local Treatment**

Enables or disables local server control of BSR treatment. In a multi-site BSR configuration, a call that arrives at a local communication server can be rerouted to a remote server located in a different part of the world. This feature maintains control at the local server and allows the server to provide local audio feedback for IP and ISDN calls, or to take back the call while the call waits in queue on a remote server. When **Meet-me Conferencing** is disabled, this field follows VDN override rules when the system changes the “active” VDN for a call.

**Note:**

This field must be enabled on both the local and remote vdns, or else call interflow attempts might result in dropped calls.

**BSR Tie Strategy**

Available only if **Vectoring (Best Service Routing)** is enabled for the system. When **Meet-me Conferencing** is disabled, this field follows VDN override rules when the system changes the “active” VDN for a call.

| Valid Entry | Usage   |
|-------------|---|
| system      | System-wide settings apply.   |
| 1st-found   | BSR uses the previously selected best choice as the best skill or location. This is the default setting.  |
| alternate   | Alternates the BSR selection algorithm when a tie in EWT or available agent criteria occurs. Every other time a tie occurs for calls from the same VDN, the consider step with the tie is selected to send the call instead of the first selected split, skill, or location. This helps balance the routing when the cost of routing remotely is not a concern. |

**Related topics:**

[Vectoring \(Best Service Routing\)](#) on page 952

**Display VDN for Route-To DAC**

Enables or disables the display of the VDN when a call arrives as a result of a route-to at an agent terminal under the following conditions:

- A route-to number with coverage is enabled, or route-to digits with coverage is enabled and the vector command routes a call to an agent as an EAS direct agent call.
- Adjunct routing routes a direct agent call to the agent.

When **Meet-me Conferencing** is disabled, this field follows VDN override rules when the system changes the “active” VDN for a call.

Available only if **Expert Agent Selection (EAS)** is enabled for the system.

**Related topics:**

[Expert Agent Selection \(EAS\)](#) on page 951

**Observe an Agent Answer**

Enables or disables a service observer to start observing a call to the VDN when the call is delivered to the agent or station.

**Send VDN as Called Ringing Name Over QSIG**

| Valid Entry | Usage   |
|-------------|---|
| y           | If the ISDN trunk call is made, receiver can view the VDN name when the telephone is ringing. |

| Valid Entry | Usage  |
|-------------|--|
| n           | The receiver cannot view the VDN name when the telephone is ringing. The default value is n. |

**Return Destination**

The VDN extension number to which an incoming trunk call is routed if it returns to vector processing after the agent drops the call. When **Meet-me Conferencing** is disabled, this field follows VDN override rules when the system changes the “active” VDN for a call.

**VDN Override for ASAI Messages**

Determines if the active VDN is sent as the called number for ISDN Trunk ASAI messages. When **Meet-me Conferencing** is disabled, this field follows VDN override rules when the system changes the “active” VDN for a call. The “active” VDN is the VDN receiving the call and will be changed to a routed-to VDN if **Allow VDN Override** is enabled. Available only if **ASAI Link Core Capabilities** is enabled for the system.

| Valid Entry | Usage   |
|-------------|---|
| n           | The “Called Number” information is sent for the “Call Offered”, “Alerting”, “Queued”, and “Connect” ASAI event notification messages. The adjunct-request message is always the called VDN extension in the Called Number IE sent in the incoming ISDN SETUP message or the local call’s called number and does not change after routing to the called VDN and subsequent routed-to VDNs. |
| ISDN Trunk  | When an incoming ISDN trunk call is routed to this VDN, the “Called Number” information sent in the ASAI event and “Adjunct Route Request” ASAI messages is the “active VDN” extension. This extension becomes associated with the call based on the VDN Override rules. This option does not apply to local/internal calls.  |
| all         | The active VDN is used for the called number for all types of calls to the VDN, including local/internal calls as well as external incoming ISDN trunk calls.   |

**Related topics:**

[ASAI Link Core Capabilities](#) on page 943

[Allow VDN Override](#) on page 1048

**VDN Timed ACW Interval**

| Valid Entry        | Usage   |
|--------------------|---|
| 1 to 9999<br>blank | Sets the length of the timed ACW Interval. When a value is entered in this field, an agent in auto-in work mode who receives a call from this VDN is automatically placed into After Call Work (ACW) when the call drops. When the administered time is over, the agent automatically becomes available. This field takes precedence over the hunt group <b>Timed ACW Interval</b> . When <b>Meet-me Conferencing</b> is disabled, this |

| Valid Entry | Usage   |
|-------------|---|
|             | field follows VDN override rules when the system changes the “active” VDN for a call. |

**Related topics:**

[Timed ACW Interval \(sec\)](#) on page 660

**Vector Directory Number: page 2 (Meet-me Conference enabled)****Related topics:**

[Meet-me Conference](#) on page 1049

**Conference Access Code****Security alert:**

To ensure conference security, always assign an access code to a Meet-me Conference VDN.

The Meet-Me Conference VDN access code. Accepts up to six digits.

**Conference Controller**

Controls which user is allowed to change the access code for a Meet-me Conference VDN using a feature access code. This can be a local user or someone dialing in from remote access trunks.

| Valid Entry             | Usage   |
|-------------------------|---|
| <i>Extension number</i> | Only a user at this extension can change the access code for that VDN using a feature access code.                              |
| blank                   | Any station user that is assigned with console permissions can change the access code for that VDN using a feature access code. |

**Conference Type**

The conference type that is appropriate for the call.

| Valid Entry | Usage  |
|-------------|--|
| 6-party     | For six or fewer participants. Default is 6-party.   |
| expanded    | Enables the Expanded Meet-me Conference feature. For a conference with more than six participants. |

**Route-to Number**

The ARS or AAR Feature Access Code (FAC) followed by the routing digits. Alternately, the unique UDP extension. Accepts up to 16 digits. Allows administration of the routing digits (the ARS/AAR Feature Access Code with the routing digits and the Conference ID digits for the VDN). Available only for expanded conference types.



**Note:**

The Route-to Number must be unique across all Expanded Meet-me Conference VDNs.

**Related topics:**

[Conference Type](#) on page 1055

**Vector Directory Number: page 3**

**VDN VARIABLES**

When **Meet-me Conferencing** is disabled, an asterisk (\*) appears next to the heading, indicating that variables V1 through V9 follow VDN override rules when the system changes the “active” VDN for a call.

**Related topics:**

[Meet-me Conference](#) on page 1049

Assignment

| Valid Entry | Usage  |
|-------------|--|
| 0 to 9      | Assigns an up to 16-digit unvalidated decimal number to each of the VDN variables V1 through V5. |
| blank       | No decimal number is assigned to the VDN variable.   |

Description

A description of the VDN variable. Accepts up to 15 characters.

Var

The number assigned to the VDN variable.

**Daylight Savings Rule**

Defines the daylight saving time rule. The daylight saving time rule is applied to `goto time-of-day` commands in the vector that is assigned to the VDN. The time-of-day calculations are based on the local time of the receiving call’s VDN. The assigned rule number applies start and stop rules that are administered for the system for that rule.

| Valid Entry | Usage  |
|-------------|--|
| system      | The system uses the same daylight saving time rule as the system clock.  |
| 0           | No daylight saving rule is applied. If the system time has a daylight saving rule specified, this rule is removed before evaluating the <code>goto if time-of-day</code> conditional.  |
| 1 to 15     | The <b>Daylight Savings Rule</b> number. When you use a number other than 0, the rule associated with the main server clock display time and the main server offset are not used. The offset and rule assigned to the active VDN for the call are applied to the operating system standard time so that local time for the VDN is used to test the time-of-day step. |

**Related topics:**

[Daylight Savings Rules](#) on page 527

[VDN Time Zone Offset](#) on page 1057

**VDN Time Zone Offset**

| Valid Entry                            | Usage   |
|--|---|
| +, -<br>00-23 - hour<br>00-59 - minute | This field is applied against the switch clock when a time of day vector command is executed. Daylight savings time changes are handled by the switch clock using the existing operation.<br>When <b>Meet-me Conferencing</b> is disabled, this field follows VDN override rules when the system changes the “active” VDN for a call. The valid entries are based on a syntax of +HH:MM. The default is +00:00. When the default is set, the system switch time is used without modification. |

**Related topics:**

[Meet-me Conference](#) on page 1049

**Video Bridge**

Used to configure available ad-hoc conferencing resources. For more detailed information on Avaya Video Telephony, see *Avaya Video Telephony Solution Networking Guide, 16-601423*.

Example command: `add video-bridge n`, where *n* is the video bridge number.

**Bridge ID**

The ID number for this video bridge.

**Call Rate**

The maximum allowable call rate for the conference. Available only when **Far End Resource Info** is disabled and **Type** is not administered.

**Related topics:**

[Far End Resource Info](#) on page 1057

[Type](#) on page 1059

**Far End Resource Info**

Enables or disables far end resource tracking and reporting.

| Valid Entry | Usage  |
|-------------|--|
| y           | The far end tracks port usage and provides updates on resource availability. |
| n           | No resource information is provided from the far end.                        |

### ID Range Start/End

A range of conference IDs that this video bridge can use. There must be enough IDs so that all ports can be used — one ID for every six ports. Accepts up to nine digits.

The default is blank.

Available only for h.323 trunk groups.

#### Related topics:

[Group Type](#) on page 725

### Max Ports

| Valid Entry     | Usage  |
|-----------------|--|
| 3 to system max | The maximum number of video conferencing ports for this video bridge. Default is none. |

### Name

The name that identifies this video bridge. Accepts up to 30 alphanumeric characters.

### Priority Factory Number

Priority versus Standard factory number depends on who creates the conference; if a user with Priority Video permissions creates the conference, the **Priority Factory Number** is used.

**Priority Factory Number** can have a dedicated video bridge or a bridge with better bandwidth than the **Standard Factory Number**. Available only for h.323 or sip trunk groups when the **Far End Resource Info** is enabled.

| Valid Entry         | Usage  |
|---------------------|--|
| 1 to 9 digits (0,9) | At least one of <b>Priority Factory Number</b> or <b>Standard Factory Number</b> must be filled in. Standard and Priority factory numbers can be the same. |
| blank               | Priority calls can use the bridge, but prefer a bridge with a priority factory. This is the default.   |

#### Related topics:

[Group Type](#) on page 725

[Far End Resource Info](#) on page 1057

[Standard Factory Number](#) on page 1058

### Standard Factory Number

Priority versus Standard factory number depends on who creates the conference; if a user with Priority Video permissions creates the conference, the **Priority Factory Number** is used.

**Priority Factory Number** may have a dedicated video bridge or a bridge with better bandwidth than the **Standard Factory Number**. Available only for h.323 or sip trunk groups. For h.323, the **Far End Resource Info** must be enabled.

| Valid Entry         | Usage  |
|---------------------|--|
| 1 to 9 digits (0,9) | At least one of <b>Priority Factory Number</b> or <b>Standard Factory Number</b> must be filled in. Standard and Priority factory numbers can be the same. |
| blank               | Non-priority conferences are unable to use this video bridge. Default is blank.  |

**Related topics:**

[Group Type](#) on page 725

[Far End Resource Info](#) on page 1057

[Priority Factory Number](#) on page 1058

**Trunk Groups**

| Valid Entry        | Usage   |
|--------------------|---|
| 1 to 2000<br>blank | Assigns trunk groups to this video bridge. At least one incoming and one outgoing trunk, or a two-way trunk, must be assigned. All trunks on a given video bridge must be the same type; H.323 and SIP trunks cannot be mixed.<br>The default is blank. |

**Related topics:**

[Group Type](#) on page 725

**Type**

The type of video bridge. Can be administered for existing or new video bridges. Available only if **Far End Resource Info** is disabled.

| Valid Entry | Usage  |
|-------------|--|
| Exact       | All participants in the conference must use the exact rate specified or be in the audio-only mode.                       |
| Maximum     | <b>Call Rate</b> is enabled, and any call rate up to the configured rate is allowed in a conference. Default is Maximum. |
| Region      | The initial entry for an existing video bridge. <b>Call Rate</b> is not available.                                       |

**Related topics:**

[Call Rate](#) on page 1057

[Far End Resource Info](#) on page 1057

**Virtual MAC Addresses**

Lists the virtual Media Access Control (MAC) addresses on the system.

Example command: `display virtual-mac-address n`, where *n* is the virtual MAC addresses table number.

## MAC Address

Virtual MAC address shared by duplicated TN2602AP circuit packs. Accepts up to 15 alphanumeric characters.

 **Note:**

The 4606, 4612, and 4624 telephones do not support the bearer duplication feature of the TN2602AP circuit pack. If these telephones are used while an interchange from archive to standby media processor is in process, calls might be dropped.

## Used

Indicates whether or not the associated virtual MAC address has been assigned in the system.

---

## Configure Options

The Uniform Dial Plan call type works identically with the ext call type, with an exception: if the dialed digits match the call type of UDP, Communication Manager automatically checks the UDP Table first to see if there is a match, regardless of the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen. If there is no match, Communication Manager then checks the local server.

If the dialed digits match the call type of ext, Communication Manager checks the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen.

If the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen is **udp-table-first**, Communication Manager checks the UDP Table first to see if there is a match. If there is no match, Communication Manager then checks the local server.

If the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen is **local-extensions-first**, Communication Manager checks the local server first to see if there is a match. If there is no match, Communication Manager then checks the UDP Table.

The UDP call type allows Communication Manager to recognize strings of 14 to 18 digits, which are longer than the maximum extension length of 13 digits. However, the UDP call type can be used with any length in case this provides a useful new capability to customers.

### UDP in System Manager

You can select the Uniform Dial Plan option in the Synchronize CM Data and Configure Options page under **Elements > Inventory**. When you select the **Consider UDP** option, the corresponding dial plan is not considered for the available extension range while adding an endpoint. When you do not select the **Consider UDP** option, the corresponding dial plan is considered for the available extension range while adding an endpoint.

# Chapter 6: Managing templates

---

## Templates

---

### Template Management

A template is a file that contains stored settings. You can use templates to streamline the process of performing various routine activities. Templates save the data that you enter so that you can perform similar activities later without re-entering the same data. System Manager allows you to create, store, and use templates to simplify tasks like adding, editing, and viewing endpoints or subscribers. System Manager offers several default templates and you can create your own templates as well.

Templates exist in two categories, default templates and user-defined templates. The default templates exist on the system and you cannot edit or remove them. You can, however, modify or remove user-defined templates any time.

---

### Template Versioning

#### Template Versioning

You can version endpoint templates with Communication Manager 5.0, Communication Manager 5.1, Communication Manager 5.2, and Communication Manager 6.0. You can associate a template with a specific version of a Communication Manager or an adopting product through template versioning. You can use the **Template Version** field under endpoint templates to accommodate endpoint template versioning.

You can also use template versioning for subscriber templates using the following versions: MM 5.0, MM 5.1, MM 5.2, MM 6.0, CMM 5.2, and CMM 6.0.

---

## Adding Endpoint templates

- 
1. From the navigation pane, click **Elements > Templates > Endpoint**.
  2. Click **New**.
  3. Click **Set type**.
  4. Enter a name in the **Template Name** field.
  5. Complete the mandatory fields under the **General Options**, **Feature Options**, **Site Data**, **Abbreviated Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections.
  6. Click **Commit**.
- 

**Related topics:**

[Endpoint / Template field descriptions](#) on page 57

---

## Editing Endpoint templates

- 
1. Click **Elements > Templates > Endpoint**.
  2. On the Endpoint Templates page, select the template you want to edit from the template list.
  3. Click **Edit** or click **View > Edit**.
  4. Complete the Edit Endpoint Template page.
  5. Click **Commit** to save the changes.
- 

**Related topics:**

[Endpoint / Template field descriptions](#) on page 57

---

## Viewing Endpoint templates

- 
1. From the navigation pane, click **Elements > Templates > Endpoint**.
  2. Select the template you want to view from the Endpoint Templates page.
  3. Click **View**.  
You can view the **General Options**, **Feature Options**, **Site Data**, **Abbreviated Call Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections in the View Endpoint Template page.

---

### Related topics:

[Endpoint / Template field descriptions](#) on page 57

---

## Deleting Endpoint templates

- 
1. From the navigation pane, click **Elements > Templates > Endpoint**.
  2. Select the endpoint template or templates you want to delete.
  3. Click **Delete**.

**Note:**

You cannot delete any of the default templates.

---

---

## Duplicating Endpoint templates

- 
1. From the navigation pane, click **Elements > Templates > Endpoint**.
  2. From the endpoint template list select the template you want to copy.
  3. Click **Duplicate**.
  4. Enter the name of the new template in the **New Template Name** field.

5. Choose the appropriate set type from the **Set Type** field.
6. Complete the Duplicate Endpoint Template page and click **Commit**.

---

**Related topics:**

[Endpoint / Template field descriptions](#) on page 57

---

## Distribution of templates

- 
1. From the navigation pane, click **Elements > Templates > Endpoint**.
  2. Select an endpoint template from the endpoint template list.
  3. Click **More Actions > Distribute**.
  4. Select the Communication Managers to which you want to distribute the template you have chosen.
  5. Click **Commit** to distribute the template value.  
All the endpoint(s) associated with this template for the selected Communication Managers will now have the same field values as that in the template.
- 

---

## Viewing Associated Endpoints

- 
1. From the navigation pane, click **Elements > Templates > Endpoint**.
  2. Select one of the endpoint templates from the list of endpoint templates.
  3. Click **More Actions > View Associated Endpoints**.  
You can view the endpoints in the System Manager database that are associated with the endpoint template you have chosen on the Associated Endpoints page.
-

---

## Adding Subscriber templates

---

1. From the navigation pane, click **Elements > Templates > Messaging**
2. From the list of supported messaging versions, select a messaging version.
3. Click **Show List**.
4. Click **New**.
5. Complete the **Basic Information, Subscriber Directory, Mailbox Features, Secondary Extensions** and **Miscellaneous** sections in the Add Subscriber Template page.
6. Click **Commit**.

Subscriber templates have different versions based on their software version. The subscriber templates you create have to correspond to the MM or CMM software version. When you select a messaging template, the **Software Version** field in the Add Subscriber Template page displays the appropriate version information.

---

### Related topics:

[Subscriber Templates \(CMM\) field descriptions](#) on page 1088

[Subscriber Templates \(MM\) field descriptions](#) on page 1090

---

## Editing Subscriber templates

---

1. From the navigation pane, click **Elements > Templates > Messaging**
2. From the supported messaging version list, select a messaging version.
3. Click **Show List**.
4. Select a subscriber template from the Subscriber Template list.
5. Click **Edit** or **View > Edit**.
6. Edit the required fields in the Edit Subscriber Template page.
7. Click **Commit** to save the changes.

**Note:**

You cannot edit any of the default subscriber templates.

---

**Related topics:**

[Subscriber Templates \(CMM\) field descriptions](#) on page 1088

[Subscriber Templates \(MM\) field descriptions](#) on page 1090

---

## Viewing Subscriber templates

- 
1. From the navigation pane, click **Elements > Templates > Messaging**
  2. From the supported messaging versions list, select one of the messaging versions.
  3. Click **Show List**.
  4. Select a subscriber template from the Subscriber Template list.
  5. Click **View** to view the mailbox settings of this subscriber.



**Note:**

You cannot edit any of the fields in the View Subscriber Template page.

---

**Related topics:**

[Subscriber Templates \(CMM\) field descriptions](#) on page 1088

[Subscriber Templates \(MM\) field descriptions](#) on page 1090

---

## Deleting Subscriber templates

- 
1. From the navigation pane, click **Elements > Templates > Messaging**
  2. From the list of supported messaging versions, select a supported messaging version.
  3. Click **Show List**.
  4. From the Subscriber Template list, select the template or templates you want to delete.
  5. Click **Delete**.



**Note:**

You cannot delete any default subscriber template.

---

## Duplicating Subscriber templates

- 
1. From the navigation pane, click **Elements > Templates > Messaging**
  2. From the list of supported messaging versions, select a messaging version.
  3. Click **Show List**.
  4. From the Subscriber Template list, select the subscriber template you want to copy.
  5. Click **Duplicate**.
  6. Complete the Duplicate Subscriber Template page and click **Commit**.
- 

### Related topics:

[Subscriber Templates \(CMM\) field descriptions](#) on page 1088

[Subscriber Templates \(MM\) field descriptions](#) on page 1090

---

## Viewing Associated Subscribers

- 
1. From the navigation pane, click **Elements > Templates > Messaging**
  2. From the list of supported messaging versions, select a messaging version.
  3. Click **Show List**.
  4. From the Subscriber Template list, select a subscriber template for which you want to view the associated subscribers.
  5. Click **More Actions > View Associated Subscribers**.  
You can view all the associated subscribers in the System Manager database for the template you have chosen in the Associated Subscribers page.
- 

---

## Template List

You can view the template list when you click the **Template** option in the **Elements** tab. You must click the **Endpoint** or **Messaging** option to view the endpoint or messaging template list.

You can apply filters and sort each of the columns in the endpoint or messaging template list. When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name  | Description   |
|---|---|
| <b>Name</b>                                       | Name of the template.   |
| <b>Owner</b>                                      | Specifies the name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates this field specifies the name of the user who created the template. |
| <b>Version</b>                                    | Specifies the version of the template.  |
| <b>Default</b>                                    | Specifies whether the template is default or user-defined.  |
| <b>Last Modified</b>                              | Specifies the time and date when the endpoint or messaging template was last modified.  |
| <b>Set type</b> (for endpoint templates)          | Specifies the set type of the endpoint template.  |
| <b>Type</b> (for messaging templates)             | Specifies whether the messaging type is MM or CMM.  |
| <b>Software Version</b> (for messaging templates) | Specifies the type of messaging version of the messaging template.  |

---

## Filtering Templates

1. From the navigation pane, click **Elements > Templates**.
2. Click either **Endpoint** or **Messaging** for endpoint templates and messaging templates respectively.
3. Select the Communication Manager or supported messaging version, whichever applicable.
4. Click **Show List**.
5. Click **Filter: Enable** in the Template List.
6. Filter the endpoint or subscriber templates according to one or multiple columns.
7. Click **Apply**.  
To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.



**Note:**

The table displays only those endpoint or subscriber templates that match the filter criteria.

---

## Add station Template

### Endpoint / Template field descriptions

You can use these fields to perform endpoint / template tasks. This page has the exclusive fields that occur for endpoints and templates apart from the **General options, Feature Options, Site Data, Data Module/Analog Adjunct, Abbreviated Call Dialing, Enhanced Call Fwd** and **Button Assignment** sections.

#### Field description for Endpoints

| Name            | Description   |
|-----------------|---|
| <b>System</b>   | Specifies the Communication Manager that the endpoint is assigned to.   |
| <b>Template</b> | Specifies all the templates that correspond to the set type of the endpoint.  |
| <b>Set Type</b> | Specifies the set type or the model number of the endpoint.   |
| <b>Name</b>     | Specifies the name associated with an endpoint. The name you enter displays on called telephones that have display capabilities. Some messaging applications, such as Communication Manager Messaging recommend that you enter the user's name (last name first) and their extension to identify the telephone. The name entered is also used for the integrated directory. |

#### Field description for Templates

| Name                 | Description   |
|----------------------|---|
| <b>Set Type</b>      | Specifies the set type or the model of the endpoint template.                                     |
| <b>Template Name</b> | Specifies the name of the endpoint template. You can enter the name of your choice in this field. |

#### Extension

The extension for this station.

For a virtual extension, a valid physical extension or a blank can be entered. Blank allows an incoming call to the virtual extension to be redirected to the virtual extension "busy" or "all" coverage path.

#### Port

The port assigned to the station.

| Valid Entry | Usage   |
|-------------|---|
| 01 to 64    | First and second numbers are the cabinet number |
| A to E      | Third character is the carrier                  |

| Valid Entry | Usage   |
|-------------|---|
| 01 to 20    | Fourth and fifth characters are the slot number   |
| 01 to 32    | Sixth and seventh characters are the circuit number   |
| x or X      | Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) stations, as well as for SBS Extensions.     |
| IP          | Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have an IP set. This is automatically entered for certain IP station set types, but you can enter for a DCP set with softphone permissions. This changes to the s00000 type when the set registers. |
| xxxVmpp     | Specifies the media gateway. <ul style="list-style-type: none"> <li>• xxx is the gateway number, which is in the range 001 to 250.</li> <li>• m is the module number, which is in the range 1 to 9.</li> <li>• pp is the port number, which is in the range 01 to 32.</li> </ul>  |

**General Options**

This section lets you set the general fields for a station.

**COS**

The Class of Service (COS) number used to select allowed features.

**COR**

Class of Restriction (COR) number with the desired restriction.

**Coverage Path 1 or Coverage Path 2**

The coverage-path number or time-of-day table number assigned to the station.



**Note:**

If Modified Misoperation is active, a Coverage Path must be assigned to all stations on Communication Manager.

**Related topics:**

[Misoperation Alerting](#) on page 607

**TN**

| Valid Entry | Usage                        |
|-------------|------------------------------|
| 1 to 100    | The Tenant Partition number. |

**Security Code**

The security code required by users for specific system features and functions, including the following: Personal Station Access, Redirection of Calls Coverage Off-Net, Leave Word Calling, Extended Call Forwarding, Station Lock, Message Retrieval, Terminal Self-

Administration, and Demand Printing. The required security code length is administered system-wide.

**Related topics:**

[Minimum Station Security Code Length](#) on page 853

**Emergency Location Ext**

The Emergency Location Extension for this station. This extension identifies the street address or nearby location when an emergency call is made. Defaults to the telephone's extension. Accepts up to eight digits.

 **Note:**

On the ARS Digit Analysis Table in Communication Manager, 911 must be administered to be call type emer or alrt for the E911 Emergency feature to work properly.

**Related topics:**

[Remote Softphone Emergency Calls](#) on page 63

**Message Lamp Ext**

The extension of the station tracked with the message waiting lamp.

**Lock Messages**

Controls access to voice messages by other users.

| Valid Entry | Usage   |
|-------------|---|
| y           | Restricts other users from reading or canceling the voice messages, or retrieving messages using Voice Message Retrieval. |
| n           | Allows other users to read, cancel, or retrieve messages.   |

**Feature Options**

This section lets you set features unique to a particular voice terminal type.

**Location**

This field appears only when the **Multiple Locations** field is set to y and the **Type** field is set to H.323 or SIP station types.

| Valid entry | Usage  |
|-------------|--|
| 1 to 250    | (Depending on your server configuration, see <i>Avaya Aura™ Communication Manager System Capacities Table</i> , 03-300511.) Assigns the location number to a particular station. Allows IP telephones and softphones connected through a VPN to be associated with the branch an employee is assigned to. This field is one way to associate a location with a station. For the other ways and for a list of features that use location, see the Location sections in <i>Avaya Aura™ Communication Manager Feature Description and Implementation</i> , 555-245-205. |
| blank       | Indicates that the existing location algorithm applies. By default, the value is blank.  |

**Active Station Ringing**

Defines how calls ring to the telephone when it is off-hook without affecting how calls ring at this telephone when the telephone is on-hook.

| Valid Entry    | Usage   |
|----------------|---|
| continuous     | All calls to this telephone ring continuously.  |
| single         | Calls to this telephone receive one ring cycle and then ring silently.  |
| if-busy-single | Calls to this telephone ring continuously when the telephone is off-hook and idle. Calls to this telephone receive one ring cycle and then ring silently when the telephone is off-hook and active. |
| silent         | All calls to this station ring silently.  |

**Auto Answer**

In EAS environments, the auto answer setting for the Agent LoginID can override a station's setting when an agent logs in.

| Valid Entry | Usage  |
|-------------|--|
| all         | All ACD and non-ACD calls terminated to an idle station cut through immediately. Does not allow automatic hands-free answer for intercom calls. With non-ACD calls, the set is also rung while the call is cut through. The ring can be prevented by activating the ringer-off feature button when the <b>Allow Ringer-off with Auto-Answer</b> is enabled for the system.                       |
| acd         | Only ACD split /skill calls and direct agent calls to auto answer. Non-ACD calls terminated to a station ring audibly. For analog stations, the station is off-hook and idle, only the ACD split/skill calls and direct agent calls auto answer; non-ACD calls receive busy treatment. If the station is active on an ACD call and a non-ACD call arrives, the Agent receives call-waiting tone. |
| none        | All calls terminated to this station receive an audible ringing treatment.   |
| icom        | Allows a telephone user to answer an intercom call from the same intercom group without pressing the <b>intercom</b> button.   |

**Related topics:**

[Allow Ringer-off with Auto-Answer](#) on page 619

**MWI Served User Type**

Controls the auditing or interrogation of a served user's message waiting indicator (MWI).

| Valid Entries | Usage  |
|---------------|--|
| fp-mwi        | The station is a served user of an fp-mwi message center.  |
| qsig-mwi      | The station is a served user of a qsig-mwi message center.   |
| blank         | The served user's MWI is not audited or if the user is not a served user of either an fp-mwi or qsig-mwi message center. |

**Coverage After Forwarding**

Governs whether an unanswered forwarded call is provided coverage treatment.

| Valid Entry | Usage  |
|-------------|--|
| y           | Coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters.    |
| n           | No coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters. |
| s(system)   | Administered system-wide coverage parameters determine treatment.  |

**Related topics:**

[Coverage After Forwarding](#) on page 932

**Per Station CPN - Send Calling Number**

Determines Calling Party Number (CPN) information sent on outgoing calls from this station.

| Valid Entries | Usage  |
|---------------|--|
| y             | All outgoing calls from the station deliver the CPN information as "Presentation Allowed."                                     |
| n             | No CPN information is sent for the call.   |
| r             | Outgoing non-DCS network calls from the station delivers the Calling Party Number information as "Presentation Restricted."    |
| blank         | The sending of CPN information for calls is controlled by administration on the outgoing trunk group the calls are carried on. |

**Display Language**

| Valid Entry   | Usage  |
|---|--|
| english<br>french<br>italian<br>spanish<br>user-defined | The language that displays on stations.<br>Time of day is displayed in 24-hour format (00:00 - 23:59) for all languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.).   |
| unicode   | Displays English messages in a 24-hour format . If no Unicode file is installed, displays messages in English by default.<br><br> <b>Note:</b><br>Unicode display is only available for Unicode-supported telephones. Currently, 4610SW, 4620SW, 4621SW, 4622SW, Sage, Spark, and 9600-series telephones (Avaya one-X Deskphone Edition SIP R2 or later) support Unicode display. Unicode is also an option for DP1020 (aka 2420J) and SP1020 (Toshiba SIP Phone) telephones when enabled for the system. |

**Personalized Ringing Pattern**

Defines the personalized ringing pattern for the station. Personalized Ringing allows users of some telephones to have one of 8 ringing patterns for incoming calls. For virtual stations, this field dictates the ringing pattern on its mapped-to physical telephone.

L = 530 Hz, M = 750 Hz, and H = 1060 Hz

| Valid Entries | Usage                  |
|---------------|------------------------|
| 1             | MMM (standard ringing) |
| 2             | HHH                    |
| 3             | LLL                    |
| 4             | LHH                    |
| 5             | HHL                    |
| 6             | HLL                    |
| 7             | HLH                    |
| 8             | LHL                    |

**Hunt-to Station**

The extension the system should hunt to for this telephone when the telephone is busy. A station hunting chain can be created by assigning a hunt-to station to a series of telephones.

**Remote Softphone Emergency Calls**

Tells Communication Manager how to handle emergency calls from the IP telephone.

 **Caution:**

An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. Please be advised that an Avaya IP endpoint cannot dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. Do not use an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations. Please contact your Avaya representative if you have questions about emergency calls from IP telephones.

Available only if the station is an IP Softphone or a remote office station.

| Valid Entry | Usage   |
|-------------|---|
| as-on-local | If the emergency location extension that corresponds to this station's IP address is not administered (left blank), the value as-on-local sends the station emergency location extension to the Public Safety Answering Point (PSAP). |

| Valid Entry | Usage  |
|-------------|--|
|             | <p>If the administrator populates the IP address mapping with emergency numbers, the value as-on-local functions as follows:</p> <ul style="list-style-type: none"> <li>• If the station emergency location extension is the same as the IP address mapping emergency location extension, the value as-on-local sends the extension to the Public Safety Answering Point (PSAP).</li> <li>• If the station emergency location extension is different from the IP address mapping emergency location extension, the value as-on-local sends the IP address mapping extension to the Public Safety Answering Point (PSAP).</li> </ul>  |
| block       | <p>Prevents the completion of emergency calls. Use this entry for users who move around but always have a circuit-switched telephone nearby, and for users who are farther away from the server than an adjacent area code served by the same 911 Tandem office. When users attempt to dial an emergency call from an IP Telephone and the call is blocked, they can dial 911 from a nearby circuit-switched telephone instead.</p>  |
| cesid       | <p>Allows Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP. The end user enters the emergency information into the IP Softphone.</p> <p>Use this entry for IP Softphones with road warrior service that are near enough to the server that an emergency call routed over the it's trunk reaches the PSAP that covers the server or switch. If the server uses ISDN trunks for emergency calls, the digit string is the telephone number, provided that the number is a local direct-dial number with the local area code, at the physical location of the IP Softphone. If the server uses CAMA trunks for emergency calls, the end user enters a specific digit string for each IP Softphone location, based on advice from the local emergency response personnel.</p> |
| option      | <p>Allows the user to select the option (extension, block, or cesid) that the user selected during registration and the IP Softphone reported. This entry is used for extensions that can be swapped back and forth between IP Softphones and a telephone with a fixed location.</p> <p>The user chooses between block and cesid on the softphone. A DCP or IP telephone in the office automatically selects the extension.</p>  |

**Related topics:**

[Emergency Location Ext](#) on page 59

[IP Softphone](#) on page 71

[Emergency Location Extension](#) on page 674

[Remote Office Phone](#) on page 901

**Service Link Mode**

Determines the duration of the service link connection. The service link is the combined hardware and software multimedia connection between an Enhanced mode complex's H.320 DVC system and a server running Avaya Communication Manager that terminates the H.

320 protocol. When the user receives or makes a call during a multimedia or IP Softphone or IP Telephone session, a “service link” is established.

| Valid Entry | Usage  |
|-------------|--|
| as-needed   | Used for most multimedia, IP Softphone, or IP Telephone users. Setting the Service Link Mode to as-needed leaves the service link connected for 10 seconds after the user ends a call so that they can immediately place or take another call. After 10 seconds the link is dropped and a new link would have to be established to place or take another call. |
| permanent   | Used for busy call center agents and other users who are constantly placing or receiving multimedia, IP Softphone, or IP Telephone calls. In permanent mode, the service link stays up for the duration of the multimedia, IP Softphone, or IP Telephone application session.  |

### Loss Group

| Valid Entry | Usage   |
|-------------|---|
| 1 to 17     | Determines which administered two-party row in the loss plan applies to each station. Does not appear for stations that do not use loss — such as x-mobile stations and MASI terminals. |

### Speakerphone

Controls the behavior of speakerphones.

| Valid Entry | Usage   |
|-------------|---|
| 1-way       | Indicates that the speakerphone listen-only.  |
| 2-way       | Indicates that the speakerphone is both talk and listen.  |
| grp-listen  | Group Listen allows a telephone user to talk and listen to another party with the handset or headset while the telephone’s two-way speakerphone is in the listen-only mode. Others in the room can listen, but cannot speak to the other party through the speakerphone. The person talking on the handset acts as the spokesperson for the group. Group Listen provides reduced background noise and improves clarity during a conference call when a group needs to discuss what is being communicated to another party.<br>Available only with 6400-series and 2420/2410 telephones. |
| none        | Not administered for a speakerphone.  |

### LWC Reception

Indicates where Leave Word Calling (LWC) messages are stored.

| Valid Entry | Usage  |
|-------------|--|
| audix       | LWC messages are stored on the voice messaging system. |
| none        | LWC messages are not be stored.                        |

| Valid Entry | Usage   |
|-------------|---|
| spe         | LWC messages are stored in the system or on the switch processor element (spe). |

**Related topics:**

[AUDIX Name](#) on page 662

**Survivable COR**

Sets a level of restriction for stations to be used with the survivable dial plan to limit certain users to only to certain types of calls. You can list the restriction levels in order from the most restrictive to least restrictive. Each level assumes the calling ability of the ones above it. This field is used by PIM module of the Integrated Management to communicate with the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for Standard Local Survivability (SLS) on the H.248 gateways.

Available for all analog and IP station types.

| Valid Entries | Usage  |
|---------------|--|
| emergency     | This station can only be used to place emergency calls.  |
| internal      | This station can only make intra-switch calls. This is the default.  |
| local         | This station can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables.                                      |
| toll          | This station can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables.                                  |
| unrestricted  | This station can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users. |

**Related topics:**

[Survivable ARS Analysis Table](#) on page 919

**Time of Day Lock Table**

| Valid Entry | Usage   |
|-------------|---|
| 1 to 5      | Assigns the station to a Time of Day (TOD) Lock/Unlock table. The assigned table must be administered and active. |
| blank       | Indicates no TOD Lock/Unlock feature is active. This is the default.  |

**Survivable GK Node Name**

Any valid previously-administered IP node name. Identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the H.248 gateways. When a valid IP node name is entered into this field, Communication Manager adds the IP address of this gateway to the bottom of the Alternate Gatekeeper List for this IP network

region. As H.323 IP stations register with Communication Manager, this list is sent down in the registration confirm message. This allows the IP station to use the IP address of this Survivable Gatekeeper as the call controller of last resort.

If blank, there are no external gatekeeper nodes within a customer's network. This is the default value.

Available only if the station type is an H.323 station for the 46xx or 96xx models.

**Related topics:**

[Name](#) on page 700

[Type](#) on page 909

**Media Complex Ext**

When used with Multi-media Call Handling, indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to place either a voice or a data call, and voice conversion, coverage, and forwarding apply as if the call were made to the 1-number.

| Valid Entry                | Usage  |
|----------------------------|--|
| A valid BRI data extension | For MMCH, enter the extension of the data module that is part of this multimedia complex.  |
| H.323 station extension    | For 4600 series IP Telephones, enter the corresponding H.323 station. For IP Softphone, enter the corresponding H.323 station. If you enter a value in this field, you can register this station for either a road-warrior or telecommuter/Avaya IP Agent application. |
| blank                      | Leave this field blank for single-connect IP applications.   |

**AUDIX Name**

The voice messaging system associated with the station. Must contain a user-defined adjunct name that was previously administered.

**Related topics:**

[Name](#) on page 700

**Call Appearance Display Format**

Specifies the display format for the station. Bridged call appearances are not affected by this field. Use this field to Available only on telephones that support downloadable call appearance buttons, such as the 2420 and 4620 telephones.

 **Note:**

This field sets the administered display value only for an individual station.

| Valid Entry       | Usage  |
|-------------------|--|
| loc-param-default | The system uses the administered system-wide default value. This is the default. |

| Valid Entry    | Usage  |
|----------------|--|
| inter-location | The system displays the complete extension on downloadable call appearance buttons.                              |
| intra-location | The system displays a shortened or abbreviated version of the extension on downloadable call appearance buttons. |

**Related topics:**

[Display Parameters](#) on page 536

**IP Phone Group ID**

Available only for H.323 station types.

| Valid Entry       | Usage                                 |
|-------------------|---------------------------------------|
| 0 to 999<br>blank | The Group ID number for this station. |

**Always Use**

Enables or disables the following emergency call handling settings:

- A softphone can register no matter what emergency call handling settings the user has entered into the softphone. If a softphone dials 911, the administered **Emergency Location Extension** is used. The softphone's user-entered settings are ignored.
- If an IP telephone dials 911, the administered **Emergency Location Extension** is used.
- If a call center agent dials 911, the physical station extension is displayed, overriding the administered **LoginID for ISDN Display**.

Does not apply to SCCAN wireless telephones, or to extensions administered as type h.323.

**Related topics:**

[Emergency Location Ext](#) on page 59

**Audible Message Waiting**

Enables or disables an audible message waiting tone indicating the user has a waiting message consisting of a stutter dial tone when the user goes off-hook.

This field does *not* control the Message Waiting lamp.

Available only if **Audible Message Waiting** is enabled for the system.

**Related topics:**

[Audible Message Waiting](#) on page 944

**Auto Select Any Idle Appearance**

Enables or disables automatic selection of any idle appearance for transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being transferred or conferenced has. If that attempt fails, Communication Manager selects the first idle appearance.

**Bridged Call Alerting**

Controls how the user is alerted to incoming calls on a bridged appearance.

| Valid Entry | Usage   |
|-------------|---|
| y           | The bridged appearance rings when a call arrives at the primary telephone.  |
| n           | The bridged appearance flashes but does not ring when a call arrives at the primary telephone. This is the default.<br>If disabled and <b>Per Button Ring Control</b> is also disabled, audible ringing is suppressed for incoming calls on bridged appearances of another telephone's primary extension. |

**Related topics:**

[Per Button Ring Control](#) on page 72

**Bridged Idle Line Preference**

Specifies whether the selected line for incoming bridged calls is always an idle line.

| Valid Entry | Usage   |
|-------------|---|
| y           | The user connects to an idle call appearance instead of the ringing call. |
| n           | The user connects to the ringing call appearance.                         |

**CDR Privacy**

Enables or disables Call Privacy for each station. Allows digits in the called number field of an outgoing call record to be blanked on a per-station basis. The number of blocked digits is administered system-wide as CDR parameters.

**Related topics:**

[Privacy — Digits to Hide](#) on page 473

**Conf/Trans On Primary Appearance**

Enables or disables the forced use of a primary appearance when the held call to be conferenced or transferred is a bridge. This is regardless of the administered value for **Auto Select Any Idle Appearance** .

**Related topics:**

[Auto Select Any Idle Appearance](#) on page 68

**Coverage Msg Retrieval**

Allows or denies users in the telephone's Coverage Path to retrieve Leave Word Calling (LWC) messages for this telephone. Applies only if the telephone is enabled for LWC Reception.

**IP Video**

Enables or disables IP video capability for this signaling group. Available only if the signaling group type h.323 and sip.

**Data Restriction**

Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Cannot be assigned if **Auto Answer** is administered as all or acd. If enabled, whisper page to this station is denied.

**Related topics:**

[Auto Answer](#) on page 61

**Direct IP-IP Audio Connections**

Allows or denies direct audio connections between IP endpoints that saves on bandwidth resources and improves sound quality of voice over IP transmissions.

**Display Client Redirection**

Enables or disables the display of redirection information for a call originating from a station with Client Room Class of Service and terminating to this station. When disabled, only the client name and extension or room display. Available only if Hospitality is enabled for the system.

**Note:**

This field must be enabled for stations administered for any type of voice messaging that needs display information.

**Related topics:**

[Hospitality \(Basic\)](#) on page 946

[Hospitality \(G3V3 Enhancements\)](#) on page 946

**Select Last Used Appearance**

| Valid Entry | Usage   |
|-------------|---|
| y           | Indicates a station's line selection is not to be moved from the currently selected line button to a different, non-alerting line button. The line selection on an on-hook station only moves from the last used line button to a line button with an audibly alerting call. If there are no alerting calls, the line selection remains on the button last used for a call. |
| n           | The line selection on an on-hook station with no alerting calls can be moved to a different line button that might be serving a different extension.  |

**Survivable Trunk Dest**

Designates certain telephones as not being allowed to receive incoming trunk calls when the Media Gateway is in survivable mode. This field is used by the PIM module of the Integrated Management to successfully interrogate the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for SLS on the H.248 gateways.

Available for all analog and IP station types.

| Valid Entry | Usage  |
|-------------|--|
| y           | Allows this station to be an incoming trunk destination while the Media Gateway is running in survivability mode. This is the default. |
| n           | Prevents this station from receiving incoming trunk calls when in survivable mode.   |

### **H.320 Conversion**

Enables or disables the conversion of H.320 compliant calls made to this telephone to voice-only. Because the system can handle only a limited number of conversion calls, the number of telephones with H.320 conversion should be limited.

### **Idle Appearance Preference**

Indicates which call appearance is selected when the user lifts the handset and there is an incoming call.

| Valid Entry | Usage   |
|-------------|---|
| y           | The user connects to an idle call appearance instead of the ringing call.                       |
| n           | The Alerting Appearance Preference is set and the user connects to the ringing call appearance. |

### **IP Audio Hairpinning**

Enables or disables hairpinning for H.323 or SIP Enablement Services (SES) trunk groups. H.323 and SES-enabled endpoints are connected through the IP circuit pack without going through the time division multiplexing (TDM) bus. Available only if **Group Type** is h.323 or sip.

#### **Related topics:**

[Group Type](#) on page 860

### **IP Softphone**

Indicates whether or not this extension is either a PC-based multifunction station or part of a telecommuter complex with a call-back audio connection.

Available only for DCP station types and IP Telephones.

### **LWC Activation**

Activates or deactivates the Leave Word Calling (LWC) feature. LWC allows internal telephone users on this extension to leave short pre-programmed messages for other internal users.

LWC should be used if:

- The system has hospitality and the guest-room telephones require LWC messages indicating that wakeup calls failed
- LWC messages are stored in a voice-messaging system

### **LWC Log External Calls**

Determines whether or not unanswered external call logs are available to end users. When external calls are not answered, Communication Manager keeps a record of up to 15 calls

provided information on the caller identification is available. Each record consists of the latest call attempt date and time.

**Multimedia Early Answer**

Enables or disables multimedia early answer on a station-by-station basis.

The station should be enabled for this feature if the station receives coverage calls for multimedia complexes, but is not multimedia-capable. This ensures that calls are converted and the talk path is established before ringing at this station.

**Mute Button Enabled**

Enables or disables the mute button on the station.

**Per Button Ring Control**

Enables or disables per button ring control by the station user.

| Valid Entries | Usage   |
|---------------|---|
| y             | Allows users to select ring behavior individually for each call-appr, brdg-appr, or abrdg-appr on the station and to enable Automatic Abbreviated and Delayed ring transition for each call-appr on the station. Prevents the system from automatically moving the line selection to a silently alerting call unless that call was audibly ringing earlier. |
| n             | Calls on <b>call-appr</b> buttons always ring the station and calls on <b>brdg-appr</b> or <b>abrdg-appr</b> buttons always ring or not ring based on the <b>Bridged Call Alerting</b> value. Allows the system to move line selection to a silently alerting call if there is no call audibly ringing the station.   |

**Related topics:**

[Bridged Call Alerting](#) on page 68

**Precedence Call Waiting**

Activates or deactivates Precedence Call Waiting for this station.

**Redirect Notification**

Enables or disables redirection notification that gives a half ring at this telephone when calls to this extension are redirected through Call Forwarding or Call Coverage. Must be enabled if LWC messages are stored on a voice-messaging system.

**Related topics:**

[LWC Reception](#) on page 65

**Restrict Last Appearance**

| Valid Entries | Usage   |
|---------------|---|
| y             | Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only. |

| Valid Entries | Usage   |
|---------------|---|
| n             | Last idle call appearance is used for incoming priority calls and outgoing call originations. |

**EMU Login Allowed**

Enables or disables using the station as a visited station by an Enterprise Mobility User (EMU).

**Bridged Appearance Origination Restriction**

Restricts or allows call origination on the bridged appearance.

| Valid Entry | Usage   |
|-------------|---|
| y           | Call origination on the bridged appearance is restricted.   |
| n           | Call origination on the bridged appearance is allowed. This is normal behavior, and is the default. |

**Voice Mail Number**

The complete Voice Mail Dial Up number. Accepts up to 17 digits.

**Site Data**

This section lets you set information about the Room, Floor, Jack, Cable, Mounting, and Building.

**Room**

| Valid Entry               | Usage  |
|---------------------------|--|
| <i>Telephone location</i> | Identifies the telephone location. Accepts up to 10 characters.  |
| <i>Guest room number</i>  | Identifies the guest room number if this station is one of several to be assigned a guest room and the <b>Display Room Information in Call Display</b> is enabled for the system. Accepts up to five digits. |

**Related topics:**

[Display Room Information in Call Display](#) on page 642

**Floor**

A valid floor location.

**Jack**

Alpha-numeric identification of the jack used for this station.

**Cable**

Identifies the cable that connects the telephone jack to the system.

**Mounting**

Indicates whether the station mounting is d(esk) or w(all).

**Building**

A valid building location.

**Related topics:**

[Site Data](#) on page 877

**Set Color**

Indicates the set color. Valid entries include the following colors: beige, black, blue, brown, burg (burgundy), gray, green, ivory, orng (orange), red, teak, wal (walnut), white, and yel (yellow).

**Cord Length**

The length of the cord attached to the receiver. This is a free-form entry, and can be in any measurement units.

**Headset**

Indicates whether or not the telephone has a headset.

**Speaker**

Indicates whether or not the station is equipped with a speaker.

**Abbreviated Call Dialing**

This section lets you create abbreviated dialing lists for a specific station, and provide lists of stored numbers that can be accessed to place local, long-distance, and international calls; allows you to activate features or access remote computer equipment and select enhanced, personal, system or group lists.

**Abbreviated Dialing List 1, List 2, List 3**

Assigns up to three abbreviated dialing lists to each telephone.

| Valid Entry | Usage   |
|-------------|---|
| enhanced    | Allows the telephone user to access the enhanced system abbreviated dialing list.   |
| group       | Allows the telephone user to access the specified group abbreviated dialing list. Requires administration of a group number.                |
| personal    | Allows the telephone user to access and program their personal abbreviated dialing list. Requires administration of a personal list number. |
| system      | Allows the telephone user to access the system abbreviated dialing list.  |

**Personal List**

Establishes a personal dialing list for telephone or data module users. The personal list must first be assigned to the telephone by the System Administrator before the telephone user can add entries in the list. Users access the lists in order to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Example command: `change abbreviated-dialing personal`

### **Abbreviated Dialing Enhanced List**

Establishes system-wide or personal lists for speed dialing.

The Enhanced Abbreviated Dialing List can be accessed by users to place local, long-distance, and international calls; to activate or deactivate features; or to access remote computer equipment.

 **Note:**

Dialing must be enabled in the license file before the Enhanced List can be programmed.

Example command: `display abbreviated-dialing enhanced`

#### **Related topics:**

[Abbreviated Dialing Enhanced List](#) on page 942

### **Group List**

Implements the Abbreviated Dialing Group List. The System Administrator controls the Group Lists. Up to 100 numbers can be entered for every group list. Users can access this list to:

- Place local, long-distance, and international calls
- Activate or deactivate features
- Access remote computer equipment

Example command: `change abbreviated-dialing group`

### **Enhanced Call Fwd**

This section allows you to specify the destination extension for the different types of call forwards.

#### **Forwarded Destination**

A destination extension for both internal and external calls for each of the three types of enhanced call forwarding (Unconditional, Busy, and No Reply). Accepts up to 18 digits. The first digit can be an asterisk \*.

Requires administration to indicate whether the specific destination is active (enabled) or inactive (disabled).

### **SAC/CF Override**

Allows the user of a station with a **Team** button administered, who is monitoring another station, to directly reach the monitored station by pushing the **Team** button. This overrides any currently active rerouting, such as Send All Calls and Call Forwarding, on the monitored station.

| Valid Entries | Usage  |
|---------------|--|
| Ask           | The system asks if the user wants to follow the rerouting or override it. When the user has the option to decide whether rerouting should take place or not, a message is sent to the station that displays the active rerouting and the number of the forwarded to station. |

| Valid Entries | Usage   |
|---------------|---|
| No            | Cannot override rerouting. The station does not have the ability to override the rerouting of a monitored station.  |
| Yes           | Can override rerouting. The station has the ability to override the rerouting the monitored station has set, as long as one incoming call appearance is free. |

## Button Assignment

This section lets you assign features to the buttons on a phone. You can assign the main buttons for your station by choosing an option from the list down box for each button.

## Group Membership

This section describes the different groups that an extension can be a member of. You should select the station you want to group and then choose the group from the drop-down box, before clicking **Commit**.

## Understanding groups

Your voice system uses groups for a number of different purposes. This topic describes the different groups that an extension can be a member of. However, your voice system may include other types of groups as well (for example, trunk groups). For information on those groups, see the Administrator's Guide to Communication Manager Software.

Your voice system may have any of the following types of groups set up:

| Type                  | Description   |
|-----------------------|---|
| group page            | Group page is a feature that allows you to make an announcement to a pre-programmed group of phone users. The announcement is heard through the speakerphone built into some sets. Users will hear the announcement if their set is idle. Users cannot respond to the announcement. |
| coverage answer group | A coverage answer group lets up to 8 phones ring simultaneously when a call is redirected to the group.   |
| coverage path         | A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call. For more information on coverage paths, see "Creating Coverage Paths" in the Administrator's Guide to Communication Manager Software.                             |
| hunt group            | A hunt group is a group of extensions that receive calls according to the call distribution method you choose. When a call is made to a certain phone number, the system  |

|                             |   |
|-----------------------------|---|
|                             | <p>connects the call to an extension in the group. Use hunt groups when you want more than one person to be able to answer calls to the same number.</p> <p>For more information on hunt groups, see "Managing Hunt Groups" in the Administrator's Guide to Communication Manager Software.</p>   |
| intercom group              | <p>An intercom group is a group of extensions that can call each other using the intercom feature. With the intercom feature, you can allow one user to call another user in a predefined group just by pressing a couple of buttons.</p> <p>For more information on intercom groups, see "Using Phones as Intercoms" in the Administrator's Guide to Communication Manager Software.</p> |
| pickup group                | <p>A pickup group is a group of extensions in which one person may pick up another person's calls.</p> <p>For more information on pickup groups, see "Adding Call Pickup" in the Administrator's Guide to Communication Manager Software.</p>   |
| terminating extension group | <p>A Terminating Extension Group (TEG) allows an incoming call to ring as many as 4 phones at one time. Any user in the group can answer the call.</p> <p>For more information on terminating extension groups, see "Assigning a Terminating Extension Group" in the Administrator's Guide to Communication Manager Software.</p>   |

---

## Subscriber Templates (CMM) field descriptions

| Field                    | Description  |
|--------------------------|--|
| <b>Template name</b>     | Specifies the template of this subscriber template.                                  |
| <b>New Template Name</b> | Specifies the name of the duplicate template. You can enter the name of your choice. |
| <b>Type</b>              | Specifies the messaging type of the subscriber template.                             |
| <b>Software Version</b>  | Specifies the messaging version of the subscriber template.                          |

## Basic Information

| Field                | Description  |
|----------------------|--|
| <b>Last Name</b>     | Specifies the last name of the subscriber.   |
| <b>First Name</b>    | Specifies the first name of the subscriber.  |
| <b>Extension</b>     | <p>Specifies a number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must:</p> <ul style="list-style-type: none"> <li>• Be within the range of Extension Numbers assigned to your system.</li> <li>• Not be assigned to another local subscriber.</li> <li>• Be a valid length on the local machine.</li> </ul> |
| <b>Password</b>      | The default password that a user has to use to login to his/her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank  |
| <b>COS</b>           | The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop—down box.  |
| <b>Community ID</b>  | Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.  |
| <b>Switch Number</b> | <p>Specifies the number of the switch on which this subscriber's extension is administered. You can enter "0" through "99", or leave this field blank.</p> <ul style="list-style-type: none"> <li>• Leave this field blank if the host switch number should be used.</li> <li>• Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.</li> </ul>                     |
| <b>Account Code</b>  | Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.  |

## Subscriber Directory

| Field               | Description  |
|---------------------|--|
| <b>Email Handle</b> | Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. |
| <b>Common Name</b>  | Specifies the display name of the subscriber.  |

### Mailbox Features

| Field                     | Description  |
|---------------------------|--|
| <b>Covering Extension</b> | Specifies the number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank. |

### Secondary Extensions

| Field                      | Description  |
|----------------------------|--|
| <b>Secondary extension</b> | Specifies the number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension. |

### Miscellaneous

| Field         | Description  |
|---------------|--|
| <b>Misc 1</b> | Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 2</b> | Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 3</b> | Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 4</b> | Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Adds the subscriber template.                             |
| <b>Reset</b>  | Undoes all the changes.                                   |
| <b>Edit</b>   | Allows you to edit the fields.                            |
| <b>Done</b>   | Completes your action and takes you to the previous page. |
| <b>Cancel</b> | Takes you to the previous page.                           |

---

## Subscriber Templates (MM) field descriptions

| Field       | Description  |
|-------------|--|
| <b>Type</b> | Specifies the messaging type of the subscriber template. |

| Field                    | Description  |
|--------------------------|--|
| <b>New Template Name</b> | Specifies the name of the duplicate template. You can enter the name of your choice. |
| <b>Template name</b>     | Specifies the messaging template of a subscriber template.                           |
| <b>Software Version</b>  | Specifies the messaging version of the subscriber template.                          |

### Basic Information

| Field                   | Description   |
|-------------------------|---|
| <b>Last Name</b>        | Specifies the last name of the subscriber.  |
| <b>First Name</b>       | Specifies the first name of the subscriber.   |
| <b>Numeric Address</b>  | Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.  |
| <b>PBX Extension</b>    | The primary telephone extension of the subscriber.  |
| <b>Class Of Service</b> | The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. You can select an option from the drop-down box. |
| <b>Community ID</b>     | Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.                         |
| <b>Password</b>         | Specifies the default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.                                     |

### Subscriber Directory

| Field                   | Description   |
|-------------------------|---|
| <b>Email Handle</b>     | Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.   |
| <b>Telephone Number</b> | The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses (()) . |
| <b>Common Name</b>      | Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.   |

| Field                        | Description   |
|------------------------------|---|
| <b>ASCII Version of Name</b> | If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name. |

### Mailbox Features

| Field                             | Description  |
|-----------------------------------|--|
| <b>Backup Operator Mailbox</b>    | Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.  |
| <b>Personal Operator Schedule</b> | Specifies when to route calls to the backup operator mailbox. The default value for this field is <b>Always Active</b> .   |
| <b>TUI Message Order</b>          | Specifies the order in which the subscriber hears the voice messages. You can choose one of the following: <ul style="list-style-type: none"> <li>• <b>urgent first then newest:</b> to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received.</li> <li>• <b>oldest messages first:</b> to direct the system to play messages in the order they were received.</li> <li>• <b>urgent first then oldest:</b> to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received.</li> <li>• <b>newest messages first:</b> to direct the system to play messages in the reverse order of how they were received.</li> </ul> |
| <b>Intercom Paging</b>            | Specifies the intercom paging settings for a subscriber. You can choose one of the following: <ul style="list-style-type: none"> <li>• <b>paging is off:</b> to disable intercom paging for this subscriber.</li> <li>• <b>paging is manual:</b> if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber.</li> <li>• <b>paging is automatic:</b> if the TUI automatically allows callers to page the subscriber.</li> </ul>   |
| <b>Voicemail Enabled</b>          | Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following: <ul style="list-style-type: none"> <li>• <b>yes:</b> to allow the subscriber to create, forward, and receive messages.</li> <li>• <b>no:</b> to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The</li> </ul>   |

| Field | Description   |
|-------|---|
|       | subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber. |

## Secondary Extensions

| Field                      | Description   |
|----------------------------|---|
| <b>Secondary extension</b> | Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers. |

## Miscellaneous

| Field         | Description   |
|---------------|---|
| <b>Misc 1</b> | Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 2</b> | Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 3</b> | Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 4</b> | Specifies additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system. |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Adds the subscriber template.                             |
| <b>Reset</b>  | Undoes all the changes.                                   |
| <b>Edit</b>   | Allows you to edit the fields.                            |
| <b>Done</b>   | Completes your action and takes you to the previous page. |
| <b>Cancel</b> | Takes you to the previous page.                           |



# Chapter 7: Managing events

---

## Managing alarms

---

### Alarming

The Alarming service provides an interface for monitoring alarms generated by System Manager and other components. You can perform the following operations using the Alarming service:

- View an alarm
- Change the status of an alarm
- Export alarms to a Comma Separated Values (csv) file

System Manager generates alarms to notify users of system events. Alarms are classified by their effect on system operation and identify the system component which generated the alarm. System Manager can be configured to forward alarms to Avaya Services. It can also be configured to send SNMP traps to a customer Network Management System (NMS).

---

### Alarming field descriptions

The Alarming page displays a list of alarms. Use this page to view the alarms in the Auto-Refresh mode. In this mode, the page updates the alarm information automatically.

| Field             | Description  |
|-------------------|--|
| <b>Time Stamp</b> | Date and time when the alarm is generated.                   |
| <b>Severity</b>   | Severity of the alarm.                                       |
| <b>Status</b>     | Current status of the alarms.                                |
| <b>Host Name</b>  | The name of the host computer that generated the alarm.      |
| <b>Message</b>    | A short description of the problem that generated the alarm. |
| <b>Identifier</b> | Unique identifier for an alarm.                              |

| Field                 | Description  |
|-----------------------|--|
| <b>M/E Ref Number</b> | A unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm. |

| Button                    | Description   |
|---------------------------|---|
| <b>Alarm landing Page</b> | Switches the mode from Auto-Refresh to Manual refresh and displays the Alarming Home page. This is a toggle button. |

---

## Alarming field descriptions

The Alarming page has two sections; Upper and Lower. The upper section has buttons that you can use to view the details of the selected alarms, change the status of alarms, search for alarms, and set filters to view specific alarms. The lower section displays alarms in a table. The table provides information about the status of the alarms along with their severity. You can click a column title to sort the information in the table in ascending or descending order.

| Field                  | Description  |
|------------------------|--|
| <b>Time Stamp</b>      | Date and time when the alarm is generated.   |
| <b>Severity</b>        | Severity of the alarm.   |
| <b>Status</b>          | Current status of the alarms.  |
| <b>Host Name</b>       | The name of the host computer that generated the alarm.  |
| <b>Message</b>         | A short description of the problem that generated the alarm.   |
| <b>Identifier</b>      | Unique identifier for an alarm.  |
| <b>Agent Reference</b> | The reference number of the agent who has reported the alarm.  |
| <b>M/E Ref Number</b>  | A unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm. |

| Button                   | Description   |
|--------------------------|---|
| <b>View</b>              | Displays the details of the selected alarms.  |
| <b>Change Status</b>     | Changes the status of the selected alarm. The options are: <ul style="list-style-type: none"> <li>• Acknowledged</li> <li>• Clear</li> </ul>              |
| <b>Auto-Refresh Mode</b> | Switches to the Auto-Refresh mode. When the Alarming page is set in this mode, it automatically updates the alarms in the table. This is a toggle button. |

| Button                                   | Description  |
|--|--|
| <b>More Actions &gt; Export Selected</b> | Exports the selected alarms to a CSV file, which can be viewed with Wordpad or Excel.                  |
| <b>More Actions &gt; Export All</b>      | Exports all the alarms to to a CSV file, which can be viewed with Wordpad or Excel.                    |
| <b>Advanced Search</b>                   | Displays fields that you can use to specify the search criteria for searching an alarm.                |
| <b>Refresh</b>                           | Refreshes the log information in the table.  |
| <b>Filter: Enable</b>                    | Displays fields under select columns that you can use to set filter criteria. This is a toggle button. |
| <b>Filter: Disable</b>                   | Hides the column filter fields without resetting the filter criteria. This is a toggle button.         |
| <b>Filter: Clear</b>                     | Clears the filter criteria.  |
| <b>Filter: Apply</b>                     | Filters alarms based on the filter criteria.   |
| <b>All</b>                               | Selects all the alarms in the table.   |
| <b>None</b>                              | Clears the check box selections.   |
| <b>Previous</b>                          | Displays the logs in the previous page. This button is not available if you are on the first page.     |
| <b>Next</b>                              | Displays the logs in the next page. This button is not available if you are on the last page.          |

### Criteria section

This section appears when you click **Advanced Search** on the upper right corner of page.

| Name            | Description  |
|-----------------|--|
| <b>Criteria</b> | <p>Use this section to specify search conditions. Select the search criteria from the first drop-down list. Select the operator from the second drop-down field. Enter the search value in the text field.</p> <p>Select following search criteria from the first drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Time Stamp:</b> Searches all of the alarms that match the specified date and time. The valid format for entering the date is MM/DD/YYYY. The valid format for entering the time is HH:MM.</li> <li>• <b>Severity:</b> Searches all of the alarms that match the specified severity level.</li> <li>• <b>Status:</b> Searches all of the alarms that match the specified status.</li> <li>• <b>Host Name:</b> Searches all of the alarms that are generated from the specified host.</li> <li>• <b>Identifier:</b> Searches all of the alarms that match the specified identifier.</li> </ul> |

| Name           | Description  |           |           |            |                         |          |                    |        |                    |           |  |            |                         |         |  |                |  |
|----------------|--|-----------|-----------|------------|-------------------------|----------|--------------------|--------|--------------------|-----------|--|------------|-------------------------|---------|--|----------------|--|
|                | <ul style="list-style-type: none"> <li>• Message: Searches all of the alarms that match the specified message.</li> <li>• M/E Ref Number: Searches all of the alarms that match the specified M/E Ref Number.</li> </ul> <p>The operators available are based on the search criterion that you select in the first drop-down field. The following table list the operators that are available for a search criterion:</p> <table border="1" data-bbox="412 512 1256 1005"> <thead> <tr> <th data-bbox="412 512 618 556">Criterion</th> <th data-bbox="618 512 1256 556">Operators</th> </tr> </thead> <tbody> <tr> <td data-bbox="412 556 618 604">Time Stamp</td> <td data-bbox="618 556 1256 604">=, &gt;, &lt;, &gt;=, &lt;=, &gt;=, !=</td> </tr> <tr> <td data-bbox="412 604 618 653">Severity</td> <td data-bbox="618 604 1256 653">Equals, Not Equals</td> </tr> <tr> <td data-bbox="412 653 618 701">Status</td> <td data-bbox="618 653 1256 701">Equals, Not Equals</td> </tr> <tr> <td data-bbox="412 701 618 787">Host Name</td> <td data-bbox="618 701 1256 787">Equals, Not Equals, Starts With, Ends With, and Contains</td> </tr> <tr> <td data-bbox="412 787 618 835">Identifier</td> <td data-bbox="618 787 1256 835">=, &gt;, &lt;, &gt;=, &lt;=, &gt;=, !=</td> </tr> <tr> <td data-bbox="412 835 618 921">Message</td> <td data-bbox="618 835 1256 921">Equals, Not Equals, Starts With, Ends With, and Contains</td> </tr> <tr> <td data-bbox="412 921 618 1005">M/E Ref Number</td> <td data-bbox="618 921 1256 1005">Equals, Not Equals, Starts With, Ends With, and Contains</td> </tr> </tbody> </table> <p>When you select Begin Date and End Date from the first drop-down list, you are prompted to enter the date in the third field.</p> | Criterion | Operators | Time Stamp | =, >, <, >=, <=, >=, != | Severity | Equals, Not Equals | Status | Equals, Not Equals | Host Name | Equals, Not Equals, Starts With, Ends With, and Contains | Identifier | =, >, <, >=, <=, >=, != | Message | Equals, Not Equals, Starts With, Ends With, and Contains | M/E Ref Number | Equals, Not Equals, Starts With, Ends With, and Contains |
| Criterion      | Operators  |           |           |            |                         |          |                    |        |                    |           |  |            |                         |         |  |                |  |
| Time Stamp     | =, >, <, >=, <=, >=, !=  |           |           |            |                         |          |                    |        |                    |           |  |            |                         |         |  |                |  |
| Severity       | Equals, Not Equals   |           |           |            |                         |          |                    |        |                    |           |  |            |                         |         |  |                |  |
| Status         | Equals, Not Equals   |           |           |            |                         |          |                    |        |                    |           |  |            |                         |         |  |                |  |
| Host Name      | Equals, Not Equals, Starts With, Ends With, and Contains   |           |           |            |                         |          |                    |        |                    |           |  |            |                         |         |  |                |  |
| Identifier     | =, >, <, >=, <=, >=, !=  |           |           |            |                         |          |                    |        |                    |           |  |            |                         |         |  |                |  |
| Message        | Equals, Not Equals, Starts With, Ends With, and Contains   |           |           |            |                         |          |                    |        |                    |           |  |            |                         |         |  |                |  |
| M/E Ref Number | Equals, Not Equals, Starts With, Ends With, and Contains   |           |           |            |                         |          |                    |        |                    |           |  |            |                         |         |  |                |  |

| Button                       | Description  |
|------------------------------|--|
| <b>Clear</b>                 | Clears the entered search criteria and sets the default search criteria. |
| <b>Search</b>                | Searches the alarms based on the search conditions.                      |
| <b>Close/Advanced Search</b> | Hides the search fields.   |
| <b>+</b>                     | Adds a search condition.   |
| <b>-</b>                     | Deletes a search condition.  |

---

## Viewing alarms

- 
1. On the System Manager console, click **Events** > **Alarms** in the left navigation pane.
  2. Select an alarm. You can select multiple alarms.
  3. Click **View**.
- 

---

## Changing status of an alarm

The status of an alarm can be:

- **Acknowledged** – Maintenance support must manually set the alarm to this state, indicating the alarm is under investigation.
- **Cleared** – Maintenance support must manually set the alarm to this state, indicating that the error condition has been resolved.

- 
1. On the System Manager console, click **Events** > **Alarms** in the left navigation pane.
  2. On the Alarming page, select an alarm and click **Change Status**.  
You can select multiple alarms.
  3. Click on the status that you want to apply to the selected alarms.
- 

---

## Exporting alarms

Alarms can be exported to a Comma Separated Values (csv) file. You can open the CSV file using a text editor such as Wordpad or a spreadsheet application such as Excel.

- 
1. On the System Manager console, click **Events** > **Alarms** in the left navigation pane.
  2. On the Alarming page, perform one of the following steps:
    - To export a selected alarm to a CSV file, select an alarm and click **More Actions** > **Export Selected**.

- To export all the alarms to a CSV file, click **More Actions > Export All**.
3. Click **Save** to save the exported file to the local disk.
- 

---

## Filtering alarms

The criteria for filtering the alarms are Severity, Status, Host Name, Message, Identifier, and M/E Ref Number. You can use more than one filter criterion on the selected alarms.

- 
1. On the System Manager console, click **Events > Alarms** in the left navigation pane.
  2. On the Alarming page, select the alarms you want to filter.
  3. Click **Filter: Enable** at the top right corner of the alarm log table.
  4. Select the filter criteria you want to apply to the selected alarms.  
The **Status** and **Severity** fields have drop-down menus.  
You can enter the alarm code in the Message field to find all alarms which contain a particular alarm code.
  5. Click **Filter: Apply**.



**Note:**

A message will be displayed if no records are found which match the specified filter criteria.

---

### Result

The page displays the alarms matching the filter criteria.

---

## Searching for alarms

Use the Advanced Search function to find alarms based on certain specified conditions. The system displays only those alarms which satisfy the search conditions. Multiple search conditions can be specified.

- 
1. On the System Manager console, click **Events > Alarms** in the left navigation pane.
  2. On the Alarming page, click **Advanced Search**.

3. In the Criteria section, from the first and second drop-down fields, select the search criterion and the operator.

The default value in the first drop-down field is **Time Stamp**.

4. Select or enter the search value in the third field.
5. If you want to add another search condition, click **+** and do the following:
  - a. Select the AND or OR operator from the drop-down field.
  - b. Repeat steps 3 and 4.

Click **-** to delete a search condition. You can delete a search condition only if you have added more than one search condition.

6. Click **Search** to find alarms for the given search conditions.
- 

---

## Managing logs

---

### Logging

The logging service provides an interface for viewing logs and their details generated by System Manager or other components. The System Manager console allows you to monitor log messages. The log viewer displays a list of logs. You can view details of each log, perform a search for logs, and filter specific logs. Log detail includes information about the event which generated the log, the severity level of the log, and other relevant information. You can search logs based on search conditions and set filters to view logs that match the filter criteria. Log viewer displays only logs that are of type Audit.

---

### Log Types

Following are some of the log types that you may come across when viewing logs on the System Manager console. You can view the stations specific logs in the `/var/log/Avaya/mgmt/iptcm` directory.

#### **Security**

Security loggers gather security logs.

#### **Audit**

Audit loggers gather audit logs.

### **Operation**

Operational loggers gather operational logs.

### **Debug**

Debug loggers collect debug information to troubleshoot issues at the customer site. These loggers have been categorized based on the Communication System Management components.

### **Debug.Station**

Debug Station loggers gather debug information for station management related operations.

### **Debug.Template**

Template Debug loggers gather debug information for template management related operations.

### **Debug.CM**

CM debug loggers gather debug information for communication between Communication Manager and the Communication System Management server.

### **Debug.NCM**

NCM debug logger gathers debug information related to Element Cut Through.

### **Debug.Synch**

Synch debug logger gathers debug information for synchronization operations.

### **Debug.Model**

Model debug logger gathers debug information for database operations.

### **Debug**

Debug logger gathers debug information other than that gathered for the debug types mentioned above.

---

## **Viewing log details**

- 
1. On the System Manager console, click **Events** > **Logs** > **Log Viewer** in the left navigation pane.
  2. On the Logging page, select a log.
  3. Click **View**.
-

---

## Searching for logs

Use the Advanced Search function to find logs based on certain specified conditions. The system displays only those logs which satisfy the search conditions. Multiple search conditions can be specified.

- 
1. On the System Manager console, click **Events** > **Logs** > **Log Viewer** in the left navigation pane.
  2. On the Logging page, click **Advanced Search**.
  3. In the *Criteria* section, from the first and second drop-down fields, select the search criterion and the operator.
  4. Select or enter the search value in the third field.
  5. If you want to add another search condition, click **+** and repeat the steps 4 through 6.  
Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.
  6. Select the AND or OR operator from the drop-down field.  
This page displays this drop-down field when you specify more than one search condition.
  7. Click **Search** to find the logs for the given search conditions.
- 

---

## Filtering logs

You can filter and view logs that meet the specified filter criteria. Applying the filters requires you to specify the filter criteria in the fields provided under select columns in the table displaying the logs. The column titles are the filter criteria. You can filter logs on multiple filter criteria.

- 
1. On the System Manager console, click **Events** > **Logs** > **Log Viewer** in the left navigation pane.
  2. On the Logging page, click **Filter: Enable**.  
You can find this button on the top right corner in the table displaying logs.
  3. Enter or select the filter criteria.
  4. Click **Filter: Apply**.



**Note:**

If no records matching the filter criteria are found, the Management Console application displays a message that no records matching the search criteria are found.

---

**Result**

The page displays the logs that matches the specified filter criteria.

---

**Logging field descriptions**

The Logging page has two sections. The upper section contains buttons that allow you to view the details of the selected logs, search for logs, and set filters. The lower section displays logs in a table. The table provides information about the logs. You can click the title of the column to sort the data of the column in ascending or descending order.

| Name                    | Description  |
|-------------------------|--|
| <b>Select check box</b> | Use this check box to select a log.  |
| <b>Log ID</b>           | Unique identification number that identifies the log.  |
| <b>Time Stamp</b>       | Date and time of the log generation.   |
| <b>Host Name</b>        | Name of the system from which the log is generated.  |
| <b>Product Type</b>     | A code which uniquely identifies the component which generated the log. For example, product, device, application, service and so on. GW600, which is a product type code identifier is an example of the log product type.  |
| <b>Severity</b>         | Severity level of the log. The following are the type of severities: <ul style="list-style-type: none"> <li>• Emergency : System is unusable</li> <li>• Alert : Action must be taken immediately</li> <li>• Critical : Critical conditions</li> <li>• Error : Error conditions</li> <li>• Warning : Warning conditions</li> <li>• Notice: Normal but significant condition</li> <li>• Informational : Informational messages</li> <li>• Debug: Debug-level messages</li> </ul> |

| Name                | Description   |
|---------------------|---|
|                     |  <b>Note:</b><br>The colors of severities do not indicate logging severities.  |
| <b>Event ID</b>     | Unique identification number assigned to the event that has generated the log.  |
| <b>Message</b>      | Brief description about the log. The message is generated based on the severity level of the log. For a log with severity level debug, the message contains information about debugging an error.   |
| <b>Process Name</b> | Process on the device that has generated the message. This is usually the process name and process ID.  |
| <b>Facility</b>     | The operating system, processes, and applications quantify messages into one of the several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The following are the types of supported facilities: <ul style="list-style-type: none"> <li>• User-Level Messages</li> <li>• Security/authorization</li> <li>• Log Audit</li> </ul> |

| Button                   | Description  |
|--------------------------|--|
| <b>View</b>              | Opens the Log - View Log Detail page. Use this page to view the details of a selected log.   |
| <b>Auto-Refresh Mode</b> | Switches to the Auto-Refresh mode. When the Logging page is set in this mode, it automatically updates the logs in the table. This is a toggle button. |
| <b>Advanced Search</b>   | Displays fields that you can use to specify the search criteria for searching a log.   |
| <b>Refresh</b>           | Refreshes the log information in the table.  |
| <b>Filter: Enable</b>    | Displays fields under select columns that you can use to set filter criteria. This is a toggle button.   |
| <b>Filter: Disable</b>   | Hides the column filter fields without resetting the filter criteria. This is a toggle button.   |
| <b>Filter: Clear</b>     | Clears the filter criteria.  |
| <b>Filter: Apply</b>     | Filters logs based on the filter criteria.   |
| <b>Select: All</b>       | Selects all the logs in the table.   |
| <b>Select: None</b>      | Clears the selections.   |
| <b>Previous</b>          | Displays logs in the previous page. This button is not available if you are on the first page.   |

| Button | Description   |
|--------|---|
| Next   | Displays logs in the next page. This button is not available if you are on the last page. |

### Criteria section

This section appears when you click **Advanced Search** on the top right corner.

| Name     | Description   |
|----------|---|
| Criteria | <p>Use this section to specify search conditions. Select the search criteria from the first drop-down field. Select the operator from the second drop-down field. Enter the search value in the text field.</p> <p>Select following search criteria from the first drop-down field:</p> <ul style="list-style-type: none"> <li>• Log ID: The unique identification number assigned to the log.</li> <li>• Host Name: Name of the system for which log is generated.</li> <li>• Product type: A code which uniquely identifies the component which generated the log. For example, product, device, application, service, and so on.</li> <li>• Severity: Severity level of the log.</li> <li>• Message: Brief description about the log.</li> <li>• Event ID: Unique identification number assigned to the event.</li> <li>• Process Name: Process on the device that has generated the message</li> <li>• Time Stamp: Date and time of the log generation.</li> <li>• Facility: The operating systems, processes, and applications quantify messages into one of several categories. These categories generally consist of the facility that generated them, along with the severity of the message.</li> </ul> <p>The second drop-down field displays operators. Based on the search criterion that you select in the first drop-down field, only those operators that are applicable for the selected criterion are displayed in the second drop-down field. The following are the list of operators:</p> <ul style="list-style-type: none"> <li>• Equals</li> <li>• Not Equals</li> <li>• Starts With</li> <li>• Ends With</li> <li>• Contains</li> </ul> <p>The operators for Time Stamp are: =, &gt;, &lt;, &gt;=, &lt;=, and !=.</p> <p>When you select Time Stamp from the first drop-down field, the page provides date and time fields for entering the date and time in the respective fields. Enter the date in MM/DD/YYYY format . You can select the date from the calender. You need to enter the time in one of the following format:</p> |

| Name | Description  |
|------|--|
|      | <ul style="list-style-type: none"> <li>• 24Hr</li> <li>• AM</li> <li>• PM</li> </ul> |

| Button                       | Description  |
|------------------------------|--|
| <b>Clear</b>                 | Clears the search criterion and set it to the default search criteria. |
| <b>Search</b>                | Searches the logs based on the search conditions.                      |
| <b>Close/Advanced Search</b> | Hides the search fields.   |
| <b>+</b>                     | Adds a search condition.   |
| <b>-</b>                     | Deletes a search condition   |

---

## Logging field descriptions

Use this page to view logs in the Auto-Refresh mode. In this mode, the page updates the log information automatically.

| Name                | Description  |
|---------------------|--|
| <b>Log ID</b>       | Unique identification number that identifies the log.  |
| <b>Time Stamp</b>   | Date and time of the log generation.   |
| <b>Host Name</b>    | Name of the system from which the log is generated.  |
| <b>Product Type</b> | A code which uniquely identifies the component which generated the log. For example, product, device, application, service and so on. GW600, which is a product type code identifier is an example of the log product type.  |
| <b>Severity</b>     | Severity level of the log. The following are the type of severities: <ul style="list-style-type: none"> <li>• Emergency : System is unusable</li> <li>• Alert : Action must be taken immediately</li> <li>• Critical : Critical conditions</li> <li>• Error : Error conditions</li> <li>• Warning : Warning conditions</li> <li>• Notice: Normal but significant condition</li> <li>• Informational : Informational messages</li> <li>• Debug: Debug-level messages</li> </ul> |

| Name                | Description   |
|---------------------|---|
|                     |  <b>Note:</b><br>The colors of severities do not indicate logging severities.  |
| <b>Event ID</b>     | Unique identification number assigned to the event that has generated the log.  |
| <b>Message</b>      | Brief description about the log. The message is generated based on the severity level of the log. For a log with severity level debug, the message contains information about debugging an error.   |
| <b>Process Name</b> | Process on the device that has generated the message. This is usually the process name and process ID.  |
| <b>Facility</b>     | The operating system, processes, and applications quantify messages into one of the several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The following are the types of supported facilities: <ul style="list-style-type: none"> <li>• User-Level Messages</li> <li>• Security/authorization</li> <li>• Log Audit</li> </ul> |

| Button                      | Description  |
|-----------------------------|--|
| <b>Logging Landing Page</b> | Switches the mode from Auto-Refresh to manual refresh and displays the Logging Home page. This is a toggle button. |

---

## Managing log settings

---

### Accessing the Log Settings service

1. Log in to the System Manager web interface as an administrator.
2. On the System Manager console, click **Events > Logs > Log Settings** in the left navigation pane.  
 The system displays the Log Settings page.

---

## Viewing loggers for a log file

1. On the System Manager console, click **Events > Logs > Log Settings** in the left navigation pane.
2. On the Logging Configuration page, click a log file from the **Select Log File** field.

---

### Result

You can view the loggers in the Logger List section.

### Related topics:

[Logging Settings field descriptions](#) on page 1109

---

## Logging Settings field descriptions

Use this page to view and edit loggers defined in a log file.

### Log Configuration

| Name                   | Description   |
|------------------------|---|
| <b>Select Log File</b> | The field lists the log files that you can configure. |

### Logger List

| Name                                     | Description  |
|--|--|
| <b>Logger</b>                            | The loggers in the selected log files.   |
| <b>Log level</b>                         | Log level defines as to what level of logging is set for the corresponding logger. |
| <b>Attached Appenders &gt; Name</b>      | Name of the appender.  |
| <b>Attached Appenders &gt; File Path</b> | The path of the file to which the appender logs the information.                   |
| <b>Attached Appenders &gt; Facility</b>  | The process running on the machine that created the log message.                   |
| <b>Attached Appenders &gt; host</b>      | The name of the syslog host where the log output is stored.                        |

| Name     | Description  |
|----------|--|
| Show All | Provides you an option to select the maximum number of logger records that you can view at a time. |

| Button | Description  |
|--------|--|
| Edit   | Opens the Edit Logger page that you can use to edit loggers. |

**Related topics:**

[Viewing loggers for a log file](#) on page 1109

---

## Editing a logger in a log file

You can set log levels for loggers which define as to what level of logging the logger logs.

- 
1. On the System Manager console, click **Events > Logs > Log Settings** in the left navigation pane.
  2. On the Log Settings page, select a log file from the **Select Log File** field.
  3. Click a logger in the **Logger List** section.
  4. Click **Edit** .
  5. On the Edit logger page, in the **Log Level** field select a log level.
  6. Click **Commit** .  
The log level is set for the selected logger.

---

**Related topics:**

[Edit Logger field descriptions](#) on page 1112

## Assigning an appender to a logger

The appender where logger logs the log messages.

- 
1. On the System Manager console, click **Events > Logs > Log Settings** in the left navigation pane.
  2. On the Log Settings page, select a log file from the **Select Log File** field.
  3. Click a logger in the **Logger List** section.
  4. Click **Edit**.

5. On the Edit logger page, click **Attach** in the **Attached Appenders** section.
6. On the Attach Appender page, click an appender in the **Select Appender** field.
7. Click **Commit**.  
The appender is added to the selected logger and you can view the appender on the Log Settings page.

---

**Related topics:**

[Attach Appender field descriptions](#) on page 1114

## Modifying an appender

---

1. On the System Manager console, click **Events > Logs > Log Settings** in the left navigation pane.
2. On the Logging Configuration page, click a log file from the **Select Log File** field.
3. Click a logger in the **Logger List** section.
4. Click **Edit**.
5. On the Edit logger page, click an appender in the **Attached Appenders** section.
6. Click **Edit**.
7. On the Edit Appender page modify the appender information.

**Note:**

You can modify information in the following fields: **Threshold Log Level**, **Max File Size**, **File Path**, and **Number Of Backup Files**.

8. Click **Commit**.

---

**Related topics:**

[Edit Appender field descriptions](#) on page 1113

## Removing an appender from a logger

---

1. On the System Manager console, click **Events > Logs > Log Settings** in the left navigation pane.
2. On the Log Settings page, click a log file from the **Select Log File** field.

3. Click a logger in the **Logger List** section.
  4. Click **Edit**.
  5. On the Edit logger page, click an appender in the **Attached Appendors** section.
  6. Click **Detach**.
- 

## Edit Logger field descriptions

Use this page to edit logger and appender information. You can also add and remove appenders from the loggers.

### Logger

| Name             | Description   |
|------------------|---|
| <b>Logger</b>    | The name of the logger.   |
| <b>Log level</b> | The level of logging for which the logger logs the information. |

### Attached Appender

| Name                       | Description   |
|----------------------------|---|
| <b>Appender</b>            | The name of the appender.   |
| <b>Threshold Log Level</b> | The threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level .   |
| <b>File Path</b>           | The path of the file where the appender logs the information.   |
| <b>Max File Size</b>       | The maximum size in KB, MB, and GB reserved for the appender file.  |
| <b># Backup Files</b>      | The number of log files that an appender can use to store log information if one log file becomes full. If all the backup files are full, the appender overwrites the previous backup files in the order the files are created. |
| <b>Facility</b>            | The process running on the machine for which log messages are created.  |
| <b>Host</b>                | The name of the syslog host that stores the log output.   |
| <b>Header</b>              | The header part of the syslog packet. The header part contains timestamp and host name information.   |
| <b>Facility Printing</b>   | The printed message includes the facility name of the application.  |

| Button        | Description   |
|---------------|---|
| <b>Edit</b>   | Opens the Edit Appender page. Use this page to modify the appender information.   |
| <b>Attach</b> | Opens the Attach Appender page. Use this page to add an appender to the logger.   |
| <b>Detach</b> | Removes the selected appender from the logger.                                    |
| <b>Commit</b> | Saves the changes in the logger information to the database.                      |
| <b>Cancel</b> | Closes the Edit Logger page and takes you back to the Logging Configuration page. |

## Edit Appender field descriptions

Use this page to edit information of an appender.

| Name                       | Description   |
|----------------------------|---|
| <b>Logger</b>              | The name of the logger.<br> <b>Note:</b><br>You can only view this information.  |
| <b>Appender</b>            | The name of the appender.<br> <b>Note:</b><br>You can only view this information.  |
| <b>Threshold Log Level</b> | The threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level .   |
| <b>File Path</b>           | The path of the file where the appender logs the information.   |
| <b>Max File Size</b>       | The maximum KB, MB, and GB reserved for the appender file.  |
| <b># Backup Files</b>      | The number of log files that an appender can use to store log information if one log file becomes full. If all the backup files are full, the appender overwrites the previous backup files in the order the files are created. |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Saves the changes to the database.                                    |
| <b>Cancel</b> | Closes Edit Appender page and takes you back to the Edit Logger page. |

## Attach Appender field descriptions

Use this page to assign an appender to the logger.

| Name                   | Description   |
|------------------------|---|
| <b>Logger</b>          | The name of the logger.   |
| <b>Log Level</b>       | The level of logging for which the logger logs the information. |
| <b>Select Appender</b> | The list of appenders that you can assign to the logger.        |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Assigns the appender to the logger.  |
| <b>Cancel</b> | Closes the <b>Attach Appender</b> page and takes you back to the Edit Logger page. |

---

## Managing harvested logs

---

### Log Harvester

You can harvest log files for one or more products of same or different types running on a same computer or on different computers. You can perform the following operations:

- Create a log harvesting profile to specify the products for which you want to harvest the logs
- Submit the log harvesting request defined in a profile to the product
- View the status of the log harvesting request
- Store the harvested log files of a product in an archive file
- View the harvested log files stored in the archive file
- Download the harvested log files on to the local computer
- Search for a matching text in the harvested log files

---

## Accessing log harvest

- 
1. Log in to the System Manger console as an administrator.
  2. Click **Events** in the left navigation pane on the System Manager console.
  3. Click **Logs > Log Harvester**.
- 

---

## Creating a new log harvesting profile

You can create a new log harvesting profile by specifying the:

- IP address of the computer on which the product is running
- Product name
- Directories or log files
- Filter text if you have selected one or more directories

You can harvest log files for products running on different computers by specifying multiple search criteria.

- 
1. On the System Manager console, click **Events > Logs > Log Harvester** in the left navigation pane.
  2. On the **Log Harvesting** page, click **New**.
  3. On the **Create New Profile** page, enter the appropriate information in the **Create New Profile** and **Profile Description** fields.
  4. Select the IP address of the computer, product, and directories or files from the respective fields.  
To select multiple directories or files from the respective list boxes, press the **CTRL** key and click the individual directories or files. To clear a selection, press the **CTRL** key and click the selected item.  
You can use the **+** button to add another log harvesting request for another product or for another instance of the same product running on the same computer or on a different computer.
  5. If you have selected one or more directories, enter a text pattern as the filter criteria in the text box below the **Directories / Filter Text** list box field.

During the harvesting operation, the system harvests only those files that match the filter text.

6. Click **Save Profile** to save the profile and the log harvesting requests in the profile.

---

**Related topics:**

[Create New Profile field descriptions](#) on page 1123

---

## Viewing the harvested log files in an archive

You can view the harvested log files of a product stored in an archive file.

- 
1. On the System Manager console, click **Events > Logs > Log Harvester** in the left navigation pane.
  2. On the Log Harvesting page, select a log harvesting profile.
  3. Click **Requests**.
  4. On the Harvest Archives page, select a log harvesting request from the table in the Harvest Criteria View section.
  5. Click **Show files**.  
On the **Search Archives** page, navigate the folders in the archive to view the harvested log files.

---

## Deleting a profile

You can not delete a profile that is in use by the Log Harvester service. If you attempt to delete a profile that is in use , the system displays an error message.

- 
1. On the System Manager console, click **Events > Logs > Log Harvester** in the left navigation pane.
  2. On the **Log Harvesting** page, select a profile.
  3. Click **Delete**.
  4. On the Profile Delete Confirmation page, click **Delete**.
-

---

## Submitting a request for harvesting log files

Use this feature to submit a log harvesting request to one or more products running on the same or different computers. After the request is successfully processed, the system on which the products are installed returns the harvested log files that are specified in the request. When you select a profile and click the Request button, the system generates a single request for all the requests contained in the profile.

- 
1. On the System Manager console, click **Events > Logs > Log Harvester** in the left navigation pane.
  2. On the **Log Harvesting** page, select a profile and click **Requests**.
  3. On the **Harvest Archives** page, enter the relevant information in the **Archive Name** and **Archive Description** fields.  
The system saves the harvested log files in the specified archive file.
  4. Click **Run Profile** to send a request.  
The table in the Harvest Criteria View section provides you the status of the log harvesting request. If the execution status of the request is successful, then the system creates a zip file containing the harvested log files and saves the file in the specified location.

---

### Related topics:

[Harvest Archives field descriptions](#) on page 1124

---

## Viewing details of a log harvesting request

- 
1. On the System Manager console, click **Events > Logs > Log Harvester** in the left navigation pane.
  2. On the **Log Harvesting** page, select a profile and click **Requests**.
  3. On the **Harvest Archives** page, click a request in the table in the Harvest Criteria View section.  
If the table does not display any request, you need to submit a new request.
  4. Click **View**.  
The **Harvest - View Harvest detail** page displays the details of the selected request.
-

**Related topics:**

[Harvest - View Harvest detail field descriptions](#) on page 1126

---

## Searching for a text in a log file

Use this feature to search for a matching text in a log file of a product.

- 
1. On the System Manager console, click **Events > Logs > Log Harvester** in the left navigation pane.
  2. On the Log Harvesting page, select a log harvesting profile.
  3. Click **Requests**.
  4. On the Harvest Archives page, select a log harvesting request from the table in the Harvest Criteria View section.  
You must select a log harvesting request for which logs are successfully harvested.
  5. On the **Search Archives** page, in the **Enter search text** field enter the text that you want to search for.
  6. In the tree view navigate to the log file by expanding the folders and select the log file.
  7. Click **Search**.  
The system displays the search results in the Search Result Panel. The **Search Result Panel** field displays the line numbers as hyperlinks on which the searched text is found.
  8. Click a line number in the **Search Result Panel** field.  
When you click the line number, the system displays the line containing the searched text at the top in the **Log Browser Panel** field.

---

**Related topics:**

[Search Archives field descriptions](#) on page 1126

---

## Viewing the contents of the harvested log files

Use this feature to view the log messages stored in the harvested log files for a product. You can view the contents of one log file at a time.

- 
1. On the System Manager console, click **Events > Logs > Log Harvester** in the left navigation pane.
  2. On the Log Harvesting page, select a profile and click **Requests**.
  3. On the Harvest Archives page, click a request in the table in the Harvest Criteria View section.  
If the table does not display any request, you need to submit a new request.
  4. Click **Show Files**.
  5. On the Search Archives page select a harvested log file.  
The system displays an error message if you select a product name, IP Address of a computer on which a product is installed or a directory.
  6. Click **Search**.

---

**Related topics:**

[Search Archives field descriptions](#) on page 1126

---

## Downloading harvested log files

Use this feature to download the harvested log files of one or more products stored in a zip file on your local computer.

- 
1. On the System Manager console, click **Events > Logs > Log Harvester** in the left navigation pane.
  2. On the Log Harvesting page, select a profile and click **Requests**.
  3. On the Harvest Archives page, click a request in the table in the Harvest Criteria View section.  
If the table does not display any request, you need to submit a new request.
  4. Click **Show Files**.
  5. On the Search Archives page, select a product name, IP Address of the computer on which one or more products are running or a directory.  
If you select a product name, the system creates a zip file containing the harvested log files for the selected product instances running on the same computer or on different computers.  
If you select an IP Address of a computer under a product, the system create a zip file that contains the harvested log files for the products running on the selected computer.

If you select a directory, the system creates a zip file containing the harvested log files under the selected directory.

6. Click **Download**.

The system prompts you save the file on your local computer.

7. Click **Save**.

---

**Related topics:**

[Search Archives field descriptions](#) on page 1126

---

## Filtering log harvesting profiles

Use this feature to set filter criteria to view only those log harvesting profiles that meet the set filter criteria. The titles of the columns of the table that displays the log harvesting profiles are the filter criteria.

- 
1. On the System Manager console, click **Events > Logs > Log Harvester** in the left navigation pane.
  2. On the **Log Harvesting** page, click **Filter: Enable**.  
You can find this button at the top right of the table containing log harvesting profiles.
  3. Enter or select the filter criteria.  
You can filter the log harvesting profiles by the name, description and creator of the profiles.
  4. Click **Filter: Apply**.



**Note:**

If no records matching the filter criteria are found, the Log Harvesting page displays a message that no records matching the search criteria are found.

---

### Result

The log harvesting profile table displays the profiles that matches the specified filter criteria.

---

## Filtering log harvesting requests

Use this feature to set filter criteria to view only those log harvesting requests that meet the set filter criteria. The titles of the columns of the table that displays the log harvesting requests are the filter criteria.

- 
1. On the System Manager console, click **Events > Logs > Log Harvester** in the left navigation pane.
  2. On the Log Harvesting page, select a log harvesting profile.  
You can find this button at the top right of the table containing log harvesting profiles.
  3. Click **Requests**.
  4. On the Harvest Archives page, click **Filter: Enable**.
  5. Enter or select the filter criteria.

You can filter the log harvesting requests by the:

- Request ID of the log harvesting request. For example, to view the requests starting with Request ID 5, enter 5.
- zip file name that stores the harvested files.
- description of the log harvesting request.
- location of the archived file that stores the harvested files.
- status of the log harvesting request.
- description of the log harvesting request status.

6. Click **Filter: Apply**.

 **Note:**

If no records matching the filter criteria are found, the Log Harvesting page displays a message that no records matching the search criteria are found.

---

### Result

The table containing log harvesting requests displays only those log harvesting requests that matches the specified filter criteria.

## Viewing details of a log harvesting profile

1. On the System Manager console, click **Events > Logs > Log Harvester** in the left navigation pane.
2. On the **Log Harvesting** page, select a profile and click **View**.  
The Profile Criteria View page contains the details of the selected log harvesting profile.

**Related topics:**

[Profile Criteria View field descriptions](#) on page 1124

## Log Harvester field descriptions

This page displays the list of log harvest profiles created in System Manager. You can use buttons on this page to perform the following operations:

- View and edit the details of a selected log harvest profile
- Delete a profile
- Add a new log harvest profile
- View the details of log harvest requests for a profile

| Name                      | Description                                     |
|---------------------------|---|
| <b>Profile Name</b>       | The name of the log harvesting profile.         |
| <b>Description</b>        | A brief description of the profile.             |
| <b>Created By</b>         | The name of the creator of the profile.         |
| <b>Created Time Stamp</b> | The date and time when the profile was created. |

| Button      | Description   |
|-------------|---|
| <b>View</b> | Opens the Harvest Archives page. You can use this page to view the details of a selected log harvest profile. |
| <b>New</b>  | Opens the Create New Profile page. You can use this page to create a new log harvesting profile.              |
| <b>Edit</b> | Opens the Edit Profile page. You can use this page to edit a log harvesting profile.                          |

| Button                 | Description  |
|------------------------|--|
| <b>Delete</b>          | Deletes the selected profile. You can not delete a profile if the profile is in use by the Log Harvester service.  |
| <b>Requests</b>        | Opens the Harvest Archives page. You can use this page to run the log harvesting requests in a selected profile.   |
| <b>Filter: Disable</b> | Hides the fields displayed under the columns on which you can apply the filters without resetting the filter criteria. This is a toggle button.  |
| <b>Filter: Enable</b>  | Displays fields under the columns in the table where you can enter the filter criteria. Only columns on which you can apply filter display the fields in which you can enter the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>   | Filters the log harvest profiles present in the system based on the filter criteria.   |

---

## Create New Profile field descriptions

Use this page to create a new log harvesting profile for harvesting log messages from the log files for one or more products which may reside on one or more computers.

| Name                             | Description   |
|----------------------------------|---|
| <b>Profile Name</b>              | The name of the log harvesting profile  |
| <b>Profile Description</b>       | A brief description of the profile. This is an optional field.  |
| <b>IP</b>                        | The IP addresses of the computers on which products are installed   |
| <b>Product</b>                   | The products for which you can harvest logs   |
| <b>Directories / Filter Text</b> | Lists the directories that contains the log files for the selected product  |
| <b>Files</b>                     | The log files that you can harvest for the selected product   |
| <b>Filter Text</b>               | The text based on which the log files in the <b>Files</b> list box field are filtered. For example, if you enter a text, com in this field, the harvest operation for this profile harvests only the log files that start with the letters com. |

| Button              | Description   |
|---------------------|---|
| <b>+</b>            | Use this button to specify another log harvesting request for a product.        |
| <b>-</b>            | Deletes the log harvesting request for the product.                             |
| <b>Commit</b>       | Commits the filter criteria for the selected directories.                       |
| <b>Save Profile</b> | Saves the new profile and settings for log harvesting requests in the database. |

## Profile Criteria View field descriptions

Use this page to view the details of a selected log harvest profile.

| Name                       | Description   |
|----------------------------|---|
| <b>Profile Name</b>        | The name of the log harvesting profile  |
| <b>Profile Description</b> | A brief description of the profile  |
| <b>Product</b>             | The name of the product for which logs are harvested.   |
| <b>Hosts</b>               | The IP address of the computer on which the product resides.  |
| <b>Files</b>               | The names of the log files for which you can harvest log messages.  |
| <b>Directory</b>           | The directory that contains the log files.  |
| <b>Filter Text</b>         | The text based on which the log files are filtered for a selected directory. For example, if you enter text, com in this field, the harvest operation for this profile harvests only the log files that start with the letters com. |

| Button         | Description   |
|----------------|---|
| <b>Done</b>    | Closes this page and takes you back to the Harvest Profile List page. |
| <b>Refresh</b> | Refreshes the records in the table.                                   |

## Harvest Archives field descriptions

Use this page to create a archive for the log harvesting request. The archive created for a successful harvesting request contains the requested log files in a zip file. You can use the buttons on this page to perform the following operations:

- Run the log harvesting requests in a selected profile.
- View the details of the execution of a log harvesting request
- View the log files stored in an archived file.

| Name                       | Description   |
|----------------------------|---|
| <b>Archive Name</b>        | The name of the archive file that you want to create for storing the harvested log files. |
| <b>Archive Description</b> | A brief description of the archive. This is an optional field.                            |

| Name                       | Description   |
|----------------------------|---|
| <b>Request Id</b>          | The unique identification number assigned to a log harvesting request.  |
| <b>Zip file name</b>       | The name of the zip file that contains the harvested log files.   |
| <b>Request Time Stamp</b>  | The date and time when the log harvesting request is submitted.   |
| <b>Request Description</b> | A brief description of the log harvesting request   |
| <b>Status</b>              | The status of the log harvesting request. The options are: <ul style="list-style-type: none"> <li>• <b>SUCCESS:</b> The status is SUCCESS if System Manager successfully harvests the log messages.</li> <li>• <b>FAILURE:</b> The status is FAILURE if System Manager failed to harvest the log messages for the product.</li> </ul> |
| <b>Status Time Stamp</b>   | The date and time when the execution status of the log harvesting request is generated.   |
| <b>Status Description</b>  | A brief description of the log harvesting request status. The description provides you the information about the success or failure of the log harvesting request.  |
| <b>Location</b>            | The location where the harvested log messages are archived.   |

| Button                 | Description  |
|------------------------|--|
| <b>Run Profile</b>     | Runs the log harvesting requests for the selected profile.   |
| <b>View</b>            | Opens the View Harvest detail page. You can use this page to view the details of a selected log harvesting request.  |
| <b>Show Files</b>      | Opens the Search Archives page. You can use this page to search for a text contained in the harvested log files, download log files of one ore more products running on a same or different computers, view the contents of a log file.                                    |
| <b>Filter: Disable</b> | Hides the fields displayed under the column filter fields without resetting the filter criteria. This is a toggle button.  |
| <b>Filter: Enable</b>  | Displays fields under the column headers of the table displaying the log harvesting requests. You can enter the filter criteria in these fields. Only columns that can be filtered display the fields in which you can enter the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>   | Filters the log harvest profiles present in the system based on the filter criteria.   |

## Search Archives field descriptions

Use this page to perform the following activities on the log files contained in an archive:

- View the contents of harvested log files.
- Search a text in the harvested log files.
- Download the harvested log files on your local computer.

| Name                        | Description  |
|-----------------------------|--|
| <b>Enter search text</b>    | The text that you want search for in the harvested log files.  |
| <b>List box</b>             | Displays the hierarchy of the harvested log files in an archive. The files are organized in a tree view.   |
| <b>Log Browser Panel</b>    | Displays the contents of the selected log files  |
| <b>Search Results Panel</b> | Displays the search results. This field displays the line numbers as hyperlinks in which the searched text is found. When you click the line number, the system displays the line containing the searched text at the top in the <b>Log Browser Panel</b> field. |

| Button          | Description   |
|-----------------|---|
| <b>Previous</b> | Displays the log file contents on the previous page. This button is available only if the contents of a log files span across multiple pages. |
| <b>Next</b>     | Displays the log file contents on the next page. This button is available only if the contents of a log files span across multiple pages.     |
| <b>Search</b>   | Searches for the occurrences of the text specified in the <b>Enter search text</b> field in the selected log files.                           |
| <b>View</b>     | Displays the contents of the selected log files in the <b>Log Browser Panel</b> field.  |
| <b>Download</b> | Downloads the selected log files present in the archive on your local computer.   |

## Harvest - View Harvest detail field descriptions

Use this page to view the details of a selected log harvest request.

### View Parent

| Name              | Description  |
|-------------------|--|
| <b>Request ID</b> | The unique identification number assigned to a log harvesting request. |

| Name                       | Description   |
|----------------------------|---|
| <b>Archive</b>             | The name of the archive file that stores the harvested log files containing the log messages.   |
| <b>Status</b>              | The status of log harvesting requests. The options are: <ul style="list-style-type: none"> <li>• <b>SUCCESS</b>: The status is SUCCESS if System Manager successfully harvests the log messages.</li> <li>• <b>FAILURE</b>: The status is FAILURE if System Manager fails to harvest the log messages for the product.</li> </ul> |
| <b>Request Description</b> | A brief description of the log harvesting request.  |

### Harvest View

| Name                      | Description   |
|---------------------------|---|
| <b>Product</b>            | The unique identification number assigned to a log harvesting request.  |
| <b>Status</b>             | The status of the og harvesting request. The options are: <ul style="list-style-type: none"> <li>• <b>SUCCESS</b>: The status is SUCCESS if System Manager successfully harvests the log messages.</li> <li>• <b>FAILURE</b>: The status is FAILURE if System Manager fails to harvest the log messages for the product.</li> </ul> |
| <b>Host Name</b>          | The IP Address of the computer on which the product resides.  |
| <b>Status Description</b> | A brief description about the execution status of the request.  |
| <b>Status Time Stamp</b>  | The date and time when the execution status of the log harvesting request is generated.   |

| Button                 | Description  |
|------------------------|--|
| <b>Done</b>            | Closes this page and takes you back to the Harvest Archives page.  |
| <b>Refresh</b>         | Refreshes the records in the table.  |
| <b>Filter: Enable</b>  | Displays fields under the column headers of the table displaying the log harvesting requests. You can enter the filter criteria in these fields. Only columns that can be filtered display the fields in which you can enter the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>   | Filters the log harvesting requests based on the filter criteria.  |
| <b>Filter: Disable</b> | Hides the fields displayed under the columns on which you can apply the filters without resetting the filter criteria. This is a toggle button.  |



# Chapter 8: Managing Licenses

---

## WebLM overview

Use WebLM to manage licenses of one or more Avaya software products for your organization. WebLM is Web-based and facilitates easy tracking of licenses. To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS).

WebLM supports two configurations models:

1. WebLM standard model: In the WebLM standard model, a single WebLM server is used to support one or more licensed products. The WebLM standard model is supported for Standard license file (SLF) and Enterprise license file (ELF) types.
2. WebLM enterprise model: In a WebLM enterprise model, there are multiple WebLM servers. One WebLM server acts as a 'master WebLM' and hosts the license file from PLDS. The other WebLM servers act as the 'local WebLMs' and host allocation license files from the master WebLM server. You need an ELF to setup the WebLM enterprise model. PLDS generates license files that are either SLFs or ELFs.

For example, you can purchase two products and choose the enterprise model of licensing for one product and the standard model of licensing for the other product. PLDS generates a separate license file for each product. The license file is either an SLF or ELF based on how the product is configured in PLDS. Ensure that you verify the installation options supported by the product before installing the WebLM server. If you want to configure standard licensing, you can use either an ELF or SLF. In order to configure enterprise licensing you must have an ELF. After you install the license file on the WebLM server, any product with an ELF can have multiple instances of the WebLM server, and any product with an SLF can have only one instance of the WebLM server. For more information on the WebLM configuration models, see WebLM configuration models section in the guide.

A license file is an Extensible Markup Language (XML) file. The license file contains information regarding the product, major release, and license features and capacities. After the purchase of a licensed Avaya software product, a license file for the product must be activated in PLDS and installed on WebLM server. For information on generating license file through PLDS, see Getting Started with Avaya PLDS at <https://plds.avaya.com>.

License activations in PLDS require the host ID of the WebLM server for inclusion in the license file. The host ID of the WebLM server can be obtained from viewing the Server Properties page of the WebLM server Web page.

You have the following options for the WebLM server that will host the product license file:

- Use Existing WebLM server: If you already have a WebLM server that you are using for licensing other Avaya products. Refer to the product specific documentation or contact Avaya support, to ensure compatibility of the licensed product with the existing WebLM server version.
- Install WebLM server on a separate server from the product: If you choose to install the WebLM on a separate server, follow the instructions provided in Installing WebLM on a separate server from the product section in the guide. Refer to the product specific documentation or contact Avaya support, to ensure compatibility of the licensed product with the existing WebLM server version.
- Install WebLM server co-resident with the product: Some WebLM licensed products include WebLM server software with the product installation software. In this case, the WebLM server installation is a part of the product installation and the WebLM server version will be compatible with the product.
- Install Avaya System Manager on a separate server from the product: Avaya System Manager includes WebLM server software. If you choose to install System Manager, WebLM is also installed with it. Refer to the product specific documentation or contact Avaya support, to ensure compatibility of the licensed product with the existing WebLM server version.



**Note:**

In order to acquire licenses from WebLM server, the product software must be configured with the URL of the WebLM server.

For information on how to configure the WebLM URL with the product, see the Installation guide of the purchased Avaya software product.

---

## Obtaining the license file

Obtain a license file from PLDS to install on the WebLM Server for each licensed Avaya product that you plan to manage from the WebLM server. For additional information on using PLDS, see *Getting Started with Avaya PLDS - Avaya Partners and Customers* at <https://plds.avaya.com>.



**Caution:**

Do not change your license file after you receive it from Avaya. WebLM does not accept a modified license file.

You need the host ID of the WebLM Server in order to activate the license file in PLDS.

- 
1. Type the following path on your browser: <http://<WebLM server IP>:8080/WebLM>
  2. Login to the WebLM Server using your login credentials.

3. In the home page of the WebLM Server, on the left pane, click the **Server Properties** link.
  4. Note the **Primary Host ID**.  
While the use of the primary host ID is recommended, any of the host IDs listed on the server properties page will work in the license file.
- 

---

## Accessing WebLM

### Prerequisites

You must have permissions to access the WebLM application.

---

1. Log in to the Avaya Aura System Manager web interface.
  2. On the System Manager console, click **Licenses**.
- 

---

## Installing a license file

Use this functionality to install a license file on the WebLM server. If you are re installing a license file on a WebLM server on which RFA generated license file is installed, you need to remove the RFA generated license file from the WebLM server before installing the new license file. Use the Uninstall functionality to remove the license from the WebLM server.

### Prerequisites

You must have a license file obtained from the Avaya PLDS Web site.

---

1. Click **Install License** in the left navigation pane.
  2. On the Install License page, enter the license file path. You can also click **Browse** to select the license file.
  3. Click **Install** to install the license file.
- 

### Result

WebLM displays a message on the successful installation of the license file.

License installation may fail for various reasons. Following are some of the reasons of unsuccessful installation of the license file:

- WebLM finds an invalid digital signature on the license file. If you come across such an error then you need to request for re-delivering of the license file from PLDS.
- Another example is current capacity use exceeds capacity in license being installed.

**Related topics:**

[Obtain license file](#)

[Install License field descriptions](#) on page 1134

---

## Viewing license capacity of features for a product

Use this functionality to view the license capacity of features for a product for which you have installed a standard license file.

### Prerequisites

You must have installed the standard license file on the WebLM server for the licensed product.

---

Click the product name under the **Licensed Products** in the left navigation pane. The content pane displays the capacity of licensed features for the product.

---

**Related topics:**

[View License Capacity field descriptions](#) on page 1134

---

## Viewing peak usage for a licensed product

### Prerequisites

You must have installed the standard license file on the WebLM server for the licensed product.

- 
1. Click the product name under the **Licensed Products** in the left navigation pane.
  2. On the content pane, click **View Peak Usage**.
-

**Related topics:**

[View Peak Usage field descriptions](#) on page 1135

---

## Removing a license file

Use this functionality, to remove the license file, installed on the WebLM server.

**Prerequisites**

- 
1. On the WebLM Home page, click **Uninstall License** in the left navigation pane.
  2. On the Uninstall License page, select the license file that you want to delete.
  3. Click **Uninstall** to remove the license file from the WebLM server.
- 

**Related topics:**

[Uninstall License field descriptions](#) on page 1136

---

## Viewing server properties

---

On the WebLM Home page, click **Server Properties** in the left navigation pane.  
Host ID is the MAC address of the computer on which WebLM is installed.

**Note:**

The host ID specified in the PLDS is embedded in the license file. The license file can be installed only if the host ID of the target computer matches the host ID in the license file. Therefore, while requesting a license file, you must specify the correct host ID of the computer where the WebLM server is installed.

---

**Related topics:**

[Server Properties field descriptions](#) on page 1136

## WebLM Home field descriptions

Use this page to view the information about the product(s) and the associated license file(s) installed on the WebLM server.

| Field                       | Description   |
|-----------------------------|---|
| <b>Product Name</b>         | The name of the product for which the license file is installed.    |
| <b>Product Version</b>      | The version of the product for which the license file is installed. |
| <b>Type of License</b>      | The type of license file installed for the product.                 |
| <b>Date of Installation</b> | Date and time of installation of license file.                      |

## Install License field descriptions

Use this page to install the license file of a product on the WebLM server.

| Field/Button              | Description  |
|---------------------------|--|
| <b>Enter License Path</b> | The path where you have saved the license file.                  |
| <b>Browse</b>             | Opens the dialog box that allows you to select the license file. |
| <b>Install</b>            | Installs the product license file.                               |

**Related topics:**

[Installing a license file](#) on page 1131

## View License Capacity field descriptions

Use this page to view the total number of feature licenses of a feature that the organization has purchased and the current allocation of these purchased licenses.

| Field                    | Description   |
|--------------------------|---|
| <b>Feature (Keyword)</b> | The display name of the licensed features of the product and the keywords of each feature. These keywords are used to represent the licensed feature in the license file. |

| Field                  | Description  |
|------------------------|--|
| <b>Expiration Date</b> | The date when the license for the feature would expire.  |
| <b>Licensed</b>        | The number of feature licenses purchased by the organization for each licensed feature. The system gathers the number of feature licenses information from the license file. |
| <b>Acquired</b>        | The Number of feature licenses that are currently in use by the licensed application. The features that are of type Uncounted, the column displays <i>Not counted</i> .      |

The Acquired Licenses table displays information about the licenses acquired by the licensed application. You can view this table only if the licensed product has acquired feature licenses.

| Field              | Description   |
|--------------------|---|
| <b>Feature</b>     | The feature keyword for each licensed feature that is currently acquired by a licensed application. |
| <b>Acquired by</b> | The name of the licensed application that has acquired the license.                                 |
| <b>Count</b>       | The number of feature licenses that are currently acquired by the licensed application.             |

**Related topics:**

[Viewing license capacity of features for a product](#) on page 1132

---

## View Peak Usage field descriptions

Use this page to view the usage information of feature licenses of a licensed application for different time intervals.

| Field                                  | Description  |
|--|--|
| <b>Feature (License Keyword)</b>       | The display name of the licensed features of the product and the keywords of each feature. These keywords are used to represent the licensed feature in the license file.  |
| <b>Currently Allocated</b>             | The number of feature licenses purchased by the organization.  |
| <b>Usage: qty/%</b>                    | The number of feature licenses for each licensed feature that a licensed application is currently using. The column also displays the percentage of usage. For example, if 50 is the available feature licenses and 5 feature licenses have been used by the applications, this column will display 5/10%. |
| <b>Peak Usage (last 7 days): qty/%</b> | The highest number of feature licenses for each licensed feature that has been used in the last seven days. For example, if the peak usage   |

| Field                                   | Description  |
|---|--|
|   | for a feature license in the past seven days is 25 and the number of available licenses during these seven days was 50, then the column displays 25/50%.   |
| <b>Peak Usage (last 30 days): qty/%</b> | The highest number of feature licenses for each licensed feature that has been used in the past 30 days. For example, if the peak usage for a feature license in the past 30 days is 50 and the number of available licenses during these 30 days was 50, then the column displays 50/100% |
| <b>Time of Query</b>                    | The date and time when the last usage query for WebLM was executed   |
| <b>Status</b>                           | The success or failure of the last usage query executed for WebLM server.  |

**Related topics:**

[Viewing peak usage for a licensed product](#) on page 1132

## Uninstall License field descriptions

Use this page to uninstall a license file from the WebLM server for a licensed product.

| Field/Button                  | Description   |
|-------------------------------|---|
| <b>Installed License File</b> | The name of the license files that are currently installed on the WebLM server.       |
| <b>Product(s)</b>             | The products for which licenses are installed on the WebLM server.                    |
| <b>SID</b>                    | The System ID of the license file.  |
| <b>Select Checkbox</b>        | Allows you to select the license files that you want to remove from the WebLM server. |
| <b>Uninstall</b>              | Removes the selected license files from the WebLM server.                             |

**Related topics:**

[Removing a license file](#) on page 1133

## Server Properties field descriptions

Use this page to view the MAC Address of the server. The Server Host ID section displays the MAC Address of the server. The server can have more than one MAC Address assigned to it. The first MAC Address is the primary MAC Address and subsequent MAC Addresses are

designated as secondary and so on. The primary MAC Address is recommended for use in the license file.

 **Note:**

In case of a Solaris server where the MAC Address is not available (e.g. in a zoned environment), WebLM retrieves the hostid (8 – digit hexadecimal address) of the server and adds leading zeros before using the resulting 12 – digit ID.

**Related topics:**

[Viewing server properties](#) on page 1133

---

## Enterprise licensing

---

### Configuring enterprise licensing

#### Prerequisites

You must have installed the enterprise license file on the master WebLM server for the product. To verify the type of license file for a product, click the product name in the left navigation pane. The content pane displays the license file type installed for the product at the top of the page along with the product name and the SID value.

- 
1. Click the product name under the **Licensed Products** in the left navigation pane.
  2. Click **Enterprise Configuration** in the left navigation pane.
  3. On the Enterprise Configuration page enter appropriate information in the fields.  
To view the detailed descriptions of the fields, click the Enterprise Configuration field descriptions link in the Related topics section at the end of this topic .  
The fields marked with red asterisk are mandatory fields. You must enter valid information in these fields to successfully set up and configure the master WebLM server.
  4. In the Master WebLM Configuration section, enter the name, description, and IP Address of the master WebLM server .
  5. In the Default Periodic Operation Settings section, enter the retry count and the retry interval in minutes for the periodic operations .
  6. In the SMTP Server Settings section, enter the SMTP server name.
  7. In the Email Notification Settings for the Periodic Operation section, set the e-mail notification and enter the e-mail address.

Click **Add To List** after you enter an e-mail address in the **Email Address** field, to add the e-mail address in the list of recipients to whom WebLM server will send e-mail notifications.

8. In the Default Periodic License Allocation Schedule section, select the day and time for periodic license allocations.

This is the default setting for periodic allocation for all local WebLM servers in the enterprise.

9. In the Default Periodic Usage Query Schedule section, select the day and time of query for periodic usage.

This is the default setting for periodic allocation for all local WebLM servers in the enterprise.

10. Click **Submit**.

The system validates the information. If the information is valid, the system displays the host ID of the computer where the server is installed in the **MAC ID** field.

---

**Related topics:**

[Enterprise Configuration field descriptions](#) on page 1146

---

## Adding a local WebLM server

1. Click the product name under the **Licensed Products** in the left navigation pane.
2. Click **Local WebLM Configuration > Add Local WebLM** in the left navigation pane.
3. On the Local WebLM Configuration: Add Local WebLM page, enter the appropriate information.

To view the detailed descriptions of the fields, click the Add Local WebLM field descriptions link in the Related topics section at the end of this topic .

The fields marked with red asterisk are mandatory fields. You must enter valid information in these fields to successfully set up and configure the local WebLM server.

4. In the Local WebLM Configuration section, enter the name, description, IP Address, port of the local WebLM server and select a protocol for local WebLM server to communication with other WebLM servers.
5. In the Periodic License Allocation Schedule section, select the day and time for periodic license allocations.

6. In the Periodic Usage Query Schedule section, select the day and time of query for periodic usage .
7. Click **Configure and Validate**.  
The system validates the information. If the information is valid, the system displays the host ID of the computer where the server is installed in the **MAC ID** field.

---

**Related topics:**

[Add Local WebLM field descriptions](#) on page 1148

---

## Modifying a local WebLM server configuration

1. Click the product name under the **Licensed Products** in the left navigation pane.
2. Click **Local WebLM Configuration > Modify Local WebLM** in the left navigation pane.
3. On the Local WebLM Configuration: Modify Local WebLM page, select the local WebLM that you want to configure.
4. Click **Modify**.
5. Modify the information.

 **Note:**

You can modify information in the following fields: Name, Description, Protocol, Port, Day and Time of Periodic License Allocation Schedule, Day and Time of Periodic Usage Query Schedule.

6. Click **Modify** to save the changes.

---

**Related topics:**

[Modify Local WebLM field descriptions](#) on page 1150

---

## Removing a local WebLM server

1. On the WebLM Home page, click the product name under the **Licensed Products** in the left navigation pane.
2. Click **Local WebLM Configuration > Delete Local WebLM** in the left navigation pane.

3. On the Local WebLM Configuration: Delete Local WebLM page, select the local WebLM server that you want to delete.
4. Click **Delete**.



**Note:**

The system displays a warning message before removing the local WebLM server from the master WebLM server.

5. Click **Ok**.

---

**Related topics:**

[Delete Local WebLM field descriptions](#) on page 1151

---

## Viewing the license capacity of licensed features for a product

- 
1. Click the product name under the **Licensed Products** in the left navigation pane.
  2. Click **View by Feature** in the left navigation pane.

---

**Related topics:**

[View by Feature field descriptions](#) on page 1145

---

## Viewing the connectivity status of local WebLM servers

- 
1. Click the product name under the **Licensed Products** in the left navigation pane.
  2. Click **View by Local WebLM** in the left navigation pane.

---

**Related topics:**

[View by Local WebLM field descriptions](#) on page 1145

---

## Validating connectivity to local WebLM servers for a product

- 
1. Click the enterprise product name under the **Licensed Products** in the left navigation pane.
  2. Click **Local WebLM Configuration** in the left navigation pane.
  3. On the Local WebLM Configuration: View Local WebLMs page, select the local WebLM servers that you want to validate for connectivity.
  4. click **Validate Connectivity** to query the selected local WebLM servers.

---

### Result

The **status** column on the Local WebLM Configuration: View Local WebLMs page of the selected WebLM servers displays whether the connection request made to the local WebLM server is successful or not.

### Related topics:

[View Local WebLMs field descriptions](#) on page 1148

---

## Viewing usage by WebLM

- 
1. Click the product name under the **Licensed Products** in the left navigation pane.
  2. Click **Usages > Usage by WebLM** in the left navigation pane.
  3. On the Usages: Usage by WebLM page, select the master or local WebLM server from the **Select WebLM** field.
  4. Click **Query System**.

---

### Related topics:

[Usage by WebLM field descriptions](#) on page 1152

---

## Viewing allocations by features

1. On the WebLM Home page, click the product name under the **Licensed Products** in the left navigation pane.
2. Click **Allocations > View by Feature** in the left navigation pane.

---

### Related topics:

[Allocations by Features field descriptions](#) on page 1155

---

## Viewing enterprise usage of a license feature

1. Click the product name under the **Licensed Products** in the left navigation pane.
2. Click **Usages > Enterprise Usage** in the left navigation pane.
3. On the Usages: Enterprise Usage page, select the licensed feature from the **Select Feature (License Keyword)** field.  
The page displays the usage of the licensed feature for the master WebLM server and the local WebLM servers.

---

### Related topics:

[Enterprise Usage field descriptions](#) on page 1153

---

## Changing allocations of licensed features for a local WebLM server

Use this functionality to change the license allocations of a feature residing on a product's local WebLM sever.

1. Log in to the master WebLM server.
2. Click the product name under the **Licensed Products** in the left navigation pane.
3. Click **Allocations > Change Allocations** in the left navigation pane.

4. In the **New Allocation** column on the Allocations: Change Allocations page, enter the number of licenses that you want to allocate for the feature residing on a local WebLM server.
5. Click **Submit Allocations**.

---

**Related topics:**

[Change Allocations field descriptions](#) on page 1157

---

## Viewing periodic status of master and local WebLM servers

- 
1. Click the product name under the **Licensed Products** in the left navigation pane.
  2. Click **Periodic Status** in the left navigation pane.

---

**Related topics:**

[Periodic Status field descriptions](#) on page 1158

---

## Specifying overuse limit for licensed features

- 
- 1.
  2. On the WebLM Home page, click the product name under the **Licensed Products** in the left navigation pane.
  3. Click **Overuse** in the left navigation pane.
  4. In the **update percent overuse value** field on the Overuse page, select the percent overuse value.
  5. Click **Submit** to set the overuse limit.

---

**Related topics:**

[Overuse field descriptions](#) on page 1159

---

## Querying usage of feature licenses for master and local WebLM servers

- 
1. Click the product name under the **Licensed Products** in the left navigation pane.
  2. Click **Usages > Query Usage** in the left navigation pane.
  3. On the Usages: Query Usage page, select the master or local WebLM server for which you want to view the usage details by feature licenses.
  4. Click **Query Usage**.  
If you select all the WebLM servers and click **Query usage**, then the page displays whether the query request succeeded.

---

### Result

The Usages: Usage by WebLM page displays the details of the selected WebLM servers.

### Related topics:

[Query Usage field descriptions](#) on page 1154

---

## Viewing allocations by local WebLM

- 
1. On the WebLM Home page, click the product name under the **Licensed Products** in the left navigation pane.
  2. Click **Allocations > View by Local WebLM** in the left navigation pane.
  3. From the **Select Local WebLM** field on the Allocations: View by Local WebLM, select the local WebLM.

---

### Result

The page displays the allocations details for the selected local WebLM server on the same page.

### Related topics:

[Allocations by Local WebLM field descriptions](#) on page 1156

---

## Viewing usage summary

1. Click the product name under the **Licensed Products** in the left navigation pane.
2. Click **Usages** in the left navigation pane.

---

### Related topics:

[Usage Summary field descriptions](#) on page 1152

---

## View by Feature field descriptions

Use this page to view the license capacity for each feature license of a product.

| Name                             | Description  |
|----------------------------------|--|
| <b>Feature (License Keyword)</b> | The display name and keyword for the licensed features of the product.   |
| <b>License Capacity</b>          | The total number of feature licenses purchased by the organization for each feature.   |
| <b>Currently Available</b>       | <p>The number of floating licenses of each feature that is currently available with the master WebLM server.</p> <p> <b>Note:</b><br/>In the case of uncounted features, this column displays “Not counted”</p> |

### Related topics:

[Viewing the license capacity of licensed features for a product](#) on page 1140

---

## View by Local WebLM field descriptions

Use this page to view information related to local WebLM servers of a product.

| Name                    | Description  |
|-------------------------|--|
| <b>Local WebLM Name</b> | The name of the local WebLM server.                          |
| <b>IP Address</b>       | IP Address of the local WebLM server.                        |
| <b>Last Contacted</b>   | Date and time when the local WebLM server is last contacted. |

| Name   | Description   |
|--------|---|
| Status | Lists the success or failure of the last connection request to each local WebLM server. |

**Related topics:**

[Viewing the connectivity status of local WebLM servers](#) on page 1140

## Enterprise Configuration field descriptions

Use this page to specify the master WebLM server settings and the default settings for the periodic operations of the server. The settings you specify in the Enterprise Configuration Web page are applicable to the entire enterprise. When a local WebLM server is not available, the licensed applications use the master WebLM server settings to acquire the licenses. The master WebLM server uses the settings of the periodic operations to perform the following operations to:

- Re-send the allocation license file (ALF) to the local WebLM server.
- Query the local WebLM servers and generate the usage report.
- Query itself and generate the usage report for licenses.

### Master WebLM Configuration

| Name        | Description  |
|-------------|--|
| Name        | Name of the server.                                    |
| Description | A brief description of the server.                     |
| IP Address  | IP address of the server.                              |
| MAC ID      | Host ID of the computer where the server is installed. |

### Default Periodic Operation Settings

| Name           | Description  |
|----------------|--|
| Retry Count    | This count is the number of times a master WebLM server should try to connect to a local WebLM server for a periodic operation after a connection failure. For example, let us consider that the count is set to 2 and the master WebLM server's attempt to connect to a local WebLM server is not successful. The master WebLM server will make two more attempts to connect to the local WebLM server. |
| Retry Interval | This interval is the duration, in minutes, within which the retry count specified in the Retry Count field must be carried out. For example, let us consider that the Retry Count is 2 and the Retry Interval is 10 minutes. On failure of a connection attempt, the master WebLM server will make two attempts within 10 minutes to connect to the local WebLM server.                                  |

## SMTP Server Settings

| Name        | Description              |
|-------------|--------------------------|
| Server Name | Name of the SMTP server. |

## Email Notification Settings for Periodic Operation

| Name               | Description   |
|--------------------|---|
| Email notification | <p>Following are the options:</p> <ul style="list-style-type: none"> <li>• On: Sends an e-mail notification to the administrator if the periodic operations fail.</li> <li>• Off: No e-mail notification is sent to the administrator if the periodic operation fail.</li> </ul>  |
| Email Address      | <p>The e-mail address to which the WebLM application sends the e-mail notification if the periodic operations failed to execute.</p> <p> <b>Note:</b><br/>You must click <b>Add To List</b> to add the e-mail address in the list of recipients who will receive the e-mail notification of the periodic operation status.</p> |
| Email Addresses    | The list of e-mail addresses to which the WebLM application sends the e-mail notifications.   |
| Add To List        | Adds the e-mail address entered in the <b>Email Address</b> field to the <b>Email Addresses</b> .   |
| Remove Selected    | Removes the selected e-mail address from the <b>Email Addresses</b> field.  |

## Default Periodic License Allocation Schedule

| Name | Description  |
|------|--|
| Day  | The day of the week on which the master WebLM server must send the ALF's (Allocation license file) again to local WebLM server . |
| Time | The time of the day specified in the <b>Day</b> field when master WebLM must send the ALF's again to local WebLM server.         |

## Default Periodic Usage Query Schedule

| Name | Description  |
|------|--|
| Day  | The day of the week on which master WebLM must query local WebLM servers for usage reports.  |
| Time | The time of the day specified in the <b>Day</b> field when the master WebLM server must query local WebLM servers for usage reports. |

| Button        | Description  |
|---------------|--|
| <b>Submit</b> | Saves the enterprise configuration.                    |
| <b>Reset</b>  | Resets the values in the fields to the default values. |

**Related topics:**

[Configuring enterprise licensing](#) on page 1137

## View Local WebLMs field descriptions

Use this page to validate the local WebLM server connection. To validate the connection, the master WebLM server tries to connect to the specified local WebLM server.

 **Note:**

To validate the connectivity of a local WebLM server, the local WebLM server must be already added for the product.

| Name                    | Description   |
|-------------------------|---|
| <b>Local WebLM Name</b> | The name of the local WebLM server.   |
| <b>IP Address</b>       | IP address of the local WebLM server.   |
| <b>Last Contacted</b>   | Date and time when the local WebLM server was last contacted.                           |
| <b>Status</b>           | Lists the success or failure of the last connection request to each local WebLM server. |

| Button                       | Description  |
|------------------------------|--|
| <b>Validate Connectivity</b> | Validates the connectivity of the selected WebLM server. |
| <b>Check All</b>             | Selects all the local WebLM server.                      |
| <b>Clear All</b>             | Clears the selections of local WebLM servers.            |

**Related topics:**

[Validating connectivity to local WebLM servers for a product](#) on page 1141

## Add Local WebLM field descriptions

Use this page to add a local WebLM server.

## Local WebLM Configuration

| Name               | Description   |
|--------------------|---|
| <b>Name</b>        | Name of the server.   |
| <b>Description</b> | A brief description of the server.  |
| <b>IP Address</b>  | A unique IP address of the server. If you enter an IP address of a server that was already configured for a local WebLM server, the system displays the following error message:<br><code>IP Address is being duplicated</code> |
| <b>Protocol</b>    | Protocol scheme over which the master WebLM server listens to the local WebLM server.   |
| <b>Port</b>        | Port number on which the master WebLM server listens to the local WebLM server in the specified protocol scheme.  |
| <b>MAC ID</b>      | Host ID of the computer where the server is installed.  |

## Periodic License Allocation Schedule

| Name        | Description   |
|-------------|---|
| <b>Day</b>  | The day of the week on which the master WebLM server must send the ALF's again to local WebLM server. By default, the settings specified in the Enterprise Configuration are automatically displayed in this section. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is applicable only for this local WebLM server.                                   |
| <b>Time</b> | The time of the day specified in the <b>Day</b> field when the master WebLM server must send the ALF's again to the local WebLM server. By default, the settings specified in the Enterprise Configuration are automatically displayed in this section. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is applicable only for this local WebLM server. |

## Periodic Usage Query Schedule

| Name        | Description  |
|-------------|--|
| <b>Day</b>  | The day of the week on which the master WebLM server must query local WebLM servers for usage reports. By default, the settings specified in the Enterprise Configuration are automatically displayed in this section. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is applicable only for this local WebLM server. |
| <b>Time</b> | The time of the day specified in the <b>Day</b> field when the master WebLM server must query local WebLM servers for usage reports. By default, the settings specified in the Enterprise Configuration are automatically displayed in this section. If you change the default settings, the new settings override the settings of the Enterprise  |

| Name | Description  |
|------|--|
|      | Configuration. However, the change in the schedule is applicable only for this local WebLM server. |

| Button                        | Description   |
|-------------------------------|---|
| <b>Configure and Validate</b> | Configures the local WebLM server and validates the creation of the local WebLM server. |
| <b>Back</b>                   | Navigates back to View Local WebLMs.  |

**Related topics:**

[Adding a local WebLM server](#) on page 1138

## Modify Local WebLM field descriptions

Use this page to modify the information of a selected local WebLM server.

### Local WebLM Configuration

| Name               | Description   |
|--------------------|---|
| <b>Name</b>        | Name of the server.   |
| <b>Description</b> | A brief description of the server.  |
| <b>IP Address</b>  | IP address of the server.<br><br> <b>Note:</b><br>You can not modify the information in this field.                              |
| <b>Protocol</b>    | Protocol scheme over which the master WebLM server listens to the local WebLM server.   |
| <b>Port</b>        | Port number on which the master WebLM server listens to the local WebLM server in the specified protocol scheme.  |
| <b>MAC ID</b>      | Host ID of the computer where the server is installed.<br><br> <b>Note:</b><br>You can not modify the information in this field. |

### Periodic License Allocation Schedule

| Name       | Description   |
|------------|---|
| <b>Day</b> | The day of the week on which the master WebLM server must send the ALF's again to local WebLM server. |

| Name        | Description   |
|-------------|---|
| <b>Time</b> | The time of the day specified in the <b>Day</b> field when the master WebLM server must send the ALF's again to the local WebLM server. |

### Periodic Usage Query Schedule

| Name        | Description  |
|-------------|--|
| <b>Day</b>  | The day of the week on which the master WebLM server must query the local WebLM servers for usage reports.                               |
| <b>Time</b> | The time of the day specified in the <b>Day</b> field when the master WebLM server must query the local WebLM servers for usage reports. |

| Button        | Description  |
|---------------|--|
| <b>Modify</b> | Saves the local WebLM server configuration changes.  |
| <b>Back</b>   | Discards the configuration changes and takes the user back to the Modify Local WebLM web page. |

#### Related topics:

[Modifying a local WebLM server configuration](#) on page 1139

---

## Delete Local WebLM field descriptions

Use this page to delete a local WebLM server.

| Name                    | Description   |
|-------------------------|---|
| <b>Local WebLM Name</b> | The name of the local WebLM server.                     |
| <b>IP Address</b>       | IP Address of the local WebLM server.                   |
| <b>Select check box</b> | Select the local WebLM servers that you want to delete. |

| Button        | Description                                      |
|---------------|--|
| <b>Delete</b> | Removes the selected local WebLM server.         |
| <b>Reset</b>  | Clears the selection of the local WebLM servers. |

#### Related topics:

[Removing a local WebLM server](#) on page 1139

## Usage Summary field descriptions

Use this page to view the usage summary for a master WebLM server, a local WebLM server, or all the WebLM servers of the product.

| Name                 | Description   |
|----------------------|---|
| <b>WebLM Name</b>    | This column displays the names of the master WebLM server and the local WebLM servers of the product.   |
| <b>IP Address</b>    | The IP address of the master WebLM server and the local WebLM servers of the product.   |
| <b>Time of Query</b> | The date and time when the last usage query was executed for the WebLM server. If the status of the last usage query was Failed, this column also displays the date and time of the usage query that was last successful.   |
| <b>Status</b>        | The success or failure of the last usage query executed for each WebLM server. This column of a WebLM server will be empty if the server has not been queried even once for feature license usage. The usage query can be a periodic usage query or a non periodic usage query. |

**Related topics:**

[Viewing usage summary](#) on page 1145

## Usage by WebLM field descriptions

Use this page to query the feature license usage by Master and Local WebLM servers.

| Name                             | Description  |
|----------------------------------|--|
| <b>Select WebLM</b>              | The master and local WebLM servers for which you can view the usage.   |
| <b>Feature (License Keyword)</b> | The name and keyword of the counted features of the product.   |
| <b>Currently Allocated</b>       | The number of feature licenses for each feature that are currently allocated to the selected WebLM server. For the master WebLM server of the product, this column lists the floating licenses available with the server.  |
| <b>Usage: qty/%</b>              | The number of feature licenses for each feature that are currently used by the licensed applications, from the allocated feature licenses. The column also displays the percentage of usage. For example, if 50 is the allocated feature licenses and 5 feature licenses have been used by the applications, this column will display 5/10%. |

| Name                                    | Description   |
|---|---|
| <b>Peak Usage (last 7 days): qty/%</b>  | The highest number of feature licenses for each feature that are used by the applications in the past seven days. The column also displays the percentage of peak usage. For example, if the peak usage in the past seven days is 25 and 50 feature licenses were available during the peak usage calculation, the column displays 25/50%.          |
| <b>Peak Usage (last 30 days): qty/%</b> | The highest number of feature licenses for each feature that are used by the applications in the past 30 days. The column also displays the percentage of peak usage. For example, if the peak usage in the past 30 days is 50 and the feature licenses those were available during the peak usage calculation was 50, the column displays 50/100%. |
| <b>Time of Query</b>                    | The date and time when the usage query for the selected WebLM server was executed.  |
| <b>Status</b>                           | The success or failure of the last usage query process executed for each WebLM server. This column will be empty if the server has not been queried even once for feature license usage. The usage query can be a periodic usage query or a non periodic usage query.   |

| Button              | Description  |
|---------------------|--|
| <b>Query System</b> | Queries the selected WebLM server for feature license usage. |

**Related topics:**

[Viewing usage by WebLM](#) on page 1141

---

## Enterprise Usage field descriptions

Use this page to view the feature license usage of all WebLM servers for the selected feature.

| Name                                    | Description   |
|---|---|
| <b>Select Feature (License Keyword)</b> | The license features for which you can view the license usage.  |
| <b>License Capacity</b>                 | The total number of feature licenses purchased by the organization for each feature.  |
| <b>Available</b>                        | The number of floating licenses available with the master WebLM server.   |
| <b>WebLM Name</b>                       | The names of the WebLM servers of the product.  |
| <b>Currently Allocated</b>              | The number of feature licenses that have been currently allocated to the WebLM servers for the selected feature.                          |
| <b>Usage qty/%</b>                      | The number of feature licenses that are currently used by the licensed applications, from the allocated feature licenses for the selected |

| Name                                    | Description  |
|---|--|
|   | feature. The column also displays the percentage of usage. For example, if 50 is the allocated feature licenses and 5 feature licenses have been used by the applications, this column will display 5/10%.   |
| <b>Peak Usage (last 7 days): qty/%</b>  | The highest number of feature licenses that are used by the applications in the past seven days for the selected feature. The column also displays the percentage of peak usage. For example, if the peak usage in the past seven days is 25 and the feature licenses those were available during the peak usage calculation was 50, the column displays 25/50%. |
| <b>Peak Usage (last 30 days): qty/%</b> | The highest number of feature licenses that are used by the applications in the past 30 days for the selected feature. The column also displays the percentage of peak usage. For example, if the peak usage in the past 30 days is 50 and the feature licenses those were available during the peak usage calculation was 50, the column displays 50/100%.      |
| <b>Time of Query</b>                    | The date and time when the usage query was executed for the selected feature.  |
| <b>Status</b>                           | The success or failure of the last usage query process executed for each WebLM server.   |

**Related topics:**

[Viewing enterprise usage of a license feature](#) on page 1142

---

## Query Usage field descriptions

Use this page to query the master WebLM server, a local WebLM server, or all the WebLM servers of the product for their feature license usage report.

| Name                 | Description  |
|----------------------|--|
| <b>WebLM Name</b>    | The names of the master and the local WebLM servers of the product as links. You can view the feature license usage of a server by selecting the name of the required server in this column.<br><br> <b>Note:</b><br>The table in the Usage by WebLM Web page will be empty if the specified WebLM server has not been queried even once for feature license usage. |
| <b>IP Address</b>    | The IP address of the master WebLM server and the local WebLM servers of the product.  |
| <b>Time of Query</b> | The date and time when the last usage query was executed for the WebLM server. If the status of the last usage query was Failed, this column also displays the date and time of the usage query that was last successful.  |

| Name                    | Description   |
|-------------------------|---|
|                         |  <b>Note:</b><br>The Time of Query column of a WebLM server will be empty if the server has not been queried even once for feature license usage.  |
| <b>Status</b>           | The success or failure of the last usage query executed for each WebLM server. This column of a WebLM server will be empty if the server has not been queried even once for feature license usage. The usage query can be a periodic usage query or a non periodic usage query. |
| <b>Select Check box</b> | Check the WebLM Server for which you want to determine the usage query.   |

| Button             | Description   |
|--------------------|---|
| <b>Check All</b>   | Selects all the WebLM servers.  |
| <b>Clear All</b>   | Clears the selections for all the WebLM servers.  |
| <b>Query Usage</b> | Queries the selected WebLM servers of the product for their feature license usage report. |

**Related topics:**

[Querying usage of feature licenses for master and local WebLM servers](#) on page 1144

---

## Allocations by Features field descriptions

Use this page to view the feature license allocation information for each counted type feature of the product.

| Name                             | Description   |
|----------------------------------|---|
| <b>Feature (License Keyword)</b> | The name and license keyword of the counted features of the product.  |
| <b>Local WebLM Name</b>          | The name of the local WebLM servers of the product. By default, this column is empty. The system displays the names of the local WebLM servers only when you select the arrow beside the name of the required feature. If no local WebLM server exists for the product, this column will be empty for all the licensed features.              |
| <b>IP Address</b>                | The IP addresses of the local WebLM servers of the product. By default, this column is empty. The system displays the IP address of the local WebLM servers only when you select the arrow beside the name of the required feature. If no local WebLM server exists for the product, this column will be empty for all the licensed features. |

| Name                       | Description  |
|----------------------------|--|
| <b>License Capacity</b>    | The total number of feature licenses purchased by the organization for the respective feature.   |
| <b>Currently Allocated</b> | The total number of feature licenses of the respective feature that have been allocated to the local WebLM servers of the product. If a licensed feature is not allocated to any local WebLM server, the system displays zero as the value of the column for the licensed feature. |
| <b>Available</b>           | This column lists the number of floating licenses of the respective feature that is currently available with the master WebLM server.  |

 **Note:**

To view information regarding the number of feature licenses of a feature that is allocated to each local WebLM server, click the arrow beside the name of the required feature. When you select the arrow beside a feature, the system displays new rows below the feature row. These new rows display the feature license allocation information for each local WebLM server to which the feature is allocated.

**Related topics:**

[Viewing allocations by features](#) on page 1142

## Allocations by Local WebLM field descriptions

Use this page to view the feature license allocation information by Local WebLM.

| Name                             | Description   |
|----------------------------------|---|
| <b>Select Local WebLM</b>        | The local WebLM servers for which you can view the feature license allocation information.  |
| <b>Last Allocation</b>           | The date and time when feature licenses were last allocated to the selected local WebLM server.   |
| <b>Status</b>                    | The success or failure of the last license allocation process executed for the selected local WebLM server. The allocation process can be a periodic allocation process or a non-periodic allocation process. If the status of the last license allocation process was Failed and there was a previous license allocation process success for the server, the system displays the date and time of the license allocation process that was last successful below the Last Allocation field. |
| <b>Feature (License Keyword)</b> | The name and license keyword of the counted features that have been allocated to the selected local WebLM server.   |
| <b>License Capacity</b>          | The total number of feature licenses purchased by the organization for each feature.  |

| Name                       | Description   |
|----------------------------|---|
| <b>Currently Allocated</b> | The total number of feature licenses of each feature that have been allocated to the selected local WebLM server. |
| <b>Available</b>           | The number of licenses currently available on the master WebLM server for allocation to local WebLM servers.      |

**Related topics:**

[Viewing allocations by local WebLM](#) on page 1144

---

## Change Allocations field descriptions

Use this page to change current feature license allocation information for each local WebLM server of a product.

| Name                             | Description   |
|----------------------------------|---|
| <b>Feature (License Keyword)</b> | The name and license keyword of the counted features that have been allocated to the selected local WebLM server. |
| <b>Local WebLM Name</b>          | The name of the local WebLM server.   |
| <b>IP Address</b>                | The IP addresses of the local WebLM servers of the product.   |
| <b>License Capacity</b>          | The total number of feature licenses purchased by the organization for each feature.                              |
| <b>Currently Allocated</b>       | The total number of feature licenses of each feature that have been allocated to the selected local WebLM server. |
| <b>Currently Used</b>            | The total number of feature licenses of each feature that are in use by the product.                              |
| <b>Available</b>                 | The number of floating licenses of each feature that is currently available with the local WebLM server.          |
| <b>New Allocation</b>            | The new number of licenses allocated to a local WebLM server.   |

| Button                    | Description   |
|---------------------------|---|
| <b>Submit Allocations</b> | Allocates the number of feature licenses specified in the New Allocations field to the corresponding local WebLM servers. |
| <b>Reset</b>              | Resets the values specified in the New Allocation fields to their default values.   |

**Related topics:**

[Changing allocations of licensed features for a local WebLM server](#) on page 1142

## Periodic Status field descriptions

Use the Periodic Status option to view the status of the periodic operations such as periodic allocation of feature licenses to the local WebLM server and querying the local WebLM server for usage report.

### Periodic Allocation

| Name                    | Description  |
|-------------------------|--|
| <b>Local WebLM Name</b> | The name of the local WebLM server of a product.   |
| <b>IP Address</b>       | The IP addresses of all the local WebLM servers of the product.  |
| <b>Last Allocation</b>  | The date and time when the last periodic license allocation process was executed for each local WebLM server. If the status of the last periodic license allocation process was Failed, this column also displays the date and time of the periodic license allocation process that was last successful. |
| <b>Status</b>           | The success or failure of the last periodic license allocation process executed for each local WebLM server. The system displays the date and time of the last successful periodic license allocation process in the <b>Last Allocation</b> column.  |

### Periodic Usage

| Name                    | Description   |
|-------------------------|---|
| <b>WebLM Name</b>       | The name of the master WebLM server and local WebLM servers of a product.   |
| <b>IP Address</b>       | The IP addresses of master and local WebLM servers of a product.  |
| <b>Last Usage Query</b> | The date and time when the last periodic usage query was executed for each WebLM server. If the status of the last periodic usage query was Failed, this column also displays the date and time of the periodic usage query that was last successful. |
| <b>Status</b>           | The success or failure of the last periodic usage query executed for each WebLM server. This column of a WebLM server will be empty if the server has not been queried even once for feature license usage.   |

### Related topics:

[Viewing periodic status of master and local WebLM servers](#) on page 1143

---

## Overuse field descriptions

Use this page to specify the overuse value in percent for licensed features of a product.

| Name                                | Description  |
|-------------------------------------|--|
| <b>Update percent overuse value</b> | The overuse values in percent. For example, if there are 10 licenses available for a feature and you have set the overuse value to 50 percent then it indicates that you have 5 buffer licenses for the feature. |

| Button        | Description   |
|---------------|---|
| <b>Submit</b> | Sets the overuse value.   |
| <b>Reset</b>  | Set the values in the <b>Update percent overuse value</b> to the default value. |

### Related topics:

[Specifying overuse limit for licensed features](#) on page 1143



# Chapter 9: Managing groups, roles and resources

---

## Managing groups

---

### Manage groups

The Group and Lookup Service is a shared service that provides group administration and a lookup service for all managed resources. The Group and Lookup Service supports group administration for common resources shared across elements such as roles and users as well as element specific resources that are not shared. Using this service you can add, modify and delete groups.

---

### Group Management

The Group and Lookup Service is a shared service that provides group administration and a lookup service for all managed resources. The Group and Lookup Service supports group administration for common resources shared across elements such as roles and users as well as element specific resources that are not shared. You can perform the following operations using the Group Management service:

- Create a group
- View and Modify groups
- Create a duplicate group by copying the properties of an existing group
- Assign and remove resources for groups
- Delete groups
- Import groups
- Synchronize groups

As a shared service, Group and Lookup reduces the time and effort involved for defining groups of managed resources that are needed by more than one application or service.

---

## Viewing Groups

- 
1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
  2. On the Group Management page, select a group and perform one of the following steps:
    - If the selected group is a selection based group member, then click **View**.
    - If selected group is a query based group, then on the View Group page click **Execute Query**.

---

### Result

The View Group page displays the selected group details along with the resources assigned to them.

### Related topics:

[Searching for resources based on group membership](#) on page 1170

[Searching for resources based on group membership](#) on page 1170

[View Group field descriptions](#) on page 1176

[View Group field descriptions](#) on page 1176

---

## Creating groups

- 
1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
  2. Perform any one of the following steps:
    - To create a group, click **New** on the Group Management page.
    - To create a subgroup under a group or a subgroup, select a group or a subgroup and click **New** on the Group Management page.
  3. On the Create Group page, enter the appropriate information.
  4. Click **Commit** to create the new group.

---

### Related topics:

[Assigning resources to a group](#) on page 1168

[Assigning resources to a group](#) on page 1168

[Removing assigned resources from a group](#) on page 1173

[Removing assigned resources from a group](#) on page 1173

[New Group field descriptions](#) on page 1177

[New Group field descriptions](#) on page 1177

---

## Modifying Groups

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
3. Select a group.
4. To access the **Edit Group** page, perform any one of the following steps:
  - On the Group Management page, click **Edit**.
  - On the Group Management page, click **View > Edit**.
5. On the Edit Group page, enter the appropriate information.
6. Click **Commit** to save the changes to the database.

---

### Related topics:

[Assigning resources to a group](#) on page 1168

[Assigning resources to a group](#) on page 1168

[Removing assigned resources from a group](#) on page 1173

[Removing assigned resources from a group](#) on page 1173

[Edit Group field descriptions](#) on page 1179

[Edit Group field descriptions](#) on page 1179

---

## Creating duplicate groups

You can use this feature to create a duplicate group by copying the properties of an existing group. When you create a duplicate group, the system copies all the information from the existing group to the new group.

1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
2. On the Group Management page, select a group and click **Duplicate**.
3. On the Duplicate Group page, perform any one of the following steps:
  - To create a duplicate group at root level, click **Root** .
  - To create a duplicate group under a group or a subgroup, select a group or a subgroup and click **Selected group** .



**Note:**

Click **+** to view the subgroups of a group.

---

## Result

The duplicate group appears on the Group Management page as copy of the parent group (the parent group from which the group is created).



**Note:**

Use the edit functionality to change the properties of this group.

## Related topics:

[Assigning resources to a group](#) on page 1168

[Assigning resources to a group](#) on page 1168

[Removing assigned resources from a group](#) on page 1173

[Removing assigned resources from a group](#) on page 1173

[Duplicate Group field descriptions](#) on page 1182

[Duplicate Group field descriptions](#) on page 1182

---

## Deleting groups

1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
  2. Select the groups that you want to delete.
  3. Click **Delete** on the Group Management page.
  4. On the Delete Group Confirmation page, click **Delete**.
-

**Related topics:**

[Delete Group Confirmation field descriptions](#) on page 1181

[Delete Group Confirmation field descriptions](#) on page 1181

---

## Moving groups

You can move a group from one group to an another group or to the root level. You can also move a group from the root level to an another group.

- 
1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
  2. On the Group Management page, select a group and click **More Actions > Move**.
  3. On the Move Group page, Perform any one of the following steps:
    - To move a group to the root level, click **Root** .
    - To move a group to another group or a subgroup, select the group or the subgroup and click **Selected group** .

**Note:**

Click **+** to view the subgroups of a group.

---

**Related topics:**

[Move Group field descriptions](#) on page 1182

[Move Group field descriptions](#) on page 1182

---

## Importing groups

You can import groups from a file.

**Prerequisites**

The file from which you import groups must conform to the XML file schema.

- 
1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
  2. On the Group Management page, click **More Actions > Import**.

3. On the Import Groups page, enter the path of the file containing the groups.
4. Click **Import**.

---

**Related topics:**

[Import Groups field descriptions](#) on page 1183

[Import Groups field descriptions](#) on page 1183

---

## Synchronizing resources for a resource type

1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
2. On the Group Management page, click **More Actions > Sync**.
3. On the Resource Synchronization page, select the type of resources from the **Type** drop-down field.
4. Click **Sync**.

---

**Related topics:**

[Resource Synchronization field descriptions](#) on page 1183

[Resource Synchronization field descriptions](#) on page 1183

---

## Switching to table view

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
3. On the Group Management page, click **Switch to Table**.



**Note:**

**Switch to Table** is a toggle button.

---

**Related topics:**

[Viewing Groups](#) on page 1162

[Viewing Groups](#) on page 1162  
[Creating groups](#) on page 1162  
[Creating groups](#) on page 1162  
[Modifying Groups](#) on page 1163  
[Modifying Groups](#) on page 1163  
[Creating duplicate groups](#) on page 1163  
[Creating duplicate groups](#) on page 1163  
[Deleting groups](#) on page 1164  
[Deleting groups](#) on page 1164  
[Moving groups](#) on page 1165  
[Moving groups](#) on page 1165  
[Importing groups](#) on page 1165  
[Importing groups](#) on page 1165  
[Synchronizing resources for a resource type](#) on page 1166  
[Synchronizing resources for a resource type](#) on page 1166  
[Switching to tree view](#) on page 1167  
[Switching to tree view](#) on page 1167  
[Filtering groups](#) on page 1171  
[Filtering groups](#) on page 1171  
[Searching Groups](#) on page 1172  
[Searching Groups](#) on page 1172

---

## Switching to tree view

- 
1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
  2. On the Group Management page, click **Switch to Tree**.  
**Switch to Tree** is a toggle button.
- 

### Related topics:

[Viewing Groups](#) on page 1162  
[Viewing Groups](#) on page 1162  
[Creating groups](#) on page 1162  
[Creating groups](#) on page 1162  
[Modifying Groups](#) on page 1163  
[Modifying Groups](#) on page 1163  
[Creating duplicate groups](#) on page 1163

- [Creating duplicate groups](#) on page 1163
- [Deleting groups](#) on page 1164
- [Deleting groups](#) on page 1164
- [Moving groups](#) on page 1165
- [Moving groups](#) on page 1165
- [Importing groups](#) on page 1165
- [Importing groups](#) on page 1165
- [Synchronizing resources for a resource type](#) on page 1166
- [Synchronizing resources for a resource type](#) on page 1166
- [Switching to table view](#) on page 1166
- [Switching to table view](#) on page 1166
- [Filtering groups](#) on page 1171
- [Filtering groups](#) on page 1171
- [Searching Groups](#) on page 1172
- [Searching Groups](#) on page 1172

---

## Assigning resources to a group

You can assign only resources of the type that is configured for the group. The type of resources that can become the member of a group is set when you create a group. If the type of resource is set to ALL, you can assign all types of resource to the group. If the type is set to a specific resource type, only resources of that type can be assigned to that group.

- 
1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
  2. Perform one of the following steps:
    - Click **New > Assign Resources**.
    - Select a group if you are assigning a resource to an existing group and click **Edit > Assign Resources**.
    - Select a group if you are assigning a resource to an existing group and click **View > Edit > Assign Resources**.
  3. On the Resources page, select a resource.

The Resources page displays all the resources available in the application, but you can not select the resources that are already assigned to the group.

You can also search for a resource using the Advance search functionality.
  4. Click **Add To a Group** .
-

## Result

The application adds the selected resources to the group.

### Related topics:

[Resources field descriptions](#) on page 1183

[Resources field descriptions](#) on page 1183

---

## Searching for resources

1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
2. To access the **Resources** page, perform any one of these steps.
  - On the Group Management page, click **New > Assign Resources**.
  - On the Group Management page, click **Edit > Assign Resources**.
  - On the Group Management page, click **View > Edit > Assign Resources**.
3. On the Resources page, click **Advanced Search**.
4. Select resource type from the **Type** drop-down field.
5. In the Click to Search to find alarms for the given search conditions section, select the search criterion from each of the drop-down fields.
  - a. Select the search criterion from the first drop-down field.
  - b. Select the operator from the second drop-down field.
  - c. Enter search value in the third field.
6. If you want to add another search condition, click the **+** button.  
Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.
7. Select the AND or OR from the drop-down field.  
This option appears when you add a search condition using the **+** button.
8. Click **Search**.

---

## Result

The Resources section displays the resources matching the search criteria. If no resources are found matching the search criteria, the Resource section displays a message No records are found.

---

## Searching for resources based on group membership

You can search resources based on group membership. You can search resources using the Advanced Search feature on the Group Management page.

 **Note:**

You cannot search resources based on group membership, using the Advanced Search feature provided on the Resources page, .

- 
1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
  2. On the Group Management page, click **Advanced Search**.
  3. In the **Criteria** section, select the search criterion from each of the drop-down fields.
    - a. Select the search criterion from the first field.
    - b. Select the operator from the second field.
    - c. Enter the search value in the third field.
  4. If you want to add another search condition, click the + button.  
Click - to delete a search condition. You can delete a search condition only if you have more than one search condition.
  5. Select the AND or OR from the drop-down field.  
This option appears when you add a search condition using the + button
  6. Click **Search**.

---

### Result

The Groups and Lookup service renders a list of groups matching the search criteria.

### Related topics:

[Viewing Groups](#) on page 1162

[Viewing Groups](#) on page 1162

[Resources field descriptions](#) on page 1191

[Resources field descriptions](#) on page 1191

---

## Filtering groups

You can apply filter on the following three columns:

- Name
- Type
- Group

You may filter groups using one or multiple column filters.

- 
1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
  2. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
  3. On the Group Management page, click **Filter: Enable**.
  4. Enter the group name in the field under the **Name** column.
  5. Select the resource type from the drop-down field under the **Type** column.
  6. Enter the hierarchy level under the **Hierarchy** column.  
When you enter a hierarchy level, the table displays only those groups that you have created under that level. For example, if you want to view all the groups that you have created under root, enter / as hierarchy level.
  7. Click **Apply** .

**Note:**

To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

---

### Result

The table displays only those groups that matches the filter criteria.

---

## Filtering resources

- 
1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
  2. Select a group if you are assigning a resource to an existing group.
  3. To access the **Resources** page, perform one of the following steps.

- On the Group Management page, click **New > Assign Resources**.
  - On the Group Management page, click **Edit > Assign Resources**.
  - On the Group Management page, click **View > Edit > Assign Resources**.
4. On the Resources page, click **Filter: Enable**.
  5. Enter the resource name in the field under the **Name** column.

 **Note:**

You may choose to apply filter on one column or multiple columns.

6. Select the resource type from the field under the **Type** column.

 **Note:**

You may choose to apply filter on one column or multiple columns.

7. Click **Apply** .

 **Note:**

To hide the column filters, click **Disable**. This action does not clear the filter criteria that you have set in the column filters.

---

## Result

The table displays resources that matches the filter criteria.

---

## Searching Groups

1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
2. On the Group Management page, click **Advanced Search** displayed at the upper-right corner of the page.
3. In the Criteria section, do the following:
  - a. Select the search criterion from the first drop-down field.
  - b. Select the operator from the second drop-down field.
  - c. Enter the search value in the third field.

 **Note:**

If you want to add a search condition, click **+** and repeat sub steps a through c listed in step 4.

**Note:**

If you want to delete a search condition, click -. This button is available if there are more than one search condition.

4. Click **Search**.

---

## Result

The page displays the groups that matches the value specified for the search criteria.

---

## Removing assigned resources from a group

1. On the System Manager console, click **Groups & Roles > Groups** in the left navigation pane.
2. Perform one of the following steps:
  - If you assigned resources to the group while creating a new group, select the resources and click > **Remove**.
  - Select a group and click **Edit > Remove**.
  - Select a group and click **View > Edit > Remove**.

---

## Group Management field descriptions

Use this page to manage groups. You can use this page to perform the following tasks:

- Create, modify, view and delete a group.
- Create a copy of an existing group.
- Move a selected group from one group to another group.
- Import groups from an move a selected group from one group to another group.
- Synchronize resources for a resource type.
- Define search conditions to Search for groups.
- Apply column filters in the **Groups section** to view groups matching the filter criteria.

| Name             | Description                           |
|------------------|---------------------------------------|
| Select check box | Use this check box to select a group. |

| Name               | Description   |
|--------------------|---|
| <b>Name</b>        | Name of the group.  |
| <b>Type</b>        | Group type based on the resources.  |
| <b>Hierarchy</b>   | Position of the group in the hierarchy.   |
| <b>Description</b> | A brief description about the group.  |
| <b>Dynamic</b>     | <p>The value indicates whether resource assignment for the group is dynamic or static.</p> <p> <b>Note:</b><br/>You can view this column in Tree view.</p> |

| Button                          | Description   |
|---------------------------------|---|
| <b>View</b>                     | Opens the View Group page that allows you to see the details of the selected group.   |
| <b>Edit</b>                     | Opens the Edit Group page you can use to modify the information of the selected group.  |
| <b>New</b>                      | Opens the Create Group page you can use to create a new group.  |
| <b>Duplicate</b>                | Opens the Duplicate Group page that you can use to duplicate a group to another selected group.   |
| <b>Delete</b>                   | Deletes selected groups.  |
| <b>More Actions &gt; Move</b>   | Opens the Move page that you can use to move a group to another selected group.   |
| <b>More Actions &gt; Import</b> | Opens the Import page that you can use to import a group.   |
| <b>More Actions &gt; Sync</b>   | Opens the Resource Sync page that you can use to synchronize resources for a resource type.   |
| <b>Switch To Tree</b>           | <p>Displays groups in a tree view. This is a toggle button.</p> <p> <b>Note:</b><br/>You can view this button when you are in a Tree view.</p>   |
| <b>Switch To Table</b>          | <p>Displays groups in a table view. This is a toggle button.</p> <p> <b>Note:</b><br/>You can view this button when you are in a Table view.</p> |
| <b>Advanced Search</b>          | Displays fields that you can use to specify the search criteria for searching a group.  |
| <b>Filter: Enable</b>           | Displays fields under select columns that you can use to set filter criteria. This is a toggle button.  |

| Button                 | Description  |
|------------------------|--|
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button. |
| <b>Filter: Clear</b>   | Clears the filter criteria.  |
| <b>Filter: Apply</b>   | Filters groups based on the filter criteria.   |
| <b>Select: All</b>     | Selects all the groups in the table.   |
| <b>Select: None</b>    | Clears all the check box selections.   |
| <b>Refresh</b>         | Refreshes the groups information.  |

### Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the upper-right corner of the page

| Name            | Description  |
|-----------------|--|
| <b>Criteria</b> | <p>Displays the following three fields:</p> <ul style="list-style-type: none"> <li>• Drop-down 1 - The list of criteria that you can use to search groups.</li> <li>• Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field.</li> <li>• Field 3 – The value for the search criterion. The Group Management service retrieves and displays groups that match this value.</li> </ul> |

| Button        | Description   |
|---------------|---|
| <b>Clear</b>  | Clears the search value that you entered in the third field.  |
| <b>Search</b> | Searches group based on the specified search conditions and displays the search results in the <b>Groups</b> section. |
| <b>Close</b>  | Cancel the search operation and hides the <b>Criteria</b> section.  |

### Related topics:

- [Viewing Groups](#) on page 1162
- [Viewing Groups](#) on page 1162
- [Creating groups](#) on page 1162
- [Creating groups](#) on page 1162
- [Modifying Groups](#) on page 1163
- [Modifying Groups](#) on page 1163
- [Creating duplicate groups](#) on page 1163
- [Creating duplicate groups](#) on page 1163
- [Deleting groups](#) on page 1164
- [Deleting groups](#) on page 1164

- [Moving groups](#) on page 1165
- [Moving groups](#) on page 1165
- [Importing groups](#) on page 1165
- [Importing groups](#) on page 1165
- [Synchronizing resources for a resource type](#) on page 1166
- [Synchronizing resources for a resource type](#) on page 1166
- [Switching to table view](#) on page 1166
- [Switching to table view](#) on page 1166
- [Switching to tree view](#) on page 1167
- [Switching to tree view](#) on page 1167
- [Filtering groups](#) on page 1171
- [Filtering groups](#) on page 1171
- [Searching Groups](#) on page 1172
- [Searching Groups](#) on page 1172

## View Group field descriptions

Use this page to view a selected group. You can not modify the information in the fields while you are in view mode.

### View Group

| Name                    | Description   |
|-------------------------|---|
| <b>Name</b>             | Unique name of the group.   |
| <b>Type</b>             | Group type based on the resources . The options are: <ul style="list-style-type: none"> <li>• Creating the group having member of same resource type.</li> <li>• All — Creating the group without any restrictions on its member.</li> </ul>  |
| <b>Group Membership</b> | The options are : <ul style="list-style-type: none"> <li>• Query Based — Use this option if you want to create a group that contains resources that matches a specific query criteria. Query based groups can have resources of a specific type only. You can create only typed (resource type) query groups. Thus, these groups cannot have subgroups.</li> <li>• Selection Based — Use this option if you want to create a group that contains resources based on static assignment. These groups can have subgroups. Subgroups and parent group may have members of same resource type or different resource types.</li> </ul> |
| <b>Description</b>      | A brief description about the group.  |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Edit Group page that you can use to modify the group information. |
| <b>Done</b> | Closes the View Group page and takes you back to the Group Management page. |

## Define Query

The page displays these fields when you use **Query Based** option for creating group members.

| Name/Button          | Description   |
|----------------------|---|
| <b>Define Query</b>  | <p>Displays the following three fields:</p> <ul style="list-style-type: none"> <li>• Drop-down 1 - The list of criteria that you can use to search resources.</li> <li>• Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field.</li> <li>• Field 3 – The value corresponding to the search criteria.</li> </ul> |
| <b>+</b>             | Adds a search condition row for defining a new search condition.  |
| <b>–</b>             | Removes a search condition.   |
| <b>Execute Query</b> | <p>Runs the query and fetches resources matching the search conditions defined in the query. The page displays these resources in the <b>Results</b> section.</p> <p> <b>Note:</b><br/>This button is visible only when you create a query based group.</p>  |

The page displays following fields for assigned resources.

| Name        | Description           |
|-------------|-----------------------|
| <b>Name</b> | Name of the resource. |
| <b>Type</b> | Type of the resource. |

### Related topics:

[Viewing Groups](#) on page 1162

[Viewing Groups](#) on page 1162

---

## New Group field descriptions

Use this page to create a new group.

## New Group

| Name                    | Description   |
|-------------------------|---|
| <b>Name</b>             | Unique name of the group.   |
| <b>Type</b>             | Group type based on the resources . The options are: <ul style="list-style-type: none"> <li>• Creating the group having member of same resource type.</li> <li>• All — Creating the group without any restrictions on its member.</li> </ul>  |
| <b>Group Membership</b> | The options are : <ul style="list-style-type: none"> <li>• Query Based — Use this option if you want to create a group that contains resources that matches a specific query criteria. Query based groups can have resources of a specific type only. You can create only typed (resource type) query groups. Thus, these groups cannot have subgroups.</li> <li>• Selection Based — Use this option if you want to create a group that contains resources based on static assignment. These groups can have subgroups. Subgroups and parent group may have members of same resource type or different resource types.</li> </ul> |
| <b>Description</b>      | A brief description about the group.  |

| Button                  | Description   |
|-------------------------|---|
| <b>Assign Resources</b> | Opens the Resources page that you can use to search and assign resources to a group.<br><br> <b>Note:</b><br>when you use <b>Selection Based</b> option for creating group members in the group. |
| <b>Commit</b>           | Creates a new group with the specified configurations.  |
| <b>Cancel</b>           | Closes the Create Group page without saving any information on the page and returns to the Group Management page.   |

## Define Query

The page displays the following fields when you use **Query Based** option for creating group members.

| Name/Button         | Description  |
|---------------------|--|
| <b>Define Query</b> | Displays the following three fields: <ul style="list-style-type: none"> <li>• Drop-down 1 - The list of criteria that you can use to search resources.</li> <li>• Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field.</li> <li>• Field 3 – The value corresponding to the search criteria.</li> </ul> |

| Name/Button          | Description  |
|----------------------|--|
| +                    | Adds a search condition row for defining a new search condition.   |
| -                    | Removes a search condition.  |
| <b>Execute Query</b> | <p>Runs the query and fetches resources matching the search conditions defined in the query. The page displays these resources in the <b>Results</b> section.</p> <p> <b>Note:</b><br/>This button is visible only when you create a query based group.</p> |
| <b>Name</b>          | Name of the resource.  |
| <b>Type</b>          | Type of the resource.  |

### Assigned Resources

The page displays the following fields when you use **Selection Based** option for creating group members.

| Name                    | Description  |
|-------------------------|--|
| <b>Name</b>             | Name of the resource.  |
| <b>Type</b>             | Type of the resource.  |
| <b>Assign Resources</b> | Opens the Resources page that you can use to search and assign resources to a group. |
| <b>Remove</b>           | Remove the selected resources from the list of assigned resources.                   |

#### Related topics:

[Creating groups](#) on page 1162

[Creating groups](#) on page 1162

[Assigning resources to a new group](#) on page 1186

[Assigning resources to a new group](#) on page 1186

---

## Edit Group field descriptions

Use this page to modify a selected group. You cannot modify the following fields in the page:

- Type
- Group Membership

### Edit Group

| Name        | Description               |
|-------------|---------------------------|
| <b>Name</b> | Unique name of the group. |

| Name                    | Description   |
|-------------------------|---|
| <b>Type</b>             | Group type based on the resources . The options are: <ul style="list-style-type: none"> <li>• Creating the group having member of same resource type.</li> <li>• All — Creating the group without any restrictions on its member.</li> </ul>  |
| <b>Group Membership</b> | The options are : <ul style="list-style-type: none"> <li>• Query Based — Use this option if you want to create a group that contains resources that matches a specific query criteria. Query based groups can have resources of a specific type only. You can create only typed (resource type) query groups. Thus, these groups cannot have subgroups.</li> <li>• Selection Based — Use this option if you want to create a group that contains resources based on static assignment. These groups can have subgroups. Subgroups and parent group may have members of same resource type or different resource types.</li> </ul> |
| <b>Description</b>      | A brief description about the group.  |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Saves the changes in the database.  |
| <b>Cancel</b> | Closes the Edit Group page without saving any information and returns to the Group Management page. |

### Define Query

The page displays the following fields when you use **Query Based** option for creating group members.

| Name/Button          | Description  |
|----------------------|--|
| <b>Define Query</b>  | Displays the following three fields: <ul style="list-style-type: none"> <li>• Drop-down 1 - The list of criteria that you can use to search resources.</li> <li>• Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field.</li> <li>• Field 3 – The value corresponding to the search criteria.</li> </ul> |
| <b>+</b>             | Adds a search condition row for defining a new search condition.   |
| <b>-</b>             | Removes a search condition.  |
| <b>Execute Query</b> | Runs the query and fetches resources matching the search conditions defined in the query. The page displays these resources in the <b>Results</b> section.<br><br> <b>Note:</b><br>This button is visible only when you create a query based group.   |

| Name/Button | Description           |
|-------------|-----------------------|
| <b>Name</b> | Name of the resource. |
| <b>Type</b> | Type of the resource. |

### Assigned Resources

The page displays the following fields when you use **Selection Based** option for creating group members.

| Name                    | Description  |
|-------------------------|--|
| <b>Name</b>             | Name of the resource.  |
| <b>Type</b>             | Type of the resource.  |
| <b>Assign Resources</b> | Opens the Resources page that you can use to search and assign resources to a group. |
| <b>Remove</b>           | Remove the selected resources from the list of assigned resources.                   |

### Related topics:

[Modifying Groups](#) on page 1163

[Modifying Groups](#) on page 1163

---

## Delete Group Confirmation field descriptions

Use this page to delete the groups listed in the table.

| Name                   | Description                              |
|------------------------|--|
| <b>Name</b>            | Name of the group.                       |
| <b>Type</b>            | Group type based on the resources.       |
| <b>Hierarchy</b>       | Position of the group in the hierarchy.  |
| <b>Description</b>     | A brief description about the group.     |
| <b>Sub-Group Count</b> | Count of sub groups in the parent group. |
| <b>Resource Count</b>  | Count of the resources in the group.     |

| Button        | Description  |
|---------------|--|
| <b>Delete</b> | Deletes the groups listed in the table.                                      |
| <b>Cancel</b> | Cancel the delete operation and takes you back to the Group Management page. |

### Related topics:

[Deleting groups](#) on page 1164

[Deleting groups](#) on page 1164

---

## Duplicate Group field descriptions

Use this page to create a duplicate group from an existing group.

| Name          | Description   |
|---------------|---|
| <b>Select</b> | Select a group  |
| <b>Name</b>   | The groups under which you can create a duplicate group. Click the + to expand a group. |

| Button                | Description   |
|-----------------------|---|
| <b>Root</b>           | Creates a duplicate group at the root level.              |
| <b>Selected Group</b> | Creates a duplicate group under the selected group.       |
| <b>Cancel</b>         | Closes the page and returns to the Group Management page. |

### Related topics:

[Creating duplicate groups](#) on page 1163

[Creating duplicate groups](#) on page 1163

---

## Move Group field descriptions

Use this page to move a group to another group or to root level.

| Name          | Description  |
|---------------|--|
| <b>Select</b> | Select a group   |
| <b>Name</b>   | The groups to which you can move the selected group . Click the + to expand a group. |

| Button                | Description  |
|-----------------------|--|
| <b>Root</b>           | Moves the selected group to the root level   |
| <b>Selected Group</b> | Moves the selected group to the group that you have selected in the <b>Name</b> column |
| <b>Cancel</b>         | Closes the Move Group page and returns to the Group Management page.                   |

### Related topics:

[Moving groups](#) on page 1165

[Moving groups](#) on page 1165

---

## Import Groups field descriptions

Use this page to import groups from an XML file.

| Name                        | Description   |
|-----------------------------|---|
| <b>Please select a file</b> | The XML file that contains the groups to be imported.               |
| <b>Import</b>               | Imports the file that contains the groups.                          |
| <b>Cancel</b>               | Closes the Import Groups page and returns to Group Management page. |

### Related topics:

[Importing groups](#) on page 1165

[Importing groups](#) on page 1165

---

## Resource Synchronization field descriptions

Use this page to synchronize resources for a resource type.

| Name          | Description   |
|---------------|---|
| <b>Type</b>   | The type based on the resources it contains.  |
| <b>Done</b>   | Synchronizes resources for the selected resource type and returns to the Group Management page. |
| <b>Cancel</b> | Closes the Resource Synchronization page and returns to Group Management page.                  |

### Related topics:

[Synchronizing resources for a resource type](#) on page 1166

[Synchronizing resources for a resource type](#) on page 1166

---

## Resources field descriptions

Use this page to search and assign a resource to a group. You can use this page to perform the following tasks:

- Assign selected resources to a new or an existing group.
- Apply filters to view only those resources that match filter criteria.

- Define search conditions to search resources that match the search conditions.
- View the details of the attributes for the selected resources.
- View the group membership details for the selected resources.

The page has the following sections:

- Criteria
- Resources
- Attributes of resources
- Resource is member of following groups

**Resources section**

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use the check box to select a record.  |
| <b>ID</b>               | Unique name of the resource. Also known as native id of the resource                       |
| <b>Type</b>             | The type based on the resources.   |
| <b>View Details</b>     | Displays the attributes and membership details of the selected resources on the same page. |

| Button                 | Description  |
|------------------------|--|
| <b>Add to Group</b>    | Adds the selected resources to the group.  |
| <b>Cancel</b>          | Closes the Resources page and take you back to the Create Group page.  |
| <b>Advanced Search</b> | Displays fields that you can use to specify the search criteria for searching a resource.  |
| <b>Filter: Enable</b>  | Displays fields under the columns, <b>Name</b> and <b>Type</b> . You can use them to set filter criteria. This is a toggle button. |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                                     |
| <b>Filter: Apply</b>   | Filters resources based on the filter criteria.  |
| <b>Select: All</b>     | Selects all the resources displayed in the table in the Resources section.   |
| <b>Select: None</b>    | Clears the selection for the resources that you have selected.   |
| <b>Refresh</b>         | Refreshes resource information in the table.   |

### Attributes of resources section

| Name         | Description                                       |
|--------------|---|
| <b>Name</b>  | Name of the attribute.                            |
| <b>Value</b> | Value assigned to the attribute for the resource. |

### Resource is member of following groups section

| Name               | Description                                    |
|--------------------|--|
| <b>Name</b>        | Unique name of the group.                      |
| <b>Type</b>        | Group type based on the resources it contains. |
| <b>Hierarchy</b>   | Position of the group in the hierarchy.        |
| <b>Description</b> | A brief description about the group.           |

### Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the upper-right corner of the page.

| Name                       | Description  |
|----------------------------|--|
| <b>Type</b>                | The types based on the resources it contains.  |
| <b>Resource Attributes</b> | <p>Displays the following three fields:</p> <ul style="list-style-type: none"> <li>• Drop-down 1 - The criteria for searching a resource. The options are attributes of resources for the attribute type selected in the <b>Type</b> drop-down list.</li> <li>• Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of attribute selected in the first drop-down list.</li> <li>• Field 3 – The value corresponding to the search criterion.</li> </ul> |

| Button                 | Description  |
|------------------------|--|
| <b>Clear</b>           | Clears the search value that you entered in the third field.       |
| <b>Search</b>          | Searches the resources matching the search conditions.             |
| <b>Close</b>           | Closes the Criteria section.                                       |
| <b>Advanced Search</b> | Cancel the search operation and hides the <b>Criteria</b> section. |

### Related topics:

[Assigning resources to a group](#) on page 1168

[Assigning resources to a group](#) on page 1168

---

## Managing resources

---

### Manage resources

System Manager contains resources of different types such as users, roles and so on. You can view these resources, filter these resources base on a filter criteria, add resources of same or different types in a group.

---

### Accessing resources

- 
1. Log in to the System Manager web interface as an administrator.
  2. Click **Groups & Roles > Resources** in the left navigation pane
- 

#### Related topics:

- [Assigning resources to a new group](#) on page 1186
- [Assigning resources to a new group](#) on page 1186
- [Adding resources to a selected group](#) on page 1188
- [Adding resources to a selected group](#) on page 1188
- [Resources field descriptions](#) on page 1191
- [Resources field descriptions](#) on page 1191

---

### Assigning resources to a new group

Use this functionality to create a new group and assign resources to this group. You can choose to create the new group at root level or under an existing group.

- 
1. On the System Manager console, click **Groups & Roles > Resources** in the left navigation pane.
  2. Select a resource. You can also click the **Advanced Search** link to search a resource.

3. Click **Add To New Group** .
4. Perform one of the following steps:
  - To add a resource to a new group, perform the following steps:
    - i. On the Choose Parent Group page, click **Root** .
    - ii. On the Create Group page, enter the appropriate information.
    - iii. Click **Commit** to add the selected resource to the new group at root level.
  - To add a resource to a new subgroup under a group, perform the following steps:
    - i. On the Choose Parent Group page, click a group.

**Note:**

If you want to select a subgroup of a group, click **+** and click the subgroup.

- ii. Click **Selected Group**.
- iii. On the Create Group page, enter the appropriate information.
- iv. Click **Commit**.

**Note:**

The System creates the new group and assigns the selected resources. This group is added under the group that you selected on the Choose Parent Group page.

---

**Related topics:**

[New Group field descriptions](#) on page 1177

[New Group field descriptions](#) on page 1177

[Accessing resources](#) on page 1186

[Accessing resources](#) on page 1186

[Adding resources to a selected group](#) on page 1188

[Adding resources to a selected group](#) on page 1188

[Resources field descriptions](#) on page 1191

[Resources field descriptions](#) on page 1191

---

## Adding resources to a selected group

- 
1. On the System Manager console, click **Groups & Roles > Resources** in the left navigation pane.
  2. Select a resource from the resource table.  
You can also click the **Advanced Search** link to search a resource.
  3. Click **Add To Group** .
  4. On the Choose Parent Group page, click a group.
  5. click **Selected Group**.  
The Group Management module assign the selected resources to the groups selected on the Choose Parent Group page.

---

### Related topics:

[Accessing resources](#) on page 1186

[Accessing resources](#) on page 1186

[Assigning resources to a new group](#) on page 1186

[Assigning resources to a new group](#) on page 1186

[Resources field descriptions](#) on page 1191

[Resources field descriptions](#) on page 1191

---

## Searching for resources

- 
1. On the System Manager console, click **Groups & Roles > Resources** in the left navigation pane.
  2. On the Resources page, click **Advanced Search**.
  3. Select resource type from the **Type** drop-down field.
  4. In the Click to Search to find alarms for the given search conditions section, select the search criterion from each of the drop-down fields.
    - a. Select the search criterion from the first drop-down field.
    - b. Select the operator from the second drop-down field.
    - c. Enter search value in the third field.
  5. If you want to add another search condition, click the **+** button.

Click  to delete a search condition. You can delete a search condition only if you have more than one search condition.

6. Select the AND or OR from the drop-down field.  
This option appears when you add a search condition using the **+** button.
7. Click **Search**.

---

## Result

The Resources section displays the resources matching the search criteria. If no resources are found matching the search criteria, the Resource section displays a message No records are found.

---

## Filtering resources

You can filter and view resources that meet the specified filter criteria. Applying the filters requires you to specify the filter criteria in the fields provided under columns in the table displaying the resources. The column titles are the filter criteria. You can filter resources on multiple filter criteria.

1. On the System Manager console, click **Groups & Roles > Resources** in the left navigation pane.
2. On the Resources page, click **Filter: Enable**.
3. Enter the resource name in the field under the **Name** column.



**Note:**

You may choose to apply filter on one column or multiple columns.

4. Select the resource type from the field under the **Type** column.



**Note:**

You may choose to apply filter on one column or multiple columns.

5. Click **Apply** .



**Note:**

To hide the column filters, click **Disable**. This action does not clear the filter criteria that you have set in the column filters.

---

## Result

The table displays resources that matches the filter criteria.

## New Group field descriptions

Use this page to create a new group.

### New Group

| Name                    | Description   |
|-------------------------|---|
| <b>Name</b>             | Unique name of the group.   |
| <b>Type</b>             | Group type based on the resources . The options are: <ul style="list-style-type: none"> <li>• Creating the group having member of same resource type.</li> <li>• All — Creating the group without any restrictions on its member.</li> </ul>  |
| <b>Group Membership</b> | The options are : <ul style="list-style-type: none"> <li>• Query Based — Use this option if you want to create a group that contains resources that matches a specific query criteria. Query based groups can have resources of a specific type only. You can create only typed (resource type) query groups. Thus, these groups cannot have subgroups.</li> <li>• Selection Based — Use this option if you want to create a group that contains resources based on static assignment. These groups can have subgroups. Subgroups and parent group may have members of same resource type or different resource types.</li> </ul> |
| <b>Description</b>      | A brief description about the group.  |

| Button                  | Description   |
|-------------------------|---|
| <b>Assign Resources</b> | Opens the Resources page that you can use to search and assign resources to a group.<br><br> <b>Note:</b><br>when you use <b>Selection Based</b> option for creating group members in the group. |
| <b>Commit</b>           | Creates a new group with the specified configurations.  |
| <b>Cancel</b>           | Closes the Create Group page without saving any information on the page and returns to the Group Management page.   |

### Define Query

The page displays the following fields when you use **Query Based** option for creating group members.

| Name/Button         | Description                          |
|---------------------|--------------------------------------|
| <b>Define Query</b> | Displays the following three fields: |

| Name/Button          | Description   |
|----------------------|---|
|                      | <ul style="list-style-type: none"> <li>• Drop-down 1 - The list of criteria that you can use to search resources.</li> <li>• Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field.</li> <li>• Field 3 – The value corresponding to the search criteria.</li> </ul> |
| +                    | Adds a search condition row for defining a new search condition.  |
| –                    | Removes a search condition.   |
| <b>Execute Query</b> | <p>Runs the query and fetches resources matching the search conditions defined in the query. The page displays these resources in the <b>Results</b> section.</p> <p> <b>Note:</b><br/>This button is visible only when you create a query based group.</p>  |
| <b>Name</b>          | Name of the resource.   |
| <b>Type</b>          | Type of the resource.   |

### Assigned Resources

The page displays the following fields when you use **Selection Based** option for creating group members.

| Name                    | Description  |
|-------------------------|--|
| <b>Name</b>             | Name of the resource.  |
| <b>Type</b>             | Type of the resource.  |
| <b>Assign Resources</b> | Opens the Resources page that you can use to search and assign resources to a group. |
| <b>Remove</b>           | Remove the selected resources from the list of assigned resources.                   |

---

## Resources field descriptions

Use this page to search and assign a resource to a group. You can use this page to perform the following tasks:

- Add a selected resource to a new group or to a chosen group.
- Apply filters to view only those resources that matches filter criteria.
- Define search conditions to search resources that matches the search conditions.
- View the details of the attributes for the selected resources.
- View the group membership details for the selected resources.

The page has the following sections:

- Criteria
- Resources
- Attributes of resources
- Resource is member of following groups

### Resources section

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use the check box to select a record.  |
| <b>ID</b>               | Unique name of the resource. Also known as native id of the resource                       |
| <b>Type</b>             | The type based on the resources.   |
| <b>View Details</b>     | Displays the attributes and membership details of the selected resources on the same page. |

| Button                  | Description  |
|-------------------------|--|
| <b>Add to Group</b>     | Opens Choose Group page. Use this page to choose a group in which you want to add the selected resource.                           |
| <b>Add to New Group</b> | Opens Choose Parent Group page. Use this page to add the selected resources to a new group or to a chosen group.                   |
| <b>Cancel</b>           | Closes the Resources page returns to the Create Group page.  |
| <b>Advanced Search</b>  | Displays fields that you can use to specify the search criteria for searching a resource.  |
| <b>Filter: Enable</b>   | Displays fields under the columns, <b>Name</b> and <b>Type</b> . You can use them to set filter criteria. This is a toggle button. |
| <b>Filter: Disable</b>  | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                                     |
| <b>Filter: Apply</b>    | Filters resources based on the filter criteria.  |
| <b>Select: All</b>      | Select all the resources in the table.   |
| <b>Select: None</b>     | Clears the selection for the resources that you have selected.   |
| <b>Refresh</b>          | Refreshes resource information in the table.   |

### Attributes of resources section

| Name         | Description                                       |
|--------------|---|
| <b>Name</b>  | Name of the attribute.                            |
| <b>Value</b> | Value assigned to the attribute for the resource. |

## Resource is member of following groups section

| Name               | Description                                    |
|--------------------|--|
| <b>Name</b>        | Unique name of the group.                      |
| <b>Type</b>        | Group type based on the resources it contains. |
| <b>Hierarchy</b>   | Position of the group in the hierarchy.        |
| <b>Description</b> | A brief description about the group.           |

## Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the upper-right corner of the page.

| Name                       | Description   |
|----------------------------|---|
| <b>Type</b>                | The types based on the resources it contains.   |
| <b>Resource Attributes</b> | <p>Displays the following three fields:</p> <ul style="list-style-type: none"> <li>• Drop-down 1 - The criteria for searching a resource. The options are attributes of resources for the attribute type selected in the <b>Type</b> drop-down list.</li> <li>• Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of attribute selected in the first drop-down list.</li> <li>• Field 3 – The value corresponding to the search criteria.</li> </ul> |

| Button                 | Description  |
|------------------------|--|
| <b>Clear</b>           | Clears the search value that you entered in the third field.       |
| <b>Search</b>          | Searches the resources matching the search conditions.             |
| <b>Close</b>           | Closes the Criteria section.                                       |
| <b>Advanced Search</b> | Cancel the search operation and hides the <b>Criteria</b> section. |

## Related topics:

[Searching for resources based on group membership](#) on page 1170

[Searching for resources based on group membership](#) on page 1170

[Accessing resources](#) on page 1186

[Accessing resources](#) on page 1186

[Assigning resources to a new group](#) on page 1186

[Assigning resources to a new group](#) on page 1186

[Adding resources to a selected group](#) on page 1188

[Adding resources to a selected group](#) on page 1188

## Choose Group field descriptions

Use this page to add resources to the selected groups.

| Name               | Description  |
|--------------------|--|
| <b>Select</b>      | Use this option to select a group.   |
| <b>Name</b>        | Name of the group.   |
| <b>Type</b>        | Group type based on the type of resources. The options are: <ul style="list-style-type: none"> <li>• Groups having members of same resource type.</li> <li>• All — Groups having members of any resource types.</li> </ul>                     |
| <b>Dynamic</b>     | The value indicates whether the group uses a query to determine its members or has static members. True indicates that group membership is not permanent and determined when you run the query and false indicates groups with static members. |
| <b>Description</b> | A brief description about the group.   |

| Button                | Description  |
|-----------------------|--|
| <b>Expand All</b>     | Shows the subgroups of groups listed in the table.                     |
| <b>Collapse All</b>   | Hides the subgroups of all the expanded groups.                        |
| <b>Selected Group</b> | Adds the resource as a member of the selected group.                   |
| <b>Cancel</b>         | Closes the Choose Group page and takes you back to the Resources page. |

## Choose Parent Group field descriptions

Use this page to add resources to a selected group or to a new group.

| Name           | Description  |
|----------------|--|
| <b>Select</b>  | Use this option to select a group.   |
| <b>Name</b>    | Name of the group.   |
| <b>Type</b>    | Group type based on the type of resources. The options are: <ul style="list-style-type: none"> <li>• Groups having members of same resource type.</li> <li>• All — Groups having members of any resource types.</li> </ul> |
| <b>Dynamic</b> | The value indicates whether the group uses a query to determine its members or has static members. True indicates that group membership is not   |

| Name               | Description   |
|--------------------|---|
|                    | permanent and determined when you run the query and false indicates groups with static members. |
| <b>Description</b> | A brief description about the group.  |

| Button                | Description   |
|-----------------------|---|
| <b>Expand All</b>     | Shows the subgroups of groups listed in the table.  |
| <b>Collapse All</b>   | Hides the subgroups of all the expanded groups.   |
| <b>Root</b>           | Opens New Group page. Use this page to create a new group. The selected resource is the member of this group. |
| <b>Selected Group</b> | Adds the resource as a member of the selected group.  |
| <b>Cancel</b>         | Closes the Choose Parent Group page and takes you back to the Resources page.                                 |

---

## Managing roles

---

### Manage Roles

The Manage Roles service provides the management interface for administering roles and permissions. To define a role, you need to grant permissions on groups and resources of a particular resource type. The permissions on resources and groups for a role are the operations that a user assigned to this role can perform. You can perform the following important operations using the service:

- Create a role
- View and Modify roles
- Delete roles
- Create a duplicate group by copying the properties of an existing role
- Import roles from a file
- Search a role

## Types of default roles

Communication System Management has certain default roles. These roles are sets of permissions assigned to groups and resources. Some of the specific roles for Communication System Management are:

### CSM Admin

In this role, you can perform any action within Communication System Management. You have access to all the functions in Communication System Management.

The CM and MM Admin roles are also roles in Communication System Management. As a CM Admin user you have access to all the Communication Manager related tasks. You can perform any action related to the Communication Manager devices, like adding a station, editing a station and so on.

As an MM Admin you have access and permission to all the messaging or mailbox related activities. You cannot perform any CM related task as an MM Admin.

 **Note:**

As a CSM Admin you do not have the permission to access the scheduler.

### CSM Viewer

As a CSM Viewer you can view all the pages or screens in Communication System Management. You cannot perform any operations that require you to add or modify any information such as adding a station or editing a subscriber. You have viewing rights only.

 **Note:**

In the view role only the **View** button in the station and subscriber screens and for non-station objects is available.

---

## Viewing user roles

1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
2. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
3. On the Manage Roles page, select a role and click **View**.

---

### Related topics:

[Assigning users to roles](#) on page 1200

[Removing users from roles](#) on page 1200

[View Role field descriptions](#) on page 1217

---

## Creating a role

Use this functionality to create a role and assign a set of permissions to this role.

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, click **New**.
  3. On the New Role page, enter the name of the role and description of the role in the **Name** and **Description** fields in the Role Details section.
  4. Click **Permission Set > Add** to assign permissions on the resources for a role.
  5. Click **Commit**.
- 

### Related topics:

[Assigning permissions to a role](#) on page 1207

[New Role field descriptions](#) on page 1212

---

## Modifying user roles

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. Perform one of the following steps:
    - On the Manage Roles page, select a role and click **Edit**.
    - On the Manage Roles page, select a role and click **View > Edit**.
  3. On the Edit Role, modify the name of the role and description of the role in the **Name** and **Description** fields in the Role Details section.
  4. Click **Permission Set > Add** to modify the permissions assigned to the role.
  5. Click **Commit**.
- 

### Related topics:

[Assigning permissions to a role](#) on page 1207

[Assigning permissions to a role](#) on page 1207

[Removing permissions from a role](#) on page 1208

[Adding groups and resources to a permission](#) on page 1208

[Removing groups and resources from a permission](#) on page 1209

[Adding attributes to a role](#) on page 1209

[Removing attributes from a permission](#) on page 1210

[Edit Role field descriptions](#) on page 1215

---

## Creating duplicate roles

Use this feature to create a duplicate role by copying the properties of an existing role. When you create a duplicate role, the system copies all the information from the existing role to the duplicate role account.

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, select a role and click **Duplicate**.
  3. Enter the appropriate information.
  4. Click **Commit** to save the changes to the database.

---

### Related topics:

[Assigning permissions to a role](#) on page 1207

[Duplicate Role field descriptions](#) on page 1218

---

## Deleting user roles

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, select a role and click **Delete**.
-

---

## Searching for roles

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, click **Advanced Search** displayed at the upper-right corner of the page.
  3. In the Criteria section, do the following:
    - a. Select the search criterion from the first drop-down field.
    - b. Select the operator from the second drop-down field.
    - c. Enter the search value in the third field.

If you want to add a search condition, click **+** and repeat sub steps a through c listed in step 3.

If you want to delete a search condition, click **-**. This button is available if you have specified more than one search condition.

4. Click **Search**.

---

### Result

The page displays the roles that matches the value specified for the search criteria.

### Related topics:

[Manage Roles field descriptions](#) on page 1211

---

## Filtering roles

You can apply filter on the Role Name column

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, click **Filter: Enable**.  
You can find the button at the upper-right corner of the table displaying roles.
  3. Enter the role name in the field under the **Role Name** column.
  4. Click **Apply**.



**Note:**

To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

---

**Result**

The table displays only those roles that matches the filter criteria.

**Related topics:**

[Manage Roles field descriptions](#) on page 1211

---

## Assigning users to roles

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, select a user role and click **More Actions > Assign Roles to Users**.
  3. On the Assign Users page, select the users displayed in the **Select Users** section.
  4. Click **Commit**.
- 

---

## Removing users from roles

- 
1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
  2. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  3. On the Manage Roles page, select one or more user roles and click **More Actions > UnAssign User Roles**.
  4. On the UnAssign Roles page, select the users displayed in the Select Users section.
  5. Click **Commit**.
-

---

## Bulk importing roles

You can bulk import roles data from an XML file. While bulk importing the roles, you have the options to:

- abort or continue the import process when the import operation encounters first error in the global user settings input file.
- skip importing the roles records that already exist in the database. Use this option when you want to import new roles records and retain the existing users.
- replace all the roles records in the database with the roles records from the imported file.
- update and merge the roles data from the imported file to the existing data in the attributes.
- delete the roles records from the database that matches the records in the input XML file.

See the “XML Schema Definition for bulk importing roles” and “Sample XML for bulk importing roles” sections in the “List of XML Schema Definitions and Sample XMLs for bulk Import” topic for details on the roles imported attributes.

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, click **More Actions > Import Roles**.
  3. On the Import Roles page, enter the file name in the **Select file** field. You can also use the **Browse** button to select a file.
  4. Choose one of the error configuration options:
    - **Abort on first error**
    - **Continue processing other records**
  5. Choose one of the import options:
    - **Skip**
    - **Replace**
    - **Merge**
    - **Delete**
  6. Click **Import**.

---

### Related topics:

[Exporting roles in bulk](#) on page 1202

[Import Roles field descriptions](#) on page 1223

[List of XML Schema Definitions and Sample XMLs for bulk Import](#) on page 1420

---

## Exporting roles in bulk

You can export Roles in bulk from the System Manager database. You can find this utility in the `$MGMT_HOME/rbc/bulkexport/exportutility` directory. `MGMT_HOME` is an environment variable that represents the System Manager HOME path.

1. Go to the command prompt.
2. Change the directory to `$MGMT_HOME/rbc/bulkexport/exportutility`. `MGMT_HOME` is an environment variable that represents the System Manager HOME path.
3. Run the `# sh exportroles.sh [-u] <user> [-p] <password>...[OPTIONS]` command.

Here, `-u` (username) and `-p` (password) are the mandatory parameters. Optional parameters include:

- `-f` file name prefix of the file that you want to export
- `-r` number of records per file
- `-d` location of the file that you want to export
- `-s` start index of record
- `-e` number of records that you want to export
- `-t` job scheduling time (YYYY:MM:DD:HH:MM:SS). If you do not specify this option, the present job runs immediately

You can modify the default values of the optional arguments by changing the `$MGMT_HOME/rbc/bulkexport/exportutility/bulkexportconfig.properties` file, where `MGMT_HOME` is an environment variable that represents the System Manager HOME path.

For example, `# sh exportroles.sh -u <user> -p <password> -f roleExport -r 1000 -s 0 -e 1000.`

Refer the “XML Schema Definition for bulk importing roles” section in the “List of XML Schema Definitions and Sample XMLs for bulk Import” topic for details on the attributes that are available for bulk exporting roles.

While exporting roles records if the number of exported records exceeds the limit of records that an XML file can hold, the system creates multiple XML files. These files are packaged together in a zip file.

The system generates a zip file that contains the exported roles records in an XML file.

---

**Related topics:**

[Bulk importing roles](#) on page 1201

[List of XML Schema Definitions and Sample XMLs for bulk Import](#) on page 1420

---

## Viewing details of role import jobs

- 
1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
  2. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  3. On the Manage Roles page, click **More Actions > Import Roles**.
  4. On the Import Roles page, select one job from the table in the Job List section.
  5. Click **View Job**.

---

**Result**

The Job Detail page displays the details of the page.

**Related topics:**

[Import Roles field descriptions](#) on page 1223

---

## Scheduling a role importing job

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, click **More Actions > Import Roles**.
  3. On the Import Roles page, in the **Select file** field enter the name of the file along with the path.  
You can also use the **Browse** button to select a file.
  4. Choose one of the following error configuration options:
    - **Abort on first error**

- **Continue processing other records**
5. Choose one of the following Import types:
    - **Complete**
    - **Partial**
  6. Choose one of the options if a matching record is found:
    - **Skip**
    - **Merge**
    - **Replace**
    - **Delete**
  7. In the Job Schedule section:
    - a. Click **Schedule Later**.

If you want to run the role importing job immediately, click **Run immediately**.  
Selecting this option makes the scheduling related fields unavailable.
    - b. Enter the date in the **Date** field.

You can use the calendar icon to select a date.
    - c. In the **Time** field, enter time in hours, minutes and second format.
    - d. From the **Time Zone** field, select the time zone.
  8. Click **Import**.

---

## Result

The page displays the scheduled job in the Manage Jobs section.

## Related topics:

[Import Roles field descriptions](#) on page 1223

---

## Viewing a role import job in Scheduler

1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, click **More Actions > Import Roles**.
  3. On the Import Roles page, select a job from the table in the Job List section.
  4. Click the link displayed in the **Scheduled Job** column.
-

## Result

The Scheduler page displays the details of the Job. You can only perform those operations on the job that the Scheduler service supports for the job.

### Related topics:

[Import Roles field descriptions](#) on page 1223

---

## Aborting a role importing job on first error

An importing process may encounter errors at the time of importing roles. Use this feature to abort the importing process on encountering the first error during importing roles from the input file.

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, click **More Actions > Import Roles**.
  3. On the Import Roles page, enter the file name in the **Select file** field. You can also use the **Browse** button to select a file.
  4. Click **Abort on First Error**.
  5. Choose one of the options for **If a matching record already exists:**.
  6. Click **Import**.
- 

### Related topics:

[Import Roles field descriptions](#) on page 1223

---

## Canceling a role import job

### Prerequisites

You can cancel only a job which is in a PENDING EXECUTION or in a RUNNING state

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, click **More Actions > Import Roles**.

3. On the Import Roles page, select a job from the table in the Manage Jobs section.
4. Click **Cancel Job**.

---

**Related topics:**

[Import Roles field descriptions](#) on page 1223

---

## Deleting a role importing job

### Prerequisites

You can delete only those jobs that are successful.

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, click **More Actions > Import Roles**.
  3. On the Import Roles page, select a job from the table in the Manage Jobs section.
  4. Click **Delete Job**.

---

**Related topics:**

[Import Roles field descriptions](#) on page 1223

---

## Downloading error records for an unsuccessful role importing job

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, click **More Actions > Import Roles**.
  3. On the Import Roles page, select one job from the table in the Job List section.
  4. Click **View Job**.
  5. On the Import Roles – Job Detail page, click **Download**.

---

### Result

The system saves the error messages in a file to the specified location.

**Related topics:**

[Import Roles – Job Details field descriptions](#) on page 1225

---

## Assigning permissions to a role

When you create a role, you need to assign permission to this role. Permissions include actions that a user to which you assign the role can perform over the selected groups and resources. The actions that a user can perform over a resource or group varies with the type of resource. You can add more than one permission that may include groups and resources of a different resource type or of same resource type.

1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
2. On the Manage Roles page, perform one of the following roles:
  - Click **New**.
  - Select a role and click **Edit**.
  - Select a role and click **View > Edit**.
3. Click **Permission Set > Add**
4. From the **Resource Type** drop-down field, select a type of resource.
5. From the **Actions** list box, select the actions.  
Use the CTRL and up and down arrow keys to select more than one actions.
6. In the Selected Groups and Resources section, click **Add** to add a group and resources.
7. In the Selected Attributes section, click **Add** to add attributes.
8. Click **Add**.  
You can find the Add button following the label **Permission Set**.

**Note:**

To add another permission over groups and resources of different resource type or of same resource type with different set of resources and groups, repeat the steps from 5 to 9.

---

**Related topics:**

[Removing permissions from a role](#) on page 1208

[Adding groups and resources to a permission](#) on page 1208

[Removing groups and resources from a permission](#) on page 1209

[Adding attributes to a role](#) on page 1209

[Removing attributes from a permission](#) on page 1210

[New Role field descriptions](#) on page 1212

[Edit Role field descriptions](#) on page 1215

[Duplicate Role field descriptions](#) on page 1218

---

## Removing permissions from a role

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, perform one of the following roles:
    - Select a role and click **Edit**.
    - Select a role and click **View > Edit**.
  3. Click **Permission Set**.
  4. In the Permission Detail section, select the permission and click **Delete**.
- 

---

## Adding groups and resources to a permission

Use this functionality to specify the groups and resources over which you want to apply the permission. You may choose to apply the permission over all or selected groups and resources.

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, perform one of the following roles:
    - Click **New**.
    - Select a role and click **Duplicate**.
    - Select a role and click **Edit**.
    - Select a role and click **View > Edit**.
  3. Click **Permission Set > Add**.
  4. In the Selected Groups and Resources section, perform one of the following steps:

To apply a permission on all the groups and resources that exists under the specified Resource Type, click **All**

To apply a permission on the chosen groups and resources that exists under the specified Resource Type:

- i. click **Select**.
- ii. click **Add**
- iii. On the Select Groups and Resources page, select group and resources and click **Save**.

---

**Related topics:**

[Select Groups and Resources field descriptions](#) on page 1221

[Select Groups and Resources field descriptions](#) on page 1221

---

## Removing groups and resources from a permission

1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
2. On the Manage Roles page, perform one of the following roles:

**Note:**

If you are on the New Role page and have already added a group and/or resource, then proceed to step 4.

- Select a resource and click **Duplicate**.
  - Select a resource and click **Edit**.
  - Select a resource and click **View > Edit**.
3. Click **Permission Set**.
  4. In the Selected Groups and Resources section, select the resources and groups that you want to remove from the permission and click **Delete**.

---

## Adding attributes to a role

Use this feature to add attributes over which you want to apply the permissions. Each resource type has a set of attributes associated with it. All the groups and resources of a resource type inherit the attributes that are defined for that resource type. If you do not specify any attribute, the table in the Selected Attributes section displays none.

 **Note:**

Permission to an attribute works only when there is minimum one group or resource added to the role.

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, perform one of the following steps:
    - Click **New**.
    - Select a role and click **Edit**.
    - Select a role and click **View > Edit**.
  3. Click **Permission Set > Add**.
  4. In the Selected Attributes section, perform one of the following steps:
    - To apply permission over all the attributes that exists under the specified Resource Type, click **All**
    - To apply permission over the selected attributes that exists under the specified Resource Type:
      - i. click **Select**.
      - ii. click **Add**
      - iii. On the Select Attributes page, select attributes and click **Save**.

---

**Related topics:**

[Select Attributes field descriptions](#) on page 1222

---

## Removing attributes from a permission

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, perform one of the following roles:

 **Note:**

If you are on the New Role page and have already added an attribute, proceed to step 4.

- Select a role and click **Edit**.

- Select a role and click **View > Edit**.
3. Click **Permission Set**.
  4. In the Selected Attributes section, select the attributes that you want to remove from the permission and click **Delete**.

---

## Manage Roles field descriptions

Use this page to:

- Add, modify, view and delete roles.
- Assign roles to or remove roles from an existing user.
- Import roles from a file.

| Name                 | Description                         |
|----------------------|-------------------------------------|
| <b>Role name</b>     | Name of the role.                   |
| <b>Resource Type</b> | The type based on the resources.    |
| <b>Role Type</b>     | Type of the role.                   |
| <b>Description</b>   | Insert a description of this field. |

| Button                                       | Description   |
|--|---|
| <b>View</b>                                  | Opens the View Role page that displays the details of the selected role.                        |
| <b>Edit</b>                                  | Opens the Edit Role page that you can use to modify the selected role.                          |
| <b>New</b>                                   | Opens the New Role page that you can use to add a new role and assign permissions to the roles. |
| <b>Duplicate</b>                             | Opens the Duplicate Role page to create a duplicate role.                                       |
| <b>Delete</b>                                | Deletes a selected role.  |
| <b>More Actions &gt; Assign User Roles</b>   | Opens the Assign Users page that you can use to assign roles to the user.                       |
| <b>More Actions &gt; UnAssign User Roles</b> | Opens the UnAssign Users page that you can use to unassign roles for a user.                    |
| <b>More Actions &gt; Import Roles</b>        | Opens the Import Roles page that you can use to import roles from a file.                       |
| <b>Advanced Search</b>                       | Displays fields that you can use to specify the search criteria for searching a role.           |

| Button                 | Description  |
|------------------------|--|
| <b>Filter: Enable</b>  | Displays fields under select columns that you can use to set filter criteria. This is a toggle button. |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.         |
| <b>Filter: Apply</b>   | Filters roles based on the filter criteria.  |
| <b>Select: All</b>     | Selects all the roles in the table.  |
| <b>Select: None</b>    | Clears all the check box selections.   |
| <b>Refresh</b>         | Refreshes the role's information in the table.   |

### Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the upper-right corner of the page

| Name            | Description  |
|-----------------|--|
| <b>Criteria</b> | <p>Displays the following three fields:</p> <ul style="list-style-type: none"> <li>• Drop-down 1 - The list of criteria that you can use to search roles.</li> <li>• Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field.</li> <li>• Field 3 – The value for the search criterion. The Roles Management service retrieves and displays roles that match this value.</li> </ul> |

### Related topics:

- [Viewing user roles](#) on page 1196
- [Creating a role](#) on page 1197
- [Modifying user roles](#) on page 1197
- [Creating duplicate roles](#) on page 1198
- [Deleting user roles](#) on page 1198
- [Searching for roles](#) on page 1199
- [Filtering roles](#) on page 1199
- [Assigning users to roles](#) on page 1200
- [Removing users from roles](#) on page 1200
- [Bulk importing roles](#) on page 1201

---

## New Role field descriptions

Use this page to create a new role and assign permissions to the role. The page has two sections:

- Role Details
- Permission Set

### Role Details section

| Name               | Description                      |
|--------------------|----------------------------------|
| <b>Name</b>        | Name of the role.                |
| <b>Description</b> | A brief description of the role. |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Creates a new role.  |
| <b>Cancel</b> | Closes the New Role page and returns to the Manage Roles page. |

### Permission Set section

| Name                        | Description  |
|-----------------------------|--|
| <b>Select option button</b> | Use this button to select a permission over groups and resources.  |
| <b>Resource Type</b>        | The type based on the resources. The table displays group and resources for the resource type that you specified in the <b>Resource Type</b> drop-down field in the Permission Detail section. |
| <b>Actions</b>              | Actions that you can perform over the specified groups and resources.  |
| <b>Groups and Resources</b> | Groups and resources added to this permission.   |
| <b>Attributes</b>           | Attributes assigned to this permission.  |

| Button        | Description                                  |
|---------------|--|
| <b>Add</b>    | Adds a permission to the role.               |
| <b>Delete</b> | Deletes a selected permission from the role. |

### Permission Detail

| Name                 | Description  |
|----------------------|--|
| <b>Resource Type</b> | The type based on the resources.                                 |
| <b>Actions</b>       | Permissions that can be set for the corresponding resource type. |

### Selected Groups and Resources

| Name                    | Description                                     |
|-------------------------|---|
| <b>Select check box</b> | Use the check box to select group and resource. |

| Name                        | Description                             |
|-----------------------------|---|
| <b>Resource Name</b>        | The name of the resource.               |
| <b>Resource Type</b>        | The type based on the resources.        |
| <b>Resource Description</b> | A brief description about the resource. |

| Button              | Description  |
|---------------------|--|
| <b>Add</b>          | Opens the Select Groups and Resources page that you can use to select and add groups and resources to the permission. The user to which you assign this role can perform the operations specified in the <b>Actions</b> list box over the selected groups and resources. |
| <b>Delete</b>       | Removes the selected groups and/or resources from the permission.  |
| <b>All</b>          | Use this option button to apply permissions over all groups and resources for the specified resource type.   |
| <b>Select</b>       | Use this option button to apply permissions over the selected groups and resources for the specified resource type.  |
| <b>Select: All</b>  | Selects all the groups and roles in the table.   |
| <b>Select: None</b> | Clears all the check box selections.   |

### Selected Attributes

| Name        | Description           |
|-------------|-----------------------|
| <b>Name</b> | Name of the Attribute |

| Button              | Description  |
|---------------------|--|
| <b>Add</b>          | Opens the Select Attributes page that you can use to select an attribute.                                      |
| <b>Delete</b>       | Removes the selected groups and resources.   |
| <b>All</b>          | Use this option button to apply permissions over all the attributes of the specified group and resources.      |
| <b>Select</b>       | Use this option button to apply permissions over the selected attributes of the specified group and resources. |
| <b>Select: All</b>  | Selects all the attributes in the table.   |
| <b>Select: None</b> | Clears the check box selections.   |

### Related topics:

[Creating a role](#) on page 1197

## Edit Role field descriptions

Use this page to edit a role.

### Role Details section

| Name               | Description                      |
|--------------------|----------------------------------|
| <b>Name</b>        | Name of the role.                |
| <b>Description</b> | A brief description of the role. |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Creates a new role.   |
| <b>Cancel</b> | Cancels the role modifying operation and returns you to the to the Manage Roles page. |

### Permission Set section

| Name                        | Description  |
|-----------------------------|--|
| <b>Select option button</b> | Use this button to select a permission over groups and resources.  |
| <b>Resource Type</b>        | The type based on the resources. The table displays group and resources for the resource type that you specified in the <b>Resource Type</b> drop-down field in the Permission Detail section. |
| <b>Actions</b>              | Actions that you can perform over the specified groups and resources.  |
| <b>Groups and Resources</b> | Groups and resources added to this permission.   |
| <b>Attributes</b>           | Attributes assigned to this permission.  |

| Button        | Description                                  |
|---------------|--|
| <b>Add</b>    | Adds a permission to the role.               |
| <b>Delete</b> | Deletes a selected permission from the role. |

### Permission Detail

| Name                 | Description  |
|----------------------|--|
| <b>Resource Type</b> | The type based on the resources.                                 |
| <b>Actions</b>       | Permissions that can be set for the corresponding resource type. |

### Selected Groups and Resources

| Name                        | Description                                     |
|-----------------------------|---|
| <b>Select check box</b>     | Use the check box to select group and resource. |
| <b>Resource Name</b>        | The name of the resource.                       |
| <b>Resource Type</b>        | The type based on the resources.                |
| <b>Resource Description</b> | A brief description about the resource.         |

| Button              | Description  |
|---------------------|--|
| <b>Add</b>          | Opens the Select Groups and Resources page that you can use to select and add groups and resources to the permission. The user to which you assign this role can perform the operations specified in the <b>Actions</b> list box over the selected groups and resources. |
| <b>Delete</b>       | Removes the selected groups and/or resources from the permission.  |
| <b>All</b>          | Use this option button to apply permissions over all groups and resources for the specified resource type.   |
| <b>Select</b>       | Use this option button to apply permissions over the selected groups and resources for the specified resource type.  |
| <b>Select: All</b>  | Selects all the groups and roles in the table.   |
| <b>Select: None</b> | Clears all the check box selections.   |

### Selected Attributes

| Name        | Description           |
|-------------|-----------------------|
| <b>Name</b> | Name of the attribute |

| Button              | Description  |
|---------------------|--|
| <b>Add</b>          | Opens the Select Attributes page that you can use to select an attribute.                                      |
| <b>Delete</b>       | Removes the selected attributes.   |
| <b>All</b>          | Use this option button to apply permissions over all the attributes of the specified group and resources.      |
| <b>Select</b>       | Use this option button to apply permissions over the selected attributes of the specified group and resources. |
| <b>Select: All</b>  | Selects all the attributes in the table.   |
| <b>Select: None</b> | Clears the check box selections.   |

#### Related topics:

[Modifying user roles](#) on page 1197

## View Role field descriptions

Use this page to view the details of a selected role.

### Role Details section

| Name               | Description                      |
|--------------------|----------------------------------|
| <b>Name</b>        | Name of the role.                |
| <b>Description</b> | A brief description of the role. |

| Button        | Description   |
|---------------|---|
| <b>Edit</b>   | Opens the Edit Role page. Use the page to edit a selected role.     |
| <b>Cancel</b> | Closes the View Role page and returns you to the Manage Roles page. |

### Permission Set section

| Name                        | Description  |
|-----------------------------|--|
| <b>Resource Type</b>        | The type based on the resources. The table displays group and resources for the resource type that you specified in the <b>Resource Type</b> drop-down field in the Permission Detail section. |
| <b>Actions</b>              | Actions that you can perform over the specified groups and resources.  |
| <b>Groups and Resources</b> | Groups and resources added to this permission.   |
| <b>Attributes</b>           | Attributes assigned to this permission.  |

| Button         | Description                             |
|----------------|---|
| <b>Refresh</b> | Refreshes the permission's information. |

### User Assignment

| Name              | Description   |
|-------------------|---|
| <b>Status</b>     | The current login status of the user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status. |
| <b>Name</b>       | Name of the user.   |
| <b>Login Name</b> | The unique system login name given to the user. It takes the form of username@domain.   |
| <b>User Name</b>  | Unique name by which the system identifies the user.  |

| Name                | Description   |
|---------------------|---|
| <b>Phone Number</b> | Contact number of the user.                                 |
| <b>Last Login</b>   | Date and time when the user has last logged into the system |
| <b>User Type</b>    | The role of the user.                                       |

| Button         | Description                       |
|----------------|-----------------------------------|
| <b>Refresh</b> | Refreshes the user's information. |

**Related topics:**

[Viewing user roles](#) on page 1196

## Duplicate Role field descriptions

Use this page to create a duplicate role and assign permissions to the role. The page has two sections:

- Role Details
- Permission Set

### Role Details section

| Name               | Description                      |
|--------------------|----------------------------------|
| <b>Name</b>        | Name of the role.                |
| <b>Description</b> | A brief description of the role. |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Creates a duplicate role.                                      |
| <b>Cancel</b> | Closes the New Role page and returns to the Manage Roles page. |

### Permission Set section

| Name                        | Description                                    |
|-----------------------------|--|
| <b>Select option button</b> | Click this button to select a permission.      |
| <b>Resource Type</b>        | The type based on the resources.               |
| <b>Actions</b>              | Permissions available for the resource type.   |
| <b>Groups and Resources</b> | Groups and resources added to this permission. |
| <b>Attributes</b>           | Attributes assigned to this permission.        |

## Permission Detail

| Name                 | Description   |
|----------------------|---|
| <b>Resource Type</b> | The type based on the resources.                      |
| <b>Actions</b>       | Permissions that are available for the resource type. |

| Button        | Description                    |
|---------------|--------------------------------|
| <b>Add</b>    | Adds a permission to the role. |
| <b>Delete</b> | Deletes a selected permission. |

## Selected Groups and Resources

| Name                        | Description                                     |
|-----------------------------|---|
| <b>Select check box</b>     | Use the check box to select group and resource. |
| <b>Resource Name</b>        | The name of the resource.                       |
| <b>Resource Type</b>        | The type based on the resources.                |
| <b>Resource Description</b> | A brief description about the resource.         |

| Button              | Description   |
|---------------------|---|
| <b>Add</b>          | Opens the Select Groups and Resources page that you can use to select and add a group and resource to the permission. |
| <b>Delete</b>       | Removes the selected groups and/or resources.   |
| <b>Select: All</b>  | Selects all the groups and roles in the table.  |
| <b>Select: None</b> | Clears the selections.  |

## Selected Attributes

| Name        | Description           |
|-------------|-----------------------|
| <b>Name</b> | Name of the Attribute |

| Button              | Description   |
|---------------------|---|
| <b>Add</b>          | Opens the Select Attributes page that you can use to select an attribute. |
| <b>Delete</b>       | Removes the selected groups and/or resources.                             |
| <b>Select: All</b>  | Selects all the groups and roles in the table.                            |
| <b>Select: None</b> | Clears the selections.  |

| Button        | Description                    |
|---------------|--------------------------------|
| <b>Add</b>    | Adds a permission to the role. |
| <b>Delete</b> | Deletes a selected permission. |

**Related topics:**

[Creating duplicate roles](#) on page 1198

## Assign Users To Roles field descriptions

Use this page to assign one or more users to the selected roles. The page has two sections:

- Selected Roles
- Select Users

### Selected Roles section

The roles to which you can assign users.

| Name                 | Description  |
|----------------------|--|
| <b>Name</b>          | Name of the role.  |
| <b>Resource Type</b> | The resource type that the corresponding role is assigned. |
| <b>Description</b>   | A brief description about role.                            |

### Select Users section

The table displays the users to which you can assign the roles.

| Name                    | Description   |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select the user.  |
| <b>Status</b>           | Displays whether the user is currently online or offline. The online status indicates that the user is logged into the application and offline status indicates that the user is logged out of the application. |
| <b>User Name</b>        | The unique name that identifies the user  |
| <b>Last Login</b>       | Time and date when the user has last logged into the system.  |
| <b>User Type</b>        | The type that defines the role of the user.   |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Assigns user to the role.  |
| <b>Cancel</b> | Cancels the assign users operation and returns to the Manage Roles page. |

---

## UnAssign Roles field descriptions

Use this page to unassign a role from the selected users. The page has two sections:

- Selected Roles
- Select Users

### Selected Roles section

The role from which users are unassigned.

| Name                 | Description  |
|----------------------|--|
| <b>Name</b>          | Name of the role.  |
| <b>Resource Type</b> | The resource type that the corresponding role is assigned. |
| <b>Description</b>   | A brief description about the role.                        |

### Select Users section

The table displays the users for which you can remove the roles.

| Name                    | Description   |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select the user.  |
| <b>Status</b>           | Displays whether the user is currently online or offline. The online status indicates that the user is logged into the application and offline status indicates that the user is logged out of the application. |
| <b>User Name</b>        | The unique name that identifies the user  |
| <b>Last Login</b>       | Time and date when the user has last logged into the system.  |
| <b>User Type</b>        | The type that defines the role of the user.   |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Unassigns the role from the users.                                      |
| <b>Cancel</b> | Cancel the assign users operation and returns to the Manage Roles page. |

---

## Select Groups and Resources field descriptions

Use this page to add groups and resources to a role.

| Name                    | Description  |
|-------------------------|--|
| <b>Select check box</b> | Use this check box to select groups and resources. |

| Name               | Description  |
|--------------------|--|
| <b>Name</b>        | Name of the group and resource   |
| <b>Type</b>        | Type of a group and resource. If it is a resource then type is based on the resources it contains. If it is a group then type is based on a group with members belonging to a same resource type or group with no restrictions on the type of members. |
| <b>Description</b> | A brief description about a group or resource.   |

| Button                 | Description  |
|------------------------|--|
| <b>Save</b>            | Adds the selected resources and groups to the permission.  |
| <b>Cancel</b>          | Closes the page and returns to the New Role page.  |
| <b>Filter: Enable</b>  | Displays fields under select columns that you can use to set filter criteria. This is a toggle button. |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.         |
| <b>Filter: Apply</b>   | Filters roles based on the filter criteria.  |
| <b>Select: All</b>     | Select all the groups and roles in the table.  |
| <b>Select: None</b>    | Clears the selections.   |

**Related topics:**

[Adding groups and resources to a permission](#) on page 1208

[Adding groups and resources to a permission](#) on page 1208

## Select Attributes field descriptions

Use this page to select and apply attributes to the selected role.

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use this check box to select the attribute. Use the check box displayed as one of the column header to select all the attributes in the table. |
| <b>Name</b>             | Name of the attribute.   |

| Button              | Description  |
|---------------------|--|
| <b>Save</b>         | Adds the selected attributes to the permission.  |
| <b>Cancel</b>       | Cancels the select attributes operations and takes you back to the New Role or Edit Role page. |
| <b>Select: All</b>  | Select all the attributes in the table.  |
| <b>Select: None</b> | Clears all the check box selections.   |

**Related topics:**

[Adding attributes to a role](#) on page 1209

---

## Import Roles field descriptions

Use this page to bulk import roles from a selected file.

**File Selection**

| Name               | Description  |
|--------------------|--|
| <b>Select File</b> | The path and name of the XML file from which you want to import the roles. |

| Button        | Description   |
|---------------|---|
| <b>Browse</b> | Opens a dialog box that you can use to select the file from which you want to import the roles. |

**General**

| Name                                       | Description   |
|--|---|
| <b>Select Error Configuration</b>          | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Abort on First Error:</b> Aborts importing the role records when the import roles operation encounters the first error in the import file containing role records.</li> <li>• <b>Continue Processing other records:</b> Imports the next role record if the import role operation encounters an error while importing a user record.</li> </ul>   |
| <b>If a matching record already exists</b> | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Skip:</b> Skips a matching role record that already exists in the system during an import operation. Currently, using this option you can add a new permission to a permission set but you cannot update an existing permission in a permission set.</li> <li>• <b>Replace:</b> Re-imports or replaces all the data for a role. This is essentially the ability to replace a role along with the other data related to the role.</li> <li>• <b>Merge:</b> Imports the role data at an even greater degree of granularity. Using this option you can simultaneously perform both add and update operation of roles. For example, you can add permissions to the permission list and update a role name.</li> <li>• <b>Delete:</b> Deletes the roles records from the database that matches the records in the input XML file.</li> </ul> |

## Job Schedule

| Name                | Description  |
|---------------------|--|
| <b>Schedule Job</b> | The options for configuring the schedule of the job: <ul style="list-style-type: none"> <li>• Run immediately: Use this option if you want to run the import job immediately.</li> <li>• Schedule later: Use this option to run the job at the specified date and time.</li> </ul> |
| <b>Date</b>         | Date when you want to run the import roles job. The date format is mm dd yyyy. You can use the calendar icon to choose a date. This field is available when you select the <b>Schedule later</b> option for scheduling a job.  |
| <b>Time</b>         | Time of running the import roles job. This field is available when you select the <b>Schedule later</b> option for scheduling a job.   |
| <b>Time Zone</b>    | Time zone of your region. This field is available when you select the <b>Schedule later</b> option for scheduling a job.   |

| Button        | Description                               |
|---------------|---|
| <b>Import</b> | Imports the roles from the selected file. |

## Manage Jobs

| Name                  | Description  |
|-----------------------|--|
| <b>Check box</b>      | Use this check box to select a job.  |
| <b>Scheduled Time</b> | The date and time when the job was scheduled.  |
| <b>Status</b>         | The current status of the job. The following are the different status of the job: <ol style="list-style-type: none"> <li>1. PENDING EXECUTION: The job is in queue.</li> <li>2. RUNNING: The job execution is in progress.</li> <li>3. SUCCESSFUL: The job execution is completed.</li> <li>4. INTERRUPTED: The job execution is cancelled.</li> <li>5. FAILED: The job execution has failed.</li> </ol> |
| <b>Job Name</b>       | A link to the Scheduler user interface. You can cancel the job from the Scheduler user interface too.  |
| <b>% Complete</b>     | The job completion status in percentage.   |
| <b>Role Records</b>   | The total role records in the input file.  |
| <b>Error</b>          | Number of role records in the input file that failed to import.  |

| Button              | Description  |
|---------------------|--|
| <b>View Job</b>     | Shows the details of the selected job.   |
| <b>Delete Job</b>   | Deletes the selected job.  |
| <b>Refresh</b>      | Refreshes the job information in the table.  |
| <b>Show</b>         | Provides you an option to view all the jobs on the same page. If the table displaying scheduled jobs are spanning multiple pages, select <b>All</b> to view all the jobs on a single page. |
| <b>Select: All</b>  | Selects all the jobs in the table.   |
| <b>Select: None</b> | Clears the check box selections.   |
| <b>Previous</b>     | Displays jobs in the previous page.  |
| <b>Next</b>         | Displays jobs in the next page.  |
| <b>Cancel</b>       | Takes you back to the <b>Manage Roles</b> page.  |

**Related topics:**

[Bulk importing roles](#) on page 1201

[Viewing details of role import jobs](#) on page 1203

[Scheduling a role importing job](#) on page 1203

[Viewing a role import job in Scheduler](#) on page 1204

[Aborting a role importing job on first error](#) on page 1205

[Canceling a role import job](#) on page 1205

[Deleting a role importing job](#) on page 1206

---

## Import Roles – Job Details field descriptions

The Import Roles-Job Details page displays the details of the selected Job.

| Name             | Description   |
|------------------|---|
| <b>Start</b>     | Start date and time of the job.   |
| <b>End</b>       | End date and time of the job.   |
| <b>Status</b>    | Status of the job.  |
| <b>File</b>      | Name of the file that is used to import the roles.                            |
| <b>Count</b>     | Total number of roles in the input file.                                      |
| <b>Success</b>   | Total number of roles that are successfully imported.                         |
| <b>Fail</b>      | Total number of roles that failed to import.                                  |
| <b>Message</b>   | The message that indicates whether the roles import is successful or failure. |
| <b>Completed</b> | Displays the percentage completion of the import.                             |

| Name                 | Description                                       |
|----------------------|---|
| <b>Record Number</b> | Role Record in the file where the error occurred. |
| <b>Role Name</b>     | The role name that is getting imported.           |
| <b>Error Message</b> | A brief description of the error.                 |

| Button          | Description   |
|-----------------|---|
| <b>Download</b> | Exports and saves the role import error records in an XML file to the specified destination.<br><br> <b>Note:</b><br>This button is not available if there are no error records for role Import Jobs or if the import job type is set to <b>Abort On First Error</b> . |
| <b>Cancel</b>   | Takes you back to the Import Roles page.  |

**Related topics:**

[Downloading error records for an unsuccessful role importing job](#) on page 1206

# Chapter 10: Managing network routing policies

---

## Managing Session Manager routing

---

### Overview of Session Manager routing

This section details the procedures that are required to set up Session Manager enterprise routing. To complete the administrative procedures, you must use the Routing selection from the System Manager Common Console navigation pane.

Once the initial setup is completed, administrators can use the same screens and procedures for administering and modifying the various routing entities as well as Session Manager instances.

The primary task of Session Manager is to route session creation requests from one server to another based on the address specified in the session creation request.

The addresses which are specified to identify the ultimate destination of a session creation request are in the form of a SIP Uniform Resource Identifier (URI). It consists mainly of a user part and a domain part. Session Manager uses both parts in its routing decisions in the following manner:

- The domain part is normally a DNS domain.
- The user part is an alphanumeric string (or handle). Session Manager has special rules for efficiently routing and manipulating handles which consist entirely of digits (for example, telephone numbers).

The servers which send their session creation requests to the Session Manager are called SIP entities. Session Manager routes these requests to other SIP entities based on the routing rules you have administered.

Session Manager associates SIP entities with specific locations and can make different routing decisions based upon the location from which a session creation request arrives.

---

## Prerequisites for Routing Setup

This section assumes that the following requirements are met:

- The System Manager server is installed.
- All Session Manager instances are installed.

Refer to the section Session Manager installation for details.

---

## Routing

### Routing

Routing tells the system which SIP Entity should receive a call that matches the configured dial pattern or regular expression. Administrators can use Routing to administer Session Manager instances and related routing policies. The configuration data is distributed from the Routing database to each remote Session Manager instance.

All calls originate from a SIP Entity. Routing policies describe how a call is routed when it comes from a particular location associated with the SIP entity and a distinct pattern is dialed (or a regular expression is given) during a particular time range with a distinct ranking/cost for the route to another SIP Entity.

Locations are used for origination-based routing and specifying bandwidth for call admission control.

Routing and Session Manager allow administrators to define routing:

- by combining several locations
- by combining several dial patterns and domains
- for several ToD and rankings
- for a single routing destination

### Routing of a call using routing policy data

1. It tries to match the domain to one of the authoritative domains.
2. If Session Manager is authoritative for the domain, then it tries to match the digit pattern.

3. If Session Manager is not authoritative for the domain or if a digit pattern match is not found, it tries to use the regular expression table.
4. If no regular expression match is found, it sends the request to a Session Manager-provisioned outbound proxy.
5. If no outbound proxy has been administered for the Session Manager and it is not authoritative for the domain, then it uses DNS or the Local Host Name Resolution table to determine where to route the request.
6. If the hostname cannot be resolved to an IP address then the call fails.

## Administering initial setup of the Session Manager

Once you have completed the initial setup as a part of ongoing administration, you can modify the created entities or delete them as required.

The recommended order for the initial set up of the Session Manager using the System Manager Routing screens is as follows.

- 
1. Accept or change default settings.
  2. Create domains.
  3. Create locations.
  4. Create adaptations.
  5. Create SIP entities, some of which are routing destinations:
    - Create other SIP entities.
    - Assign locations and adaptations to the SIP entities.
  6. Create entity links:
    - Between Session Managers.
    - Between Session Managers and other SIP entities.
  7. Create time ranges.
  8. Create routing policies.
  9. Create dial patterns and assign them to routing policies and locations.
  10. Create regular expressions and assign them to routing policies.
  11. Create Session Manager instances using the Session Manager menus on the System Manager navigation pane.
-

## Routing import and export Overview

### Overview of exporting and importing routing element data

The Routing screens allow administering of the Avaya Aura Session Manager SIP routing rules. The management screens consist of nine configurable elements that relate to each other in various ways.

It is possible to populate a very large number of the above elements in System Manager by using XML files. It is also possible to export each of the elements or the entire routing configuration to XML files.

#### PRE-REQUISITES:

- Ensure that System Manager is installed and the server is running.
- Ensure that the user performing the bulk import operation has administrative privileges.
- Before you import a large amount of data, it is highly recommended that you backup the System Manager database. This backup will provide an easy way to restore the original database in case you find that the information you imported is substantially incorrect. Refer to the document Administering Avaya Aura™ System Manager for details about this operation.
- Importing a very large number of elements (thousands and above) can take a very long time and can be CPU intensive to the System Manager server. This information will also need to be synchronized with all the Session Managers. It is highly recommended that you perform large imports at a time where there is reduced platform activity in the network (for example at night or during a maintenance window).

#### FEATURES:

System Manager Routing Import/Export supports:

- Routing related data:
  - Domains
  - Locations
  - Adaptations
  - SIP Entities
  - Entity Links
  - Time Ranges
  - Routing Policies
  - Dial Patterns
  - Regular Expressions
- Each element can be imported separately as a single XML file containing many entries.

- It is possible to compress the XMLs using ZIP compression in order to decrease the size of the files that need to be uploaded to the System Manager server. Note that this is especially important when importing large files of size exceeding 10 MB or more.
- Several or all the elements can be imported in a single ZIP file containing many XML files.
- It is possible to export a single type of entity or all the entities. When exporting all the entities, the exported files are contained in a single ZIP file.
- It is important to note that the Routing elements depend on each other (see specific elements details in this guide). An import operation will fail if the needed elements do not already exist in the database or exist in the same import operation. For example: Import of a Dial Pattern with domain name avaya.com will fail if there is no such domain in the database, or if an XML file containing this domain is not imported in the same import operation as the Dial Pattern.
- When importing several entities together (either as a list of XML/ZIP files or inside a single ZIP file), the System Manager will import them in the correct order to maintain dependencies. Because of this, it is possible, for example, to import SIP Entities and Entity Links pointing to these SIP Entities in the same import operation. The import order is always:
  - a. Domains
  - b. Locations
  - c. Adaptations
  - d. SIP Entities
  - e. Entity Links
  - f. Time Ranges
  - g. Routing Policies
  - h. Dial Patterns
  - i. Regular Expressions

The order is decided by analyzing the files internal structure (it must be a well formed XML as described in this guide). Any file name can be used as long as its extension is “xml”.

- The Import operation does not halt if one of the elements fails validation. The failed element will not be added to the database, and the operation will continue to the next one.
- An audit log provides details on the failed and successful import operations.
- If an imported element already exists in the System Manager database, which means that there is an element with the same unique identifiers, then the values in the new element will overwrite the old element.
  - For example: if a domain named “avaya.com” already exist in the database, then the note, type and default values will be overwritten by the new element.

- Dial Pattern is an exception for this rule. It is not possible to import a dial pattern with elements such as <digitpattern>, <maxdigits>, <mindigits>, <sipdomainName> and <routingoriginName> already present in the database. Such an attempt will fail.
- Every operation in the Routing application is logged to an audit log including the import operation. A log entry is added for each element that is imported, even if the operation succeeds or fails. The log is located at the following file: `/var/log/Avaya/mgmt/nrp/nrpaudit.log`. The file is accessible through the System Manager Linux Shell.

 **Note:**

The Routing elements depend on each other. An import operation will fail if the needed elements do not already exist in the database or exist in the same import operation. For example import of a Dial Pattern with domain name `avaya.com` will fail if there is no such domain in the database, or if an XML file containing this domain is not imported in the same import operation as the Dial Pattern.

## Exporting Routing element data

---

1. On the System Manager console, select **Routing** > **<Any Routing element>**.
2. From the Routing Entity screen, click **More Actions** > **Export <Routing Element>**.  
For example, to export adaptations, select **Routing** > **Adaptations**. From the Adaptations screen, select **More Actions** > **Export Adaptations**.  
To export regular expressions, select **Routing** > **Regular Expressions**. From the Regular Expressions screen, click **More Actions** > **Export Regular Expressions**.
3. Select a check box for the entity to be exported from the list of entities on the screen.
4. To export multiple routing elements, from the routing element screen, click **More Actions** > **Export all data**.
5. Click **Browse** to specify the location and click **Export**.  
You must export a file in the XML format or multiple files as a zipped file.

## Importing Routing element data

---

1. On the System Manager console, select **Routing** > **<Any Routing element>**.
2. To import a single or multiple routing elements, click **More Actions** > **Import**.  
For example, to import dial patterns, select **Routing** > **Dial Patterns**. From the Dial Patterns screen, click **More Actions** > **Import**.
3. Click **Browse** to select files from the required location and click **Import**.  
You must import a file in the XML format. This file can be an XML file or a ZIP file consisting one or more XML files.

 **Note:**

- You cannot import data from the later stages in the routing definition process without importing data from the earlier stages (e.g. one must import SIP Entities before or in conjunction with the relevant Entity Links).
- The import operation can accept any routing element XMLs (e.g. you can import “Locations” even if you clicked on import from the “Domains” screen).
- The XML files that are created with the “export” operation contains version information as shown below:

```
<buildNumber>0</buildNumber>  
<implementationVersion>0</implementationVersion>  
<specificationVersion>0</specificationVersion>
```

---

## Saving, Committing, and Synchronizing configuration changes

Session Manager allows you to save the domain data to the System Manager database and distribute the changes to all the Session Manager instances.

To save the data to System Manager and distribute it to the Session Managers, click **Commit**.

When you click **Commit**, System Manager saves the data to the System Manager database. System Manager synchronizes and distributes the data to all the Session Manager instances. For example, renaming an adaptation also changes that data on the SIP Entities Details screen, or changing dial pattern data also changes that data in the routing policy where that dial pattern is used.

## Duplicating Routing entity data

You can use the **Duplicate** button on the relevant Session Manager Routing screens to duplicate routing entities. Select the check box for the relevant entity and click **Duplicate**. Duplication of data is useful if you want to create entities that are similar and want to rename them or copy an entity and make minimal changes to the entity attributes.

For example, to use a routing policy and to add a dial pattern to the copied routing policy, you can duplicate the routing policy and then add the required dial pattern to it.

---

## Domains

### About Domains

The Domains screen is used to create a set of domains and sub-domains to enable the Session Manager enterprise to use domain-based routing. This information is used to determine if a

SIP user is part of the SIP network. Domains determine if the Session Manager's dial plan can be used to route a particular call. Sub-domains are automatically checked if not provisioned. For example, Session Manager needs to check dial patterns for avaya.com if a request to 123@myserver.avaya.com comes in and myserver.avaya.com is not administered as a domain.

The administrator can create a SIP domain and sub-domains based on the corporate requirement.

- Domain name can be <organization-name.domain>, for example, avaya.com or abc.org.
- Sub-domain can be named based on the geographical location or any other corporate requirements such as office location, for example, us.avaya.com and fr.avaya.com can be sub-domains for Avaya offices in the US and in France, or dr.avaya.com and br.avaya.com can be sub-domains for Avaya offices in Denver and in Basking Ridge.

## Creating domains

Create a domain or set of domains if you plan to use domain-based routing.

- 
1. On the System Manager console, select **Routing > Domains**.
  2. Click **New**.
  3. Enter the domain name and notes for the new domain or sub-domain.
  4. Select "sip" as the domain type from the drop-down list.
  5. Click **Commit**.
- 

## Modifying domains

You can also edit or delete the domains using the **domains** option. The Domains screen is displayed.

- 
1. On the System Manager console, select **Routing > Domains**.
  2. To edit information for existing domains or sub-domains, select the check boxes for the domains that you want to edit and click **Edit**.
  3. Make changes to the domain data as required.

4. To copy existing domain data to a new domain, select the domain and click **Duplicate**. You can edit the duplicate domain name as required.
  5. Click **Commit**.
- 

## Deleting domains

---

1. On the System Manager console, select **Routing > Domains**.
  2. To delete an existing domain or domains, select the check boxes for the domains that you want to edit and click **Delete**.
  3. Click **Delete** on the confirmation page.
- 

### Related topics:

[Delete Confirmation field descriptions](#) on page 1235

## Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of selected domains.

| Button        | Description                         |
|---------------|-------------------------------------|
| <b>Delete</b> | Deletes the selected domains.       |
| <b>Cancel</b> | Cancel the deletion of the domains. |

### Related topics:

[Deleting domains](#) on page 1235

## Domains field descriptions

Use this page to create, modify, delete, and manage domains.

| Button           | Description   |
|------------------|---|
| <b>Edit</b>      | Opens the Domains page that you can use to modify the domain details. |
| <b>New</b>       | Opens the Domains page that you can use to create new domains.        |
| <b>Duplicate</b> | Creates a duplicate of the selected domain.                           |

| Button                                    | Description  |
|---|--|
| <b>Delete</b>                             | Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the domain.                            |
| <b>More Actions &gt; Refresh all data</b> | Refreshes all data. Any unsaved modifications are lost.  |
| <b>More Actions &gt; Import</b>           | Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.            |
| <b>More Actions &gt; Export Domains</b>   | Opens the Export Domains page that allows you to export the domains data as an XML file to a specified location.             |
| <b>More Actions &gt; Export all data</b>  | Opens the Export all data page that allows you to export the routing entities data as a zipped file to a specified location. |
| <b>Commit</b>                             | Distributes the selected domain to all the Session Manager instances in the enterprise.                                      |

## Domain field descriptions

Use this page to create new domains

| Name           | Description  |
|----------------|--|
| <b>Name</b>    | Name of the domain.  |
| <b>Type</b>    | List of the type of domains. Only Domains of type SIP can be used for routing. |
| <b>Default</b> | Indicates the default domain.  |
| <b>Notes</b>   | Additional notes about the domain.   |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Saves the domain and distributes it to all the instances of the Session Manager. |
| <b>Cancel</b> | Cancel the domain creation.  |

## Bulk import for Domains

Please follow these rules when creating an XML bulk import file:

- The domain name must be unique, and is referred to by other elements.
- It is not possible to create a domain with <domainType> of type “sip” that have <defaultDomain> containing the value “true”.
- The values in <domainType> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.

**Example:**

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sipdomainFullTOList>
  <SipdomainFullTO>
    <notes>this is a test</notes>
    <defaultDomain>>false</defaultDomain>
    <domainName>avaya.com</domainName>
    <domainType>sip</domainType>
    <name>avaya.com</name>
  </SipdomainFullTO>
  <SipdomainFullTO>
    <notes>this is another test</notes>
    <defaultDomain>>false</defaultDomain>
    <domainName>avaya2.com</domainName>
    <domainType>sip</domainType>
    <name>avaya2.com</name>
  </SipdomainFullTO>
</sipdomainFullTOList>
```

---

## Locations

### About Locations

You can use the Locations screen to set up and configure gateway and user locations. The IP address of the device determines the current physical location of the caller or the called user. Session Manager matches the IP address against the patterns defined on location screens. If there is no match in the IP address patterns, Session Manager uses the SIP entities location as the location.

Session Manager uses the origination location to determine which dial patterns to look at when routing the call if there are dial patterns administered for specific locations. Locations are also used to limit the number of calls coming out of or going to a physical location. This is useful for those locations where the network bandwidth is limited. This is also known as Call Admission Control (CAC). You can enable CAC in Session Manager by specifying **Average bandwidth per call** and **Managed Bandwidth** on the **Locations** screen. If the Managed Bandwidth field has a non-blank value, Session Manager keeps track of the bandwidth in use based on the calls coming out of and going to that specific location and denies new calls when the bandwidth in use reaches the limit.

If the Managed Bandwidth field is blank for a location, no CAC is done for that location. Session Manager allows you to use the following wildcard characters to specify a location:

- “\*” (star) is used to specify any number of allowed characters at the end of the string.
- “x” is used to specify a digit.

 **Note:**

Pattern can also accept IP address range. Example: 10.0.0.1-10.0.0.5

IP address mask is also a valid pattern. Example: 135.9.0.0/16

The Locations screen can contain one or several IP addresses. Each SIP entity has a particular IP address. Depending on the physical and geographic location of each SIP entity, some of the SIP entities can be grouped into a single location. For example, if there are two Communication Managers located at Denver, they can form one location named Denver.

## Creating Locations

---

1. On the System Manager console, select **Routing > Locations**. The Location Details screen is displayed.
  2. Click **New**.
  3. Enter the location name in the **Name** field.
  4. Enter notes about the location, if required.
  5. Specify the managed bandwidth for the location in the **Managed Bandwidth** field.
  6. Specify the average bandwidth per call for the location in the **Average Bandwidth per Call** field.
  7. To add a location pattern, click **Add** under **Location Pattern**.
  8. Enter an IP address pattern to match.
  9. Enter notes about the location pattern, if required.
  10. Continue clicking the **Location Pattern Add** button until all the required Location Pattern matching patterns have been configured.
  11. Click **Commit**.
- 

### Related topics:

[Location Details field descriptions](#) on page 1240

## Modifying Locations

---

1. On the System Manager console, select **Routing > Locations**.
2. If required, modify the managed bandwidth for the location in the **Managed Bandwidth** field.
3. If required, modify the average bandwidth per call for the location in the **Average Bandwidth per Call** field.

4. To edit a location name or location matching pattern, select a check box for the required location and click **Edit** and make the required changes to the location or location pattern for that location.
  5. To add or remove a location pattern, click **Add** or **Remove** under **Location Pattern**.
  6. Click **Commit**.
- 

## Deleting Locations

---

1. On the System Manager console, select **Routing > Locations**.
  2. To delete an existing location or locations, select the respective check boxes and click **Delete**.
  3. Click **Delete** on the confirmation page.
- 

### Related topics:

[Delete Confirmation field descriptions](#) on page 1239

## Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of locations.

| Button        | Description                          |
|---------------|--------------------------------------|
| <b>Delete</b> | Deletes the selected location.       |
| <b>Cancel</b> | Cancel the deletion of the location. |

### Related topics:

[Deleting Locations](#) on page 1239

## Locations field descriptions

Use this page to create, modify, delete, and manage locations.

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the Location Details page that you can use to modify the location details. |

| Button                                    | Description  |
|---|--|
| <b>New</b>                                | Opens the Location Details page that you can use to create new locations.  |
| <b>Duplicate</b>                          | Creates a duplicate of the selected location and assigns a new state to it.  |
| <b>Delete</b>                             | Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the location.                          |
| <b>More Actions &gt; Refresh all data</b> | Refreshes all data. Any unsaved modifications are lost.  |
| <b>More Actions &gt; Import</b>           | Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.            |
| <b>More Actions &gt; Export Locations</b> | Opens the Export Locations page that allows you to export the location data as an XML file to a specified location.          |
| <b>More Actions &gt; Export all data</b>  | Opens the Export all data page that allows you to export the routing entities data as a zipped file to a specified location. |
| <b>Commit</b>                             | Distributes the selected location to all the Session Manager instances in the enterprise.                                    |

## Location Details field descriptions

Use this page to set up and configure locations.

| Name                              | Description  |
|-----------------------------------|--|
| <b>Name</b>                       | Name of the location.  |
| <b>Notes</b>                      | Notes about the location.  |
| <b>Managed Bandwidth</b>          | Managed bandwidth for the location.  |
| <b>Average Bandwidth per call</b> | Average bandwidth per call for the location.   |
| <b>Location Pattern</b>           | <p>The IP address pattern that should be matched for the location. For example,</p> <ul style="list-style-type: none"> <li>• 135.12x.121.*</li> <li>• 13x.1xx.*</li> <li>• 135.*</li> <li>• 135.12x.121.123</li> </ul> <p> <b>Note:</b></p> |

| Name | Description   |
|------|---|
|      | Pattern can also accept IP address range. Example:<br>10.0.0.1-10.0.0.5<br>IP address mask is also a valid pattern. Example: 135.9.0.0/16 |

| Button        | Description   |
|---------------|---|
| <b>Add</b>    | Adds an IP address pattern to match for the location.     |
| <b>Remove</b> | Removes the IP address pattern to match for the location. |

**Related topics:**

[Creating Locations](#) on page 1238

**Denied Location field descriptions**

Use this page to specify denied locations for the selected dial pattern

| Button        | Description   |
|---------------|---|
| <b>Select</b> | Selects the location as a denied location for the dial pattern. |
| <b>Cancel</b> | Cancel the selection of the denied location.                    |

**Bulk import for Locations**

Please follow these rules when creating an XML bulk import file:

- Locations are referred to as routing origination in the import XML.
- The name of a location is unique and is referred to by other elements.
- Multiple Routing Origination Patterns (<routingoriginationpatterns>) can be configured for one Routing Origination Name.
- The values in <ManagedBandwidthUnitOfMeasurement> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.

**Example:**

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<routingoriginationFullTOList>
  <RoutingoriginationFullTO>
    <notes>this is a test</notes>
    <name>New York</name>
    <AverageBandwidthPerCall>80</AverageBandwidthPerCall>
    <AverageBandwidthPerCallUnitOfMeasurement>Kbit/sec</
AverageBandwidthPerCallUnitOfMeasurement>
    <ManagedBandwidth>500000</ManagedBandwidth>
    <ManagedBandwidthUnitOfMeasurement>Kbit/sec</
ManagedBandwidthUnitOfMeasurement>
```

```
<routingoriginations>
  <notes>this is a test</notes>
  <ipaddresspattern>1.2.3.4-1.2.3.10</ipaddresspattern>
</routingoriginations>
<routingoriginations>
  <notes>this is a test</notes>
  <ipaddresspattern>1.2.4.*</ipaddresspattern>
</routingoriginations>
<TimeToLiveInSec>3600</TimeToLiveInSec>
</RoutingoriginationsFullTO>
<RoutingoriginationsFullTO>
  <notes>this is a test</notes>
  <name>Berlin</name>
  <AverageBandwidthPerCall>80</AverageBandwidthPerCall>
  <AverageBandwidthPerCallUnitOfMeasurement>Kbit/sec</
AverageBandwidthPerCallUnitOfMeasurement>
  <ManagedBandwidth>900000</ManagedBandwidth>
  <ManagedBandwidthUnitOfMeasurement>Kbit/sec</
ManagedBandwidthUnitOfMeasurement>
  <routingoriginations>
    <notes>this is a test</notes>
    <ipaddresspattern>3.*</ipaddresspattern>
  </routingoriginations>
  <routingoriginations>
    <notes>this is a test</notes>
    <ipaddresspattern>2.3.4.5</ipaddresspattern>
  </routingoriginations>
  <TimeToLiveInSec>3600</TimeToLiveInSec>
</RoutingoriginationsFullTO>
</routingoriginationsFullTOList>
```

---

## Adaptations

### About Adaptations

You can optionally use Adaptations to modify SIP messages that are leaving a Session Manager instance (egress adaptation) and that are entering a Session Manager instance (ingress adaptation). This adaptation function is needed to convert strings containing calling and called party numbers from the local dialplan of a SIP entity to the dialplan administered on the Session Manager, and vice-versa. Adaptation is also needed when other SIP entities require special SIP protocol conventions. Each administered SIP entity may have its own unique adaptation, or one adaptation can be shared among multiple entities.

Adaptations are implemented as software modules that can be created and deployed to fit the needs of the system.

Session Manager includes a module called DigitConversionAdapter, which can convert digit strings in various message headers as well as hostnames in the Request-URI and other headers. It also contains adaptation modules which do protocol conversions, such as for AT&T, Verizon, Cisco, and Nortel systems, as well as the digit conversion. All of these adapters allow for modification of URIs specified using unique name-value pairs for egress adaptation. For example, these can be used to replace the host name in the Request-URI with an administered host name during egress adaptation. Details are explained in the Creating Adaptations section.

An adaptation administered using routing specifies the module to use as well as the digit conversion that is to be performed on headers in the SIP messages. Different digit conversions can be specified for ingress and egress adaptation.

Additionally, digit conversion can be specified to modify only “origination” type headers, only “destination” type headers, or both. The origination/source type URIs are:

- P-Asserted-Identity
- History-Info (calling portion)
- Contact (in 3xx response)

The destination type URIs are:

- Request-URI
- Message Account (in NOTIFY/message-summary body)
- Refer-To (in REFER message)

 **Note:**

Session Manager adaptations do not work on the to and the from SIP headers.

## Adaptation example

In the following example, an adaptation for AT&T service provider is needed at least for international calls.

For incoming calls, AT&T sends the 10 digit local number. To convert this into E.164, Session Manager must add a plus sign. Specify the following values:

- Matching pattern: 1
- Min: 10
- Max: 10
- Delete Digits: 0
- Insert Digits: +
- Address to modify: both

For outgoing calls to AT&T, Session Manager must convert the E.164 form to a format that AT&T supports, either 1+10 digits for North America calls, or 011+country code + number for international calls. For example, for calls to North America, specify the following values:

- Matching Pattern: +1
- Min: 12
- Max: 12

- Delete Digits: 1
- Insert Digits: <None>
- Notes: Calls to North America

For calls to Germany, specify the following values:

- Matching Pattern: +49
- Min: 13
- Max: 13
- Delete Digits: 1
- Insert Digits: 011
- Address to modify: destination
- Notes: Calls to Germany

## Adaptation Module administration

On the Adaptation Details screen, the format of the **Adaptation Module** field is:

<Name of adaptation module> <name1=value1> <name2=value2>,...

- The module name contains only the name
- The module parameters can contain either a single parameter or a list of "name=value name=value name=value".



### Note:

The list is separated by spaces and not by commas

There are currently 4 names defined which can be administered using either the full name or shortcut name:

### EGRESS Domain Modification Parameters

- `overrideDestinationDomain` (or abbreviated name `odstd`): {parameter #1 if not named}, replaces the domain in Request-URI and Notify/message-summary body with the given value for egress only.
- `overrideSourceDomain` (or abbreviated name `osrtd`): replaces the domain in the P-Asserted-Identity header and calling part of the History-Info header with the given value for egress only.

**INGRESS Domain Modification Parameters:**

- `ingressOverrideDestinationDomain` (or abbreviated name `iodstd`): replaces the domain in Request-URI and Notify/message-summary body with the given value for ingress only.
- `ingressOverrideSourceDomain` (or abbreviated name `iosrcd`): replaces the domain in the P-Asserted-Identity header and calling part of the History-Info header with the given value for ingress only.

**Example:**

```
CiscoAdapter osrcd=dr.avaya.com odstd=ny.avaya.com
```

**The same value in verbose form:**

```
CiscoAdapter overrideSourceDomain=dr.avaya.com
overrideDestinationDomain=ny.avaya.com
```

## Creating Adaptations

---

1. On the System Manager console, select **Routing > Adaptations**. The Adaptations screen is displayed.
2. Click **New**. The Adaptation Details screen is displayed.
3. Enter the Name, Adaptation Module and any other required fields in the first section.
  - a. Enter a descriptive name for the adaptation.
  - b. Specify an adaptation module.
    - **Module name** field contains only the name (4 options)
    - **Module parameter** field contain either a single parameter or a list of "name=value name=value name=value".

 **Note:**

The list is separated by spaces and not by commas

- c. Enter a list of URI parameters to append to the Request-URI on egress in the **Egress URI Parameters** field.
 

URI parameters can be added to the Request-URI. For example, the parameter "user=phone" can be appended for all INVITEs routing to a particular SIP entity. The egress Request-URI parameters are administered from the Adaptation Details using the Egress URI Parameters field.

The field's format is the string that should be appended to the Request URI. The string must conform to the augmented BNF defined for the SIP Request

URI in RFC3261. A leading ';' is optional. Entry “;user=phone;custApp=1” is equivalent to “user=phone;custApp=1”.

- d. Enter description about the adaptation module in the **Notes** field.
4. Click **Add** under **Digit Conversion for Incoming Calls** if you need to configure ingress digit conversion. Ingress adaptation is used to administer digit manipulation for calls coming into the Session Manager instance.
5. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
6. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.  
The minimum value can be 1 or more. The maximum value can be 36.
7. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
8. Enter the digits that you want inserted before the number in the **Insert Digits** field.
9. From the drop-down list, select the value for **Address to modify**. A setting of both will look for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination will always take priority over entries that match a pattern of both.
10. Continue clicking the Ingress Adaptation **Add** button until all the required ingress matching patterns have been configured.
11. To remove a matching pattern for ingress adaptations, select the check box next to that pattern and click **Remove**.
12. Click **Add** under **Digit Conversion for Outgoing Calls** if you need to configure egress digit conversion. Egress adaptation administers digit manipulation for calls going out of the Session Manager instance.
13. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
14. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.  
The minimum value can be 1 or more. The maximum value can be 36.
15. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
16. Enter the digits that you want inserted before the number in the **Insert Digits** field.
17. From the drop-down list, select the value for **Address to modify**. A setting of both will look for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination will always take priority over entries that match a pattern of both.

18. Continue clicking the Egress Adaptation **Add** button until all the required egress matching patterns have been configured.
19. To remove a matching pattern for egress adaptations, select the check box next to that pattern and click **Remove**.
20. Click **Commit**.

---

**Related topics:**

[Adaptation Details field descriptions](#) on page 1252

## Modifying Adaptations

---

1. On the System Manager console, select **Routing > Adaptations**. The Adaptation screen is displayed.
2. Select the adaptation for modification and click **Edit**  
All adaptation modules have the ability to replace domain (also known as host name) portion of the URI with a specified value for source and destination type URIs on outgoing calls (egress) and to append parameters to the Request URI on for outgoing calls (egress). This adaptation functionality is expandable to adapt additional deployments needing further flexibility.
3. Edit the Name, Adaptation Module and any other required fields in the first section. Currently there is only one adaptation module named "DigitConversionAdapter".
  - a. Enter a descriptive name for the adaptation.
  - b. Specify an adaptation module.
    - **Module name** field contains only the name (4 options)
    - **Module parameter** field contain either a single parameter or a list of "name=value name=value name=value".

 **Note:**

The list is separated by spaces and not by commas

- c. Enter a list of URI parameters to append to the Request-URI on egress in the **Egress URI Parameters** field.  
URI parameters can be added to the Request-URI. For example, the parameter "user=phone" can be appended for all INVITEs routing to a particular SIP entity. The egress Request-URI parameters are administered from the Adaptation Details using the Egress URI Parameters field.  
The field's format is the string that should be appended to the Request URI. The string must conform to the augmented BNF defined for the SIP Request

URI in RFC3261. A leading ';' is optional. Entry ";user=phone;custApp=1" is equivalent to "user=phone;custApp=1".

- d. Enter description about the adaptation module in the **Notes** field.
4. Click **Add** under **Digit Conversion for Incoming Calls** if you need to configure ingress digit conversion. Ingress adaptation is used to administer digit manipulation for calls coming into the Session Manager instance.
5. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
6. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.  
The minimum value can be 1 or more. The maximum value can be any number up to 36.
7. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
8. Enter the digits that you want inserted before the number in the **Insert Digits** field.
9. From the drop-down list, select the value for Address to modify. A setting of both will look for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination will always take priority over entries that match a pattern of both.
10. Continue clicking the Ingress Adaptation **Add** button until all the required ingress matching patterns have been configured.
11. To remove a matching pattern for ingress adaptations, select the check box next to that pattern and click **Remove**.
12. Click **Add** under **Digit Conversion for Outgoing Calls** if you need to configure egress digit conversion. Egress adaptation administers digit manipulation for calls going out of the Session Manager instance.
13. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
14. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.  
The minimum value can be 1 or more. The maximum value can be any number up to 36. The minimum value must be less than or equal to the maximum value.
15. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
16. Enter the digits that you want inserted before the number in the **Insert Digits** field.
17. From the drop down list, select the value for Address to modify. A setting of both will look for adaptations on both origination and destination type headers. Entries

that match a pattern of type origination or destination will always take priority over entries that match a pattern of both.

18. Continue clicking the Egress Adaptation **Add** button until all the required egress matching patterns have been configured.
  19. To remove a matching pattern for egress adaptations, select the check box next to that pattern and click **Remove**.
  20. Click **Commit**.
- 

## Deleting Adaptations

---

1. On the System Manager console, select **Routing > Adaptations**.
  2. To delete an existing Adaptation or Adaptations, select the respective check boxes and click **Delete**.
  3. Click **Delete** on the confirmation page.
- 

### Related topics:

[Delete Confirmation field descriptions](#) on page 1249

## Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of selected adaptations

| Button        | Description  |
|---------------|--|
| <b>Delete</b> | Deletes entries for the selected adaptations from the database |
| <b>Cancel</b> | Cancels the deletion of the selected adaptations               |

### Related topics:

[Deleting Adaptations](#) on page 1249

## Installed vendor adapters

### Cisco Adapter (CiscoAdapter)

The Cisco Adapter provides two basic header manipulations: converting between Diversion and History-Info headers and converting between P-Asserted-Id and Remote-Party-Id headers. The Diversion and Remote-Party-Id headers have not been accepted by the IETF.

They are replaced by History-Info and P-Asserted-Identity respectively, but are still used in the Cisco products. The Cisco Adapter also performs all the conversions available by the Digit Conversion Adapter.

**Case 1:**

Cisco requires the use of the Diversion header, rather than the History-Info header to provide information related to how and why the call arrives to a specific application or user. The following examples illustrate the adaptations.

**Example 1:**

Communication Manager user 66600001 forwards to Cisco user 60025.

Communication Manager's outgoing INVITE has this history-info:

```
History-Info: "<sip:66600001@ny.avaya.com>;index=1"
History-Info: "stn 66600001"
<sip:66600001@ny.avaya.com?Reason=SIP%3Bcause%3D302%3Btext%3D%22Moved%20Temporarily%22&Reason=Redirection%3Bcause%3DCFI>;index=1.1
History-Info: <sip:600025@ny.avaya.com>;index=1.2
```

In the message sent to Cisco this is converted to:

```
Diversion: "stn 66600001" <sip:66600001@ny.avaya.com>;reason=no-
answer;privacy=off;screen=no
```

**Example 2:**

Communication Manager user calls Cisco user 60025. The call is routed to Message Manager at extension 688810.

The INVITE message from the Cisco server contains the Diversion Header:

```
Diversion: "Ken's Desk" <sip:600025@ny.avaya.com>;reason=user-
busy;privacy=off;screen=no
```

The message is adapted and the outgoing INVITE to MM replaces the Diversion header with the following:

```
History-Info: <sip:600025@ny.avaya.com>;index=1
History-Info: "Ken's Desk"
<sip:600025@ny.avaya.com?Reason=SIP%3Bcause%3D486%3Btext%3D%22Bus
y%20Here%22&Reason=Redirection%3Bcause%3DNORMAL%3Bavaya-cm-reason%3D
%22cover-busy%22%3Bavaya-cm-vm-address-digits%3D81080000%3Bavaya-cm-vm-
address-handle%3Dsip:80000%40avaya.com>;index=1.1
History-Info: "MM" <sip:688810@ny.avaya.com>;index=1.2
```

**Case 2:**

Cisco requires information in the P-Asserted-Identity (PAI) header to be received in the Remote-Party-Id (RPI) header. Any incoming message containing a P-Asserted-Identity header being routed to Cisco will replace that header with the Remote-Party-Id header. Similarly, calls from Cisco containing the Remote-Party-Id header will be converted to a P-Asserted-Identity header when routed to non-Cisco entities.

**Example 3:**

A call is placed from 12345 at Communication Manager and routed to the Cisco PBX.

The INVITE from Communication Manager contains:

```
P-Asserted-Identity: "Ryan" <sip:12345@avaya.com>
```

This header is converted to RPI when the request is sent to the Cisco PBX:

```
Remote-Party-Id: "Ryan"
```

```
<sip:12345@avaya.com>;party=called;screen=no;privacy=off
```

**Example 4:**

A call is placed from 23456 at Cisco PBX and routed to Communication Manager.

The INVITE from Cisco PBX contains:

```
Remote-Party-Id: "Ryan"
```

```
<sip:23456@avaya.com>;party=called;screen=no;privacy=off
```

This header is converted to PAI when the request is sent to Communication Manager:

```
P-Asserted-Identity: "Ryan" <sip:23456@avaya.com>
```

**Verizon Adapter (VerizonAdapter)**

The Verizon adapter requires the same History-Info to Diversion adaptations that the Cisco Adapter uses. The Verizon Adapter also performs all the conversions available by the Digit Conversion Adapter.

**AT&T Adapter (AttAdapter)**

AT&T does not handle the History-Info header. The adaptation module removes, on egress to AT&T, any History-Info headers in a request or response. Messages from AT&T do not change. The AT&T Adapter also performs all the conversions available by the Digit Conversion Adapter.

**Adaptations field descriptions**

Use this page to create, modify, delete, and manage adaptations.

| Button                                      | Description  |
|---|--|
| <b>Edit</b>                                 | Opens the Adaptation Details page that you can use to modify the adaptation details.   |
| <b>New</b>                                  | Opens the Adaptation Details page that you can use to create new adaptations.  |
| <b>Duplicate</b>                            | Creates a duplicate of the selected adaptation and assigns a new state to it   |
| <b>Delete</b>                               | Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the adaptation.                        |
| <b>More Actions &gt; Refresh all data</b>   | Refreshes all data. Any unsaved modifications are lost.  |
| <b>More Actions &gt; Import</b>             | Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.            |
| <b>More Actions &gt; Export Adaptations</b> | Opens the Export Adaptation page that allows you to export the adaptation data as an XML file to a specified location.       |
| <b>More Actions &gt; Export all data</b>    | Opens the Export all data page that allows you to export the routing entities data as a zipped file to a specified location. |
| <b>Commit</b>                               | Distributes the selected adaptation to all the Session Manager instances in the enterprise.                                  |

## Adaptation Details field descriptions

Use this page to specify the adaptation details.

### General section

| Name                         | Description   |
|------------------------------|---|
| <b>Name</b>                  | Name of the adaptation. Must be unique and be between 3 and 64 characters in length.                    |
| <b>Module name</b>           | The module name contains only the name (4 options)  |
| <b>Module parameter</b>      | The module parameters contain either a single parameter or a list of "name=value name=value name=value" |
| <b>Egress URI Parameters</b> | The terminating trunk group parameters  |
| <b>Notes</b>                 | Other details that you wish to add.   |

## Digit Conversion for Incoming Calls section

| Name                     | Description  |
|--------------------------|--|
| <b>Select check box</b>  | Use this check box to select and use the digit conversion for the incoming calls   |
| <b>Matching Pattern</b>  | Pattern to match for the incoming calls. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.  |
| <b>Min</b>               | Minimum number of digits to be matched   |
| <b>Max</b>               | Maximum number of digits to be matched   |
| <b>Delete Digits</b>     | Number of digits to be deleted from the dialled number   |
| <b>Insert Digits</b>     | Number of digits to be added before the dialled number   |
| <b>Address to Modify</b> | Selecting both looks for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination always take priority over entries that match a pattern of both. |
| <b>Notes</b>             | Any other details that you wish to add   |

## Digit Conversion for Outgoing Calls section

| Name                     | Description  |
|--------------------------|--|
| <b>Select check box</b>  | Use this check box to select and use the digit conversion for the outgoing calls   |
| <b>Matching Pattern</b>  | Pattern to match for the outgoing calls. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.  |
| <b>Min</b>               | Minimum number of digits to be matched   |
| <b>Max</b>               | Maximum number of digits to be matched   |
| <b>Delete Digits</b>     | Number of digits to be deleted from the dialled number   |
| <b>Insert Digits</b>     | Number of digits to be added before the dialled number   |
| <b>Address to Modify</b> | Selecting both looks for adaptations on both origination and destination type headers. Entries that match a pattern of type origination or destination always take priority over entries that match a pattern of both. |
| <b>Notes</b>             | Any other details that you wish to add   |

| Button        | Description  |
|---------------|--|
| <b>Add</b>    | Adds digit conversion for incoming or outgoing calls for the adaptations     |
| <b>Remove</b> | Removes digit conversion from incoming or outgoing calls for the adaptations |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Saves the adaptation details and distributes them to the Session Manager instances in the enterprise |
| <b>Cancel</b> | Cancels changes to the adaptation details and returns to the Adaptations page                        |

**Related topics:**

[Creating Adaptations](#) on page 1245

## Bulk import for Adaptations

Please follow these rules when creating an XML bulk import file:

- The name of an adaptation is unique and is referred to by other elements.
- The value of <adaptationmodule> is a combination of the fields “Module Name” and “Module Parameters” in the System Manager user interface. The values are separated by a single space.
- Multiple Ingress and Egress configurations <<EgressadaptationFullTO>, <IngressadaptationFullTO>> can be configured for one Adaptation name.
- The values in <addressToModify> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.

**Example:**

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<adaptationFullTOList>
  <AdaptationFullTO>
    <notes>this is a test</notes>
    <adaptationmodule>VersionModule param1=17 param2=15</adaptationmodule>
    <egressuriparameters>url1</egressuriparameters>
    <name>VerisonAdaptation</name>
    <EgressadaptationFullTO>
      <notes>test</notes>
      <deletedigits>1</deletedigits>
      <insertdigits>3</insertdigits>
      <matchingpattern>809</matchingpattern>
      <maxdigits>20</maxdigits>
      <mindigits>3</mindigits>
      <addressToModify>origination</addressToModify>
    </EgressadaptationFullTO>
    <EgressadaptationFullTO>
      <notes>test</notes>
      <deletedigits>1</deletedigits>
      <insertdigits>3</insertdigits>
      <matchingpattern>810</matchingpattern>
      <maxdigits>21</maxdigits>
      <mindigits>3</mindigits>
      <addressToModify>destination</addressToModify>
    </EgressadaptationFullTO>
    <EgressadaptationFullTO>
      <notes>test</notes>
      <deletedigits>1</deletedigits>
      <insertdigits>3</insertdigits>
      <matchingpattern>811</matchingpattern>
      <maxdigits>22</maxdigits>
    </EgressadaptationFullTO>
  </AdaptationFullTO>
</adaptationFullTOList>
```

```

        <mindigits>3</mindigits>
        <addressToModify>both</addressToModify>
    </EgressadaptationFullTO>
    <IngressadaptationFullTO>
        <notes>test</notes>
        <deletedigits>1</deletedigits>
        <insertdigits>2</insertdigits>
        <matchingpattern>148</matchingpattern>
        <maxdigits>25</maxdigits>
        <mindigits>3</mindigits>
        <addressToModify>origination</addressToModify>
    </IngressadaptationFullTO>
    <IngressadaptationFullTO>
        <notes>test</notes>
        <deletedigits>1</deletedigits>
        <insertdigits>2</insertdigits>
        <matchingpattern>149</matchingpattern>
        <maxdigits>26</maxdigits>
        <mindigits>3</mindigits>
        <addressToModify>destination</addressToModify>
    </IngressadaptationFullTO>
    <IngressadaptationFullTO>
        <notes>test</notes>
        <deletedigits>1</deletedigits>
        <insertdigits>2</insertdigits>
        <matchingpattern>150</matchingpattern>
        <maxdigits>27</maxdigits>
        <mindigits>3</mindigits>
        <addressToModify>both</addressToModify>
    </IngressadaptationFullTO>
</AdaptationFullTO>
</adaptationFullTOList>

```

---

## SIP Entities

### About SIP Entities

SIP entities are all the network entities that are a part of the SIP System. SIP entities include Session Manager instances, Communication Managers, Session Border Controllers (SBCs), SIP trunks, and so on.

### Authentication of trusted SIP entities

Routing uses the following information for the authentication of SIP entities by performing validation on IP/Transport Layer and TLS Layer:

- FQDN or IP Address of the SIP entity
- Credential name of the SIP entity
- Protocol of the Entity Links. This is a SIP connection transport type (TCP/TLS/UDP)
- Trust State of the Entity Link (This defines whether the entity link is Trusted or not)

For information about administering these fields, refer to [Creating SIP entities](#).

## IP and transport layer validation

When a SIP entity connects to Session Manager over a TCP or TLS port, Session Manager validates that:

- The IP address matches one of the SIP entities configured in routing that have trusted entity links with the Session Manager. If the SIP entities are configured as FQDN, Session Manager performs a DNS resolution before doing the verification.
- Transport for the incoming SIP connection matches with one of the entity links associated with this SIP entity and the Session Manager. Also, the Trust State of the entity link must be configured as trusted. Session Manager does not accept connections matching untrusted entity links.

For SIP packets over UDP, above validation is performed for each packet. For SIP TLS connections, further validation is performed as described in the next section.

## TLS layer validation

Session Manager applies the following additional validations for SIP TLS connections:

1. During a TLS handshake, mutual TLS authentication is performed, that is, Identity certificate of the SIP entity is validated against the trusted CA certificate repository in the Session Manager for SIP TLS. If this verification fails, Session Manager does not accept the connection.
2. If the mutual TLS authentication is successful, further validation is performed on the SIP entity Identity Certificate as per the Credential Name or the far-end IP address.
  - If the Credential Name string is empty, the connection is accepted.
  - If the Credential Name string is not empty, the Credential Name and the IP address of the far-end is searched for in the following fields in the identity certificate provided by the SIP entity:
    - CN value from the subject
    - subjectAltName.dNSName
    - subjectAltName.uniformResourceIdentifier (For IP address comparison, IP address string is converted to SIP:W.X.Y.Z before comparison. W.X.Y.Z is the remote socket IPV4 address. Also, case insensitive search is performed in this case)

With entity links from both Session Manager instances, checking the **Override Port & Transport with DNS SRV** check box on the SIP entity form indicates that both the Port and Protocol (Transport) on the SIP entity form are ignored.

- If you select the check box, the port and transport administered in the local host name resolution table is used, which could override the entity link.
- If the FQDN is not in the local table and DNS is consulted, if you have not selected the check box, only an A-Record lookup is done in DNS to resolve the host name to an IP address. Transport and port specified in the entity link are used. If you selected the check box, a full DNS lookup (as described in RFC 3263) is done, and the transport and port specified in the entity link could be overridden.

## Creating SIP Entities

Use the SIP entities screen to create SIP entities. To administer minimal routing via Session Manager, you need to configure a SIP entity of type Communication Manager and a second SIP entity of type Session Manager.

- 
1. On the System Manager console, select **Routing > SIP Entities**.
  2. Click **New**.
  3. Enter the Name of the SIP entity in the **Name** field.
  4. Enter the FQDN or IP address of the SIP entity in the **FQDN or IP Address** field.
  5. Select the type of SIP entity from the drop-down menu in the **Type** field.
  6. Enter any other required information in the **General** section.
  7. If you need to specify an Adaptation Module for the SIP entity, click the drop-down selector for the **Adaptation** field and select a value.
  8. If you need to specify the Location for the SIP entity, click the drop-down selector for the **Location** field and select a location.
  9. If the SIP entity Type is “Session Manager” and you need to specify an Outbound Proxy for the SIP entity, click the drop-down selector for the **Outbound Proxy** field.
  10. Enter a regular expression string in the **Credential name** field. The Credential name is used for TLS connection validation by searching for this string in the SIP entity identity certificate.
    - If you do not want to perform the additional validation on the SIP entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty.
    - If you want to verify that a specific string or SIP entity FQDN is present within the SIP entity identity certificate, enter that string or SIP entity FQDN using the regular expression syntax.

- If you want to verify that the SIP entity IP address is present within the SIP entity identity certificate, enter the SIP entity IP address using the regular expression syntax.



**Note:**

IP Address is searched by default when any string is configured in the Credential Name.

The Credential name is a regular expression string and follows Perl version 5.8 syntax. Here are some examples:

For “www.sipentity.domain.com”, use the string “www\.sipentity\.domain\.com”.

For “192.14.11.22”, use string “192\.14\.11\.22”. You can look for a subset of the string or you can create a wild card search. For example, to look for “domain.com” as a substring, use the string “domain\.com”

11. Under SIP Link Monitoring, use the drop-down menu to select one of the following:
  - Use Session Manager Configuration – Use the settings under **Session Manager > Session Manager Administration**
  - Link Monitoring Enabled – Enables link monitoring on this SIP entity.
  - Link Monitoring Disabled – Link monitoring will be turn off for this SIP entity.
12. If you need to specify the Port parameters, click **Add** under Port. When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.
13. Enter the necessary Port and Protocol parameters.
14. To remove an incorrectly added Port, select the respective **Port** check box and click **Remove**.
15. Click **Commit**.

---

**Related topics:**

[SIP Entity Details field descriptions](#) on page 1261

## Modifying SIP entities

---

1. On the System Manager console, select **Routing > SIP Entities**.
2. Select the SIP entity for modification and click **Edit** .
3. Modify the Name, FQDN (fully Qualified Domain Name) or IP address of the SIP entity, Type (Session Manager, SBC, CM, VoicePortal, Gateway, SIP Trunk, or Other) and any other required fields in the first section.

4. If you need to specify an Adaptation Module for the SIP entity, click the drop-down selector for the **Adaptation** field.
  5. If you need to specify the Location for the SIP entity, click the drop-down selector for the **Location** field.
  6. If the SIP entity Type is “Session Manager” and you need to specify an Outbound Proxy for the SIP entity, click the drop-down selector for the **Outbound Proxy** field.
  7. Select the correct time zone from the **Time Zone** drop-down list.
  8. Enter or modify a value in seconds in the **SIP Timer B/F (secs)** field. This value must be between 1 and 32 seconds. The default is 4. This is the time Session Manager should await a response from a SIP entity before trying an alternate route.
  9. Enter or modify a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate.
    - If you do not want to perform the additional validation on SIP entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty.
    - If you want to verify that a specific string or SIP entity FQDN is present within the SIP entity identity certificate, enter that string or SIP entity FQDN using the regular expression syntax.
    - If you want to verify that the SIP entity IP address is present within the SIP entity identity certificate, enter the SIP entity IP address using the regular expression syntax. Please note that the system looks for the IP Address by default when any string is configured in the Credential Name.
-  **Note:**  
The Credential name is a regular expression string and follows Perl version 5.8 syntax. Here are some of the examples:
- For “www.sipentity.domain.com”, use the string “www\.sipentity\.domain\.com”.
  - For “192.14.11.22”, use string “192\.14\.11\.22”.
  - You can search a subset of the string or can create a wild card search. For example, for searching for “domain.com” as a substring, use the string “\*domain\.com\*”
10. Under SIP Link Monitoring, the following options are available from the drop-down menu:
    - a. **Use Session Manager Configuration**
    - b. **Link Monitoring Enabled** – Enables link monitoring on this SIP entity.
    - c. **Link Monitoring Disabled** – Link monitoring will be turn off for this SIP entity.
  11. If you need to specify the Port parameters, click **Add** under Port. When Session Manager receives a request where the host-part of the request-URI is the IP

address of the Session Manager, it associates one of the administered domains with the port on which the request was received.

12. Enter the necessary Port and Protocol parameters.
  13. To remove an incorrectly added Port, select the respective **Port** check box and click **Remove**.
  14. Click **Commit**.
- 

## Deleting SIP Entities

---

1. On the System Manager console, select **Routing > SIP Entities**.
  2. To delete an existing SIP entity or entities, select the respective check boxes and click **Delete**.
  3. Click **Delete** or **Cancel** on the confirmation page.
- 

## Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of the SIP entity.

| Button        | Description  |
|---------------|--|
| <b>Delete</b> | Deletes the selected SIP entity or entities.                 |
| <b>Cancel</b> | Cancels the deletion of the selected SIP entity or entities. |

## SIP Entities field descriptions

Use this page to create, modify, delete, and manage SIP entities.

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the SIP Entity Details page that you can use to modify the SIP entity.   |
| <b>New</b>  | Opens the SIP Entity Details page that you can use to create new SIP entities. |

| Button   | Description  |
|--|--|
| <b>Duplicate</b>                                       | Creates a duplicate of the selected SIP entity and assigns a new state to it.  |
| <b>Delete</b>  | Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the SIP entity.  |
| <b>More Actions &gt; Refresh all data</b>              | Refreshes all data. Any unsaved modifications are lost.  |
| <b>More Actions &gt; Display SIP Entity References</b> | Opens the Overview of References to SIP Entities page which displays the routing policies, adaptations, and locations that correspond to the SIP entity. |
| <b>More Actions &gt; Import</b>                        | Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.  |
| <b>More Actions &gt; Export SIP Entities</b>           | Opens the Export SIP Entities page that allows you to export the SIP entity data as an XML file to a specified location.                                 |
| <b>More Actions &gt; Export all data</b>               | Opens the Export all data page that allows you to export data for all routing entities as a zipped file to a specified location.                         |
| <b>Commit</b>  | Distributes the selected SIP entity to all the Session Manager instances in the enterprise.  |

## SIP Entity Details field descriptions

Use this page to specify SIP entity details.

| Name                      | Description   |
|---------------------------|---|
| <b>Name</b>               | SIP entity name. This name must be unique and can have between 3 and 64 characters.         |
| <b>FQDN or IP Address</b> | Fully qualified domain name or IP address of the SIP entity.                                |
| <b>Type</b>               | SIP entity type, such as a Session Manager, Communication Manager, SIP trunk, or a gateway. |
| <b>Notes</b>              | Additional notes about the SIP entity.  |
| <b>Adaptation</b>         | Adaptation to be used for the SIP entity. Select from already defined adaptations.          |
| <b>Location</b>           | SIP entity location. Select from previously defined locations.                              |
| <b>Outbound Proxy</b>     | Outbound proxy if the entity type is Session Manager, and you wish to specify a proxy.      |
| <b>Time Zone</b>          | Time zone for the SIP entity.   |

| Name  | Description  |
|---|--|
| <b>Override Port &amp; Transport with DNS SRV</b> | Specify if you wish to use DNS routing. SIP uses DNS procedures to allow a client to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS routing to allow a server to send a response to a backup client if the primary client fails. |
| <b>SIP Timer B/F (secs)</b>                       | Amount of time the Session Manager should wait for a response from the SIP entity.   |
| <b>Credential name</b>                            | Enter a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate.   |
| <b>Monitoring On/Off</b>                          | Select or clear the check box to turn SIP monitoring on or off.  |
| <b>Proactive cycle time (secs)</b>                | Enter a value between 120 and 9000 seconds. The default is 900. This specifies how often the entity is monitored when the link to the entity is up or active.  |
| <b>Reactive cycle time (secs)</b>                 | Enter a value between 30 and 900 seconds. The default is 120. This specifies how often the entity is monitored when a link to the entity is down or inactive.  |
| <b>Number of retries</b>                          | Enter a value between 0 and 15. The default is 1. This specifies the number of times Session Manager tries to ping or reach the SIP entity before marking it as down or unavailable.   |
| <b>Port</b>                                       | Add a listening port for the SIP entity.   |
| <b>Protocol</b>                                   | Protocol that the SIP entity uses.   |
| <b>SIP Domain</b>                                 | The domain of the SIP entity.  |
| <b>Notes</b>                                      | Additional notes about the port and port parameters.   |

| Button        | Description  |
|---------------|--|
| <b>Add</b>    | Adds the selected entity.  |
| <b>Remove</b> | Removes the selected entity.   |
| <b>Commit</b> | Saves the SIP entity and distributes it to the Session Managers in the enterprise. |
| <b>Cancel</b> | Cancel the creation or modification of the SIP entity.                             |

**Related topics:**

[Creating SIP Entities](#) on page 1257

## SIP Entity List field descriptions

Use this page to select and associate SIP entities to a routing policy.

| Name                      | Description  |
|---------------------------|--|
| <b>Name</b>               | Select a SIP entity name check box from the list to associate it to the selected routing policy.                 |
| <b>FQDN or IP Address</b> | Displays the fully qualified domain name or IP address of the SIP entity.  |
| <b>Type</b>               | Displays the type of the SIP entity such as Session Manager, SBC, CM, VoicePortal, Gateway, SIP Trunk, or Other. |
| <b>Notes</b>              | Additional notes.  |

| Button        | Description  |
|---------------|--|
| <b>Select</b> | Confirm selection of the SIP entity for associating to the routing policy. |
| <b>Cancel</b> | Cancel the selection of the SIP entity.                                    |

## Bulk import for SIP Entities

Please follow these rules when creating an XML bulk import file:

- The name of a SIP Entity is unique and is referred to by other elements.
- <adaptationName> must either be empty or refer to an existing adaptation with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the SIP Entity. SIP Entity of type “ASM” <Avaya Session Manager> cannot contain an adaptation entry.
- <adaptationName> contains the adaptation module name and parameters separated by spaces <examples below>.
- Listen ports (<listenports>) are only relevant for SIP Entity of type “ASM”. Do not include these entries for any other type of SIP Entity.
- Multiple listen ports entries (<listenports>) can be configured for one ASM SIP Entity.
  - <sipdomainName> must refer to an existing domain with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the SIP Entity.
  - The values in <transportprotocol> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.
- The values of <timezoneName> should be same (being case sensitive) as that of the field “Time Zone” in the SIP Entity user interface in System Manager.
- The field <userfc3263> corresponds to the “Override Port & Transport with DNS SRV” check box in the SIP entity form.

- The value of <entitytype> must contain one of the following values exactly as they appear below being case sensitive.
  - CM — communication manager (CM in the user interface)
  - ASM — Session Manager in the user interface
  - Modular Messaging — Session Manager in the user interface
  - VP — Voice Portal in the user interface
  - Gateway — Gateway in the user interface
  - SIP Trunk — SIP Trunk in the user interface
  - OTHER — Other in the user interface.
- The values in <cdrSetting> must appear exactly same being case sensitive, as they appear in the System Manager user interface.
- The field <do\_monitoring> corresponds to the field “SIP Link Monitoring” in the SIP Entity details form. The relation is as follows:
  - In order to enable SIP Link monitoring, <do\_monitoring> value must be “yes”
  - In order to enable SIP Link monitoring, <do\_monitoring> value must be “no”
  - In order to use the Session Manager configuration, the <do\_monitoring> tag must be completely omitted.

**Example:**

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sipentityFullTOList>
  <SipentityFullTO>
    <notes>this is a test</notes>
    <entitytype>CM</entitytype>
    <fqdnoripaddr>9.8.7.6</fqdnoripaddr>
    <name>BerlinCM</name>
    <adaptationName>VerisonAdaptation param1=12 param2=14</adaptationName>
    <cdrSetting>egress</cdrSetting>
    <credentialname>credential test</credentialname>
    <do_monitoring>yes</do_monitoring>
    <monitor_proactive_secs>900</monitor_proactive_secs>
    <monitor_reactive_secs>120</monitor_reactive_secs>
    <monitor_retries>1</monitor_retries>
    <routingoriginName>Berlin</routingoriginName>
    <timer_bf_secs>4</timer_bf_secs>
    <timeZoneName>Europe/Berlin</timeZoneName>
    <userfc3263>>false</userfc3263>
  </SipentityFullTO>
  <SipentityFullTO>
    <notes>this is a test</notes>
    <entitytype>CM</entitytype>
    <fqdnoripaddr>9.8.7.5</fqdnoripaddr>
    <name>NewYorkCM</name>
    <adaptationName>VerisonAdaptation param1=7 param2=8</adaptationName>
    <cdrSetting>egress</cdrSetting>
    <credentialname>credential test</credentialname>
    <do_monitoring>yes</do_monitoring>
    <monitor_proactive_secs>900</monitor_proactive_secs>
    <monitor_reactive_secs>120</monitor_reactive_secs>
    <monitor_retries>1</monitor_retries>
  </SipentityFullTO>
</sipentityFullTOList>
```

```

<routingoriginName>New York</routingoriginName>
<timer_bf_secs>4</timer_bf_secs>
<timeZoneName>America/New_York</timeZoneName>
<userfc3263>>false</userfc3263>
</SipentityFullTO>
<SipentityFullTO>
  <notes>this is a test</notes>
  <entitytype>ASM</entitytype>
  <fqdnoripaddr>4.5.6.7</fqdnoripaddr>
  <name>SessionManager1</name>
  <cdrSetting>egress</cdrSetting>
  <credentialname>credential test</credentialname>
  <do_monitoring>use-instance</do_monitoring>
  <listenports>
    <notes>this is a test</notes>
    <portnumber>5067</portnumber>
    <sipdomainName>avaya.com</sipdomainName>
    <transportprotocol>TLS</transportprotocol>
  </listenports>
  <monitor_proactive_secs>900</monitor_proactive_secs>
  <monitor_reactive_secs>120</monitor_reactive_secs>
  <monitor_retries>1</monitor_retries>
  <routingoriginName>New York</routingoriginName>
  <timer_bf_secs>4</timer_bf_secs>
  <timeZoneName>America/New_York</timeZoneName>
  <userfc3263>>false</userfc3263>
</SipentityFullTO>
</sipentityFullTOList>

```

---

## SIP Entity References

### About SIP Entity References

Session Manager enables you to see all references to a SIP entity such as its location, the routing policy that is created for the SIP entity, and adaptations, if any. If a single SIP entity has more than one combination of these references, Session Manager displays each of the combinations on a separate row.

### Displaying SIP Entity References

1. On the System Manager console, select **Routing > SIP Entities**.
2. From the SIP Entity menu, select the check box for a SIP entity whose references you want to see.
3. From the **More Actions** drop-down list, select **Display SIP Entity References**.

Session Manager displays the overview of SIP entity references such as the entity location, name of the routing policy attached to the entity, and adaptations, if any.

4. Click **Back** to navigate to the SIP entities.

---

**Related topics:**

[Overview of References to SIP Entities field descriptions](#) on page 1266

## Overview of References to SIP Entities field descriptions

Use this page to view information about the SIP entity references associated with the selected SIP entity

| Name                       | Description   |
|----------------------------|---|
| <b>SIP Entity Name</b>     | Lists the names of the SIP entities                               |
| <b>Location Name</b>       | Lists the location associated with the specified SIP entity       |
| <b>Routing Policy Name</b> | Lists the routing policy associated with the specified SIP entity |
| <b>Adaptation Name</b>     | Lists the name of the adaptation associated with the SIP entity   |

| Button      | Description                             |
|-------------|---|
| <b>Back</b> | Returns to the <b>SIP Entities</b> page |

**Related topics:**

[Displaying SIP Entity References](#) on page 1265

---

## Entity Links

### About Entity Links

Session Manager enables you to create an entity link between the Session Manager and any other administered SIP entity. You must configure an entity link between a Session Manager and any entity that you have administered if you want Session Manager to be able to send or receive messages from that entity directly. To be able to communicate with other SIP entities, each Session Manager instance must know the port and the transport protocol of its entity link to these SIP entities in the network. Session Manager does not need to know the port and transport protocol if the **Override Port & Transport** box is checked on the SIP entity. Port and transport must be administered even if the **Override Port & Transport** is checked on the SIP entity, although their values will not be used.

Routing entity links connect two SIP entities through the Session Manager. They enable you to define the network topology for SIP routing.

- Entity Links are configured to connect two SIP entities.
- Trusted Hosts are indicated by assigning the *Trust State* to the link that connects the entities.

## Creating Entity Links

---

1. On the System Manager console, select **Routing > Entity Links**.
  2. Click **New**.
  3. Enter the name in the **Name** field.
  4. Enter the SIP entity 1 by selecting the required **Session Manager** SIP entity from the drop-down list and provide the required port. SIP entity 1 must always be an Session Manager instance.  
The default port for TCP and UDP is 5060. The default port for TLS is 5061.
  5. Enter the SIP entity 2 by selecting the required non-Session Manager SIP entity from the drop-down list and provide the required port.  
The port is the port on which you have configured the remote entity to receive requests for the specified transport protocol.
  6. If the SIP entity is trusted, select the **Trusted** check box. Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
  7. Select the protocol you require for the link using the **Protocol** drop-down list.
  8. Click **Commit**.
- 

## Modifying entity links

---

1. On the System Manager console, select **Routing > Entity Links**.
2. Select an entity link for modification and click **Edit**.
3. Modify the name in the **Name** field if required.
4. If required, modify the SIP entity 1 by selecting the required **Session Manager** SIP entity 1 from the drop-down list and provide the required port.  
SIP entity 1 must always be a Session Manager instance.

5. If required, modify the SIP entity 2 by selecting the required SIP entity from the drop-down list and provide the required port.
  6. If you want to indicate that the link is a trusted link, select the **Trusted** check box.
  7. Select the transport protocol you require for the link using the **Protocol** drop-down list.
  8. Click **Commit**.
- 

## Deleting Entity Links

---

1. On the System Manager console, select **Routing > Entity Links**.
  2. To delete an existing link or links, select the respective check boxes and click **Delete**.
  3. Click **Delete** on the confirmation page.
- 

## Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of SIP entity links.

| Button        | Description   |
|---------------|---|
| <b>Delete</b> | Deletes the SIP entity link entries from the database.                            |
| <b>Cancel</b> | Cancel the deletion of SIP entity links and returns to the SIP entity Links page. |

## Entity Links field descriptions

Use this page to create, modify, delete, and manage entity links.

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Entity Links page that you can use to modify the entity link details. |
| <b>New</b>  | Opens the Entity Links page that you can use to create new entity links.        |

| Button   | Description  |
|--|--|
| <b>Duplicate</b>                                 | Creates a duplicate of the selected entity link and assigns a new state to it.   |
| <b>Delete</b>                                    | Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the entity link.                               |
| <b>More Actions &gt;<br/>Refresh all data</b>    | Refreshes all data. Any unsaved modifications are lost.  |
| <b>More Actions &gt;<br/>Import</b>              | Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.                    |
| <b>More Actions &gt;<br/>Export Entity Links</b> | Opens the Export Entity Links page that allows you to export the entity links data as an XML file to a specified location.           |
| <b>More Actions &gt;<br/>Export all data</b>     | Opens the Export all data page that allows you to export the data for all routing elements as a zipped file to a specified location. |
| <b>Commit</b>                                    | Distributes the selected entity links to all the Session Manager instances in the enterprise.  |

| Name                | Description   |
|---------------------|---|
| <b>Name</b>         | Name of the SIP entity link. This name must be unique and can have 3 to 64 characters.              |
| <b>SIP Entity 1</b> | Select a SIP entity from the drop-down list. This entity must always be a Session Manager instance. |
| <b>Port</b>         | Port to be used for SIP entity 1.   |
| <b>SIP Entity 2</b> | Select a SIP entity from the drop-down list. This entity need not be a Session Manager entity.      |
| <b>Port</b>         | Port to be used for SIP entity 2.   |
| <b>Trusted</b>      | Specifies that the link between the two SIP entities is trusted.                                    |
| <b>Protocol</b>     | Protocol to be used for the entity link.  |
| <b>Notes</b>        | Any details or notes that you wish to add.  |

## Bulk import for Entity Links

Please follow these rules when creating an XML bulk import file:

- The name of an Entity Link must be unique.
- <entityName1> , <entityName2> must refer to an existing SIP Entity with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Entity Link.
- The values in <transportProtocol> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.

**Example:**

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<entitylinkFullTOList>
  <EntitylinkFullTO>
    <notes></notes>
    <listenPortEntity1>5061</listenPortEntity1>
    <listenPortEntity2>5061</listenPortEntity2>
    <name>SessionManager1_BerlinCM_5061_TLS</name>
    <transportProtocol>TLS</transportProtocol>
    <trusted>true</trusted>
    <entityName1>SessionManager1</entityName1>
    <entityName2>BerlinCM</entityName2>
  </EntitylinkFullTO>
  <EntitylinkFullTO>
    <notes></notes>
    <listenPortEntity1>5061</listenPortEntity1>
    <listenPortEntity2>5061</listenPortEntity2>
    <name>NewYorkCM-SessionManager1-TLS</name>
    <transportProtocol>TLS</transportProtocol>
    <trusted>true</trusted>
    <entityName1>SessionManager1</entityName1>
    <entityName2>NewYorkCM</entityName2>
  </EntitylinkFullTO>
</entitylinkFullTOList>
```

---

## Time Ranges

### About the Time Ranges

Time ranges indicate when a particular rank or cost of a routing policy is to be used when determining the least-cost route. They do not indicate when routing policies are available to be considered for routing.

You must specify as many time ranges as necessary to cover all hours and days in a week for each administered routing policy.

For example, routing policy A can be in effect on all weekdays from 9:00 a.m. to 5:59 p.m., routing policy B can be in effect on all weekdays from 6:00 pm. to 9 a.m., and routing policy C time ranges can be in effect on weekends. These three time ranges together cover how calls should be routed throughout the week.

### Creating Time Ranges

You can use the Time Ranges screen to administer time ranges with start and end times.

- 
1. On the System Manager console, select **Routing > Time Ranges**.
  2. Click **New**.

3. Enter the name, select the required days by entering the start and end times and notes for the new time range. Start times start with the first second of the hour:minute. End Times go through the last second of the end hour:minute.
4. Click **Commit**.

---

**Related topics:**

[Time Range List field descriptions](#) on page 1273

## Modifying Time Ranges

---

1. On the System Manager console, select **Routing > Time Ranges**.
2. Select a time range for modification and click **Edit**.
3. If required, modify the name.
4. If required, modify the days by modifying the start and end times and notes. Start times start with the first second of the start hour:minute. End Times go through the last second of the end hour:minute.
5. Click **Commit**.

## Deleting Time Ranges

---

1. On the System Manager console, select **Routing > Time Ranges**.
2. To delete an existing time range or ranges, select the respective check boxes and click **Delete**.
3. Click **Delete** on the confirmation page.

---

**Related topics:**

[Delete Confirmation field descriptions](#) on page 1271

## Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of time ranges.

| Button        | Description   |
|---------------|---|
| <b>Delete</b> | Deletes the selected time ranges from the database. |
| <b>Cancel</b> | Cancel the deletion of the selected time ranges.    |

**Related topics:**

[Deleting Time Ranges](#) on page 1271

## Time Ranges field descriptions

Use this page to create, modify, delete, and manage time ranges.

| Field             | Description  |
|-------------------|--|
| <b>Name</b>       | Enter a name for the time range. It can have between three and 64 characters. The name cannot contain the following characters:<br><, >, ^, %, \$, @, #, * |
| Days (Mo to Su)   | Select the days of the week for which the time range should be used.   |
| <b>Start Time</b> | Start time for the time range. Use 24-hour time format.  |
| <b>End Time</b>   | End time for the time range. Use 24-hour time format.  |
| <b>Notes</b>      | Additional notes.  |

| Button                                      | Description  |
|---|--|
| <b>Edit</b>                                 | Opens the Time Ranges page that you can use to modify the time range details.  |
| <b>New</b>                                  | Opens the Time Ranges page that you can use to create new time ranges.   |
| <b>Duplicate</b>                            | Creates a duplicate of the selected time range and assigns a new state to it.  |
| <b>Delete</b>                               | Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the time range.                                |
| <b>More Actions &gt; Refresh all data</b>   | Refreshes all data. Any unsaved modifications are lost.  |
| <b>More Actions &gt; Import</b>             | Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.                    |
| <b>More Actions &gt; Export Time Ranges</b> | Opens the Export Time Ranges page that allows you to export the time ranges data as an XML file to a specified location.             |
| <b>More Actions &gt; Export all data</b>    | Opens the Export all data page that allows you to export data for all the routing entities as a zipped file to a specified location. |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Distributes the selected time range to all the Session Manager instances in the enterprise. |

## Time Range List field descriptions

Use this page to view time ranges associated to a routing policy.

| Name              | Description   |
|-------------------|---|
| <b>Name</b>       | Name of the time range. This name must be unique and can have between 3 and 64 characters. Select the check box to use the time range for a routing policy. |
| <b>Mon</b>        | Selected check box indicates that the time range is used for Mondays. Similarly, other days of the week for which the time range to be used are selected.   |
| <b>Start Time</b> | Start time for the time range. For a 24-hour time range, the start time is 0.00.  |
| <b>End Time</b>   | End time for the time range. For a 24-hour time range, the end time is 23:59.   |
| <b>Notes</b>      | Additional notes about the time range.  |

| Button        | Description   |
|---------------|---|
| <b>Select</b> | Associates the selected time range to the routing policy. |
| <b>Cancel</b> | Cancels the selection of the time range.                  |

### Related topics:

[Creating Time Ranges](#) on page 1270

## Bulk import for Time Ranges

Please follow these rules when creating an XML bulk import file:

The name of a Time Range must be unique and is referred to by other elements.

### Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<timerangeFullTOList>
  <TimerangeFullTO>
    <notes>this is a test</notes>
    <includesFriday>true</includesFriday>
    <includesMonday>true</includesMonday>
    <includesSaturday>>false</includesSaturday>
    <includesSunday>>false</includesSunday>
    <includesThursday>true</includesThursday>
    <includesTuesday>true</includesTuesday>
  </TimerangeFullTO>
</timerangeFullTOList>
```

```
<includesWednesday>true</includesWednesday>
<name>regularweek</name>
<startTime>00:00:00</startTime>
<stopTime>23:59:00</stopTime>
</TimerangeFullTO>
<TimerangeFullTO>
  <notes></notes>
  <includesFriday>false</includesFriday>
  <includesMonday>false</includesMonday>
  <includesSaturday>true</includesSaturday>
  <includesSunday>true</includesSunday>
  <includesThursday>false</includesThursday>
  <includesTuesday>false</includesTuesday>
  <includesWednesday>false</includesWednesday>
  <name>weekend</name>
  <startTime>00:00:00</startTime>
  <stopTime>23:59:00</stopTime>
</TimerangeFullTO>
<TimerangeFullTO>
  <notes>Time Range 24/7</notes>
  <includesFriday>true</includesFriday>
  <includesMonday>true</includesMonday>
  <includesSaturday>true</includesSaturday>
  <includesSunday>true</includesSunday>
  <includesThursday>true</includesThursday>
  <includesTuesday>true</includesTuesday>
  <includesWednesday>true</includesWednesday>
  <name>24/7</name>
  <startTime>00:00:00</startTime>
  <stopTime>23:59:00</stopTime>
</TimerangeFullTO>
</timerangeFullTOList>
```

---

## Routing Policies

### About Routing Policies

Use the Routing Policies page to create and modify routing policies.

All “ Routing Policies” together form the “enterprise wide dial plan”.

Routing Policies can include the “Origination of the caller”, the “dialed digits” of the called party, the “domain” of the called party and the actual time the call occurs.

Optionally, instead of “dialed digits” of the called party and the “domain” of the called party a “regular expression” can be defined.

Depending on one or multiple of the inputs mentioned above a destination where the call should be routed is determined.

Optionally, the destination can be qualified by “deny” which means that the call will not be routed.

Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

## Creating Routing Policies

---

1. On the System Manager console, select **Routing > Policies**.
  2. Click **New**.
  3. Enter a routing policy name and notes in the relevant fields in the General section. Note that the routing policy can be disabled by selecting the **Disabled** check box.
  4. Click **Select** under the SIP Entities as Destination section. This is where you can select the destination SIP entity for this routing policy.
  5. Select the required destination and click **Select**.
  6. If you need to associate the Time of Day routing parameters with this Routing Policy, click **Add** from the Time of Day section.
  7. Select the Time of Day patterns that you want to associate with this routing pattern and press **Select**.  
If there are gaps in the Time of Day coverage that you select, Session Manager displays a warning message. If such gaps exist in the Time of the Day coverage, randomness in routing selections may be observed
  8. Enter the relative Rankings that you would like associated with each Time Range. Lower ranking values indicate higher priority.
  9. Under Dial Patterns or Regular Expressions, click **Add** to associate existing Dial Patterns and Regular Expressions with the Routing Policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**.  
This field can be left blank; the routing policy can be added to the dial pattern or regular expression when you add it.
  10. Under Dial Patterns or Regular Expressions, click **Remove** to dissociate existing Dial Patterns and Regular Expressions with the Routing Policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**. This field can be left blank; the routing policy can be added to the dial pattern or regular expression when you add it.
  11. Click **Commit**.
- 

### Related topics:

[Routing Policy Details field descriptions](#) on page 1278

## Modifying Routing Policies

---

1. On the System Manager console, select **Routing > Policies**. The Routing Policies screen is displayed.
  2. Select a routing policy for modification and click **Edit**.
  3. If required, modify the routing policy name and notes in the relevant fields in the General section. Note that the routing policy can be disabled by selecting the **Disabled** check box.
  4. Click **Select** under the SIP entities as Destination section. This is where you can select the destination SIP entity for this routing policy.
  5. If required, select or modify the required destination and click **Select**.
  6. If you need to associate the Time of Day routing parameters with this Routing Policy, click **Add** from the Time of Day section.
  7. Select the Time of Day patterns that you want to associate with this routing pattern and press **Select**.
  8. Enter the relative rankings that you would like associated with each Time Range. Lower ranking values indicate higher priority.
  9. If you need to dissociate the Time of Day routing parameters from this Routing Policy, click **Remove** from the Time of Day section.
  10. Under Dial Patterns or Regular Expressions, click **Add** to associate existing Dial Patterns and Regular Expressions with the Routing Policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**.  
If you have not specified the dial patterns or regular expressions yet, you can add the routing policy to the dial pattern or regular expression when you add them later.
  11. Under Dial Patterns or Regular Expressions, click **Remove** to dissociate existing Dial Patterns and Regular Expressions with the Routing Policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**.
  12. Click **Commit**.
-

## Deleting Routing Policies

1. On the System Manager console, select **Routing > Policies**.
2. To delete an existing routing policy or routing policies, select the respective check boxes and click **Delete**.
3. Click **Delete** on the confirmation page.

 **Note:**

If you delete a routing policy, all dial patterns and regular expressions that are linked only to this routing policy are also deleted.

### Related topics:

[Delete Confirmation field descriptions](#) on page 1277

## Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of the routing policy.

| Button        | Description  |
|---------------|--|
| <b>Delete</b> | Deletes the selected routing policy as well as any dial patterns and regular expressions that are associated <i>only</i> with this routing policy. |
| <b>Cancel</b> | Cancels the deletion of the routing policy.  |

### Related topics:

[Deleting Routing Policies](#) on page 1277

## Routing Policies field descriptions

Use this page to create, modify, delete, and manage routing policies.

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the Routing Policy Details page that you can use to modify the routing policy.   |
| <b>New</b>  | Opens the Routing Policy Details page that you can use to create a new routing policy. |

| Button   | Description  |
|--|--|
| <b>Duplicate</b>                                 | Creates a duplicate of the selected routing policy and assigns a new state to it.  |
| <b>Delete</b>                                    | Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the routing policy.                            |
| <b>More Actions &gt; Refresh all data</b>        | Refreshes all data. Any unsaved modifications are lost.  |
| <b>More Actions &gt; Import</b>                  | Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.                    |
| <b>More Actions &gt; Export Routing Policies</b> | Opens the Export Routing Policies page that allows you to export the routing policy data as an XML file to a specified location.     |
| <b>More Actions &gt; Export all data</b>         | Opens the Export all data page that allows you to export data for all the routing entities as a zipped file to a specified location. |
| <b>Commit</b>                                    | Distributes the selected routing policy to all the Session Manager instances in the enterprise.                                      |

## Routing Policy Details field descriptions

Use this page to specify the details for creating or modifying a routing policy.

### General section

| Name            | Description  |
|-----------------|--|
| <b>Name</b>     | Name of the routing policy.  |
| <b>Disabled</b> | Selecting this check box specifies that the routing policy is to be disabled and should not be used. |
| <b>Notes</b>    | Additional notes about the routing policy.   |

### SIP Entity as Destination section

| Button        | Description  |
|---------------|--|
| <b>Select</b> | Opens the SIP entity List page. You can use this page to select a SIP entity as a destination and associate it to the selected routing policy. |

### Time of Day section

| Button     | Description  |
|------------|--|
| <b>Add</b> | Adds a new time of the day to the selected routing policy. |

| Button                    | Description   |
|---------------------------|---|
| <b>Remove</b>             | Removes the selected time of day entry from the selected routing policy.  |
| <b>View Gaps/Overlaps</b> | Selecting a time of day entry and selecting <b>View Gaps/Overlaps</b> generates a Duration Lists report and displays if there are any gaps or overlaps in the time of day entries for each day of the week. |

### Dial Patterns section

| Button        | Description   |
|---------------|---|
| <b>Add</b>    | Adds a new dial pattern to the selected routing policy.             |
| <b>Remove</b> | Removes the selected dial pattern from the selected routing policy. |

### Regular Expressions section

| Button        | Description   |
|---------------|---|
| <b>Add</b>    | Adds a new regular expression to the selected routing policy.             |
| <b>Remove</b> | Removes the selected regular expression from the selected routing policy. |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Saves the routing policy changes and distributes those to the Session Manager instances in the enterprise. |
| <b>Cancel</b> | Cancel modifications to the routing policy.  |

### Related topics:

[Creating Routing Policies](#) on page 1275

## Routing Policy List field descriptions

Use this page to select a routing policy that the regular expression should be associated with.

| Name               | Description   |
|--------------------|---|
| <b>Name</b>        | Name of the routing policy to be associated with the selected regular expression.                 |
| <b>Disabled</b>    | Denotes that the associated routing policy is to be disabled for the selected regular expression. |
| <b>Destination</b> | Destination SIP entity for the routing policy.  |
| <b>Notes</b>       | Additional notes about the routing policy.  |

| Button | Description  |
|--------|--|
| Select | Confirms the selection of the routing policy for associating it with the regular expression. |
| Cancel | Cancel the selection of the routing policy.  |

## Bulk import for Routing Policies

Please follow these rules when creating an XML bulk import file:

- The name of a routing policy <referred to as routing policy> is unique and is referred to by other elements.
- <sipentityName> must refer to an existing SIP element with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Routing Policy.
- Multiple time of day entries (<timeofdayNames>) can be configured for one Routing Policy.

<timerangeName> must refer to an existing Time Range with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Routing Policy.

### Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<routingpolicyFullTOList>
  <RoutingpolicyFullTO>
    <notes>this is a test</notes>
    <disabled>>false</disabled>
    <name>toBerlin</name>
    <sipentityName>BerlinCM</sipentityName>
    <timeofdayNames>
      <rank>1</rank>
      <timerangeName>regularweek</timerangeName>
    </timeofdayNames>
    <timeofdayNames>
      <rank>0</rank>
      <timerangeName>24/7</timerangeName>
    </timeofdayNames>
  </RoutingpolicyFullTO>
</routingpolicyFullTOList>
```

---

## Dial Patterns

### About Dial Patterns

A dial pattern specifies which routing policy or routing policies are used to route a call based on the digits dialed by a user which match that pattern. Session Manager matches these dialed digits after applying any administered ingress adaptation.

The originating location of the call and the domain in the request-URI also determine how the call gets routed.

Session Manager tries to match the request-URI of a request to a row in the dial pattern table. The rows considered for the match are all rows where:

- The domain in the dial pattern table matches the domain in the request-URI, and,
- The originating location in the dial pattern table row matches the originating location of the request, or, if there are no rows matching the originating location, the originating location in the table is set to -ALL-, or, if there was no originating location, the originating location in the table is -ALL-, and
- The digit pattern in the row matches the user-part of the request-URI, ignoring any parameters that are in the user part of the request-URI

If no rows match using the above criteria, Session Manager modifies the domain in the request URI to remove one level of subdomain. For example, if `us.yourcompany.com` was tried, then Session Manager tries `yourcompany.com`.

As another example, you have two Communication Manager instances. Each Communication Manager has a call number range including all direct inward dialing (DID) numbers. Any user on CM-1 has a dial pattern `+1301501xxxx`. Similarly, any user on CM-2 has a dial pattern `+1301601xxxx`. You would enter the 2 dial patterns as:

- CM-1: `+1301501`
- CM-2: `+1301601`

A call to `+13015016789` would match the dial pattern for CM-1.

A call to `+13016011234` would match the dial pattern for CM-2.

The pattern matching algorithm works as follows:

- Valid digits are 0-9
- Valid characters for the leading position are `+`, `*`, and `#`. Any other characters are not matched.
- `x` (lowercase only) is a wildcard character that matches a character from the allowed characters above. White spaces are not allowed.

- Longer matches get a higher priority over shorter matches. For example, +1601555 has a higher priority as compared to +1601.
- For matches of equal length, exact matches have a higher priority over wildcard matches. For example, +1601555 has a higher priority as compared to +1xxx555.
- For both routing policies and adaptations, the pattern matching works in the same manner.

## Creating Dial Patterns

The Dial Patterns screen is used to create Dial Patterns and associate the Dial Patterns to a Routing Policy and Locations.

- 
1. On the System Manager console, select **Routing > Dial Patterns**.
  2. Click **New**. The Dial Pattern Details screen is displayed.
  3. Enter the Dial Pattern General information in the General section. Note that a Domain can be provided to restrict the Dial Pattern to the specified Domain.
  4. Click **Add** under the Originating Locations and Routing Policies section.
  5. Select all the required Locations and Routing Policies that you want associated with the Dial Pattern by selecting the check box in front of each item.
  6. Click **Select** to indicate that you have completed your selections.
  7. If you need to specify that calls from the specified locations will be denied, click **Add** under the Denied Locations section.
  8. Select all the Locations that are to be denied and click **Select** to indicate that you have completed your selections.
  9. Click **Commit**.



**Note:**

You cannot save a dial pattern unless you add at least a routing policy or a denied location.

---

**Related topics:**

[Dial Pattern Details field descriptions](#) on page 1285

## Modifying Dial Patterns

---

1. On the System Manager console, select **Routing > Dial Patterns**.
2. Select a dial pattern for modification and click **Edit**. The Dial Pattern Details screen is displayed.
3. Enter the Dial Pattern General information in the General section. Note that a Domain can be provided to restrict the Dial Pattern to the specified Domain.
4. Click **Add** under the Locations and Routing Policies sections one after the other.
5. Select all the required Locations and Routing Policies that you want associated with the Dial Pattern by selecting the check box in front of each item.
6. Click **Select** to indicate that you have completed your selections.
7. Similarly, to remove locations, click **Remove**, select the locations to remove, and click **Select**.
8. If you need to specify that calls from the specified locations will be denied, click **Add** under the Denied Locations section.
9. Select all the Locations that are to be denied and click **Select** to indicate that you have completed your selections.
10. Similarly, to remove locations from the denied list, click **Remove**, select the locations to remove, and click **Select**.
11. Click **Commit**.

**Note:**

You cannot save a dial pattern unless it has at least one routing policy or a denied location associated to it.

---

## Deleting Dial Patterns

---

1. On the System Manager console, select **Routing > Dial Patterns**.
2. To delete an existing dial pattern or patterns, select the respective check boxes and click **Delete**.
3. Click **Delete** on the confirmation page.



**Note:**

When you delete a Dial Pattern, it is also deleted from all the Routing Policies that it is associated to.

**Related topics:**

[Dial Pattern Details field descriptions](#) on page 1285

## Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of selected dial patterns.

| Button        | Description   |
|---------------|---|
| <b>Delete</b> | Deletes entries for the selected dial patterns from the database. |
| <b>Cancel</b> | Cancels the deletion of the selected dial patterns.               |

## Dial Patterns field descriptions

Use this page to create, modify, delete, and manage dial patterns.

| Button                                       | Description   |
|--|---|
| <b>Edit</b>                                  | Opens the Dial Pattern Details page that you can use to modify the dial pattern details.                          |
| <b>New</b>                                   | Opens the Dial Pattern Details page that you can use to create new dial patterns.                                 |
| <b>Duplicate</b>                             | Creates a duplicate of the selected dial pattern and assigns a new state to it.                                   |
| <b>Delete</b>                                | Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the dial pattern.           |
| <b>More Actions &gt; Refresh all data</b>    | Refreshes all data. Any unsaved modifications are lost.   |
| <b>More Actions &gt; Dial Pattern Report</b> | Displays Dial Patterns and the corresponding Locations, Routing Policies and Domains.                             |
| <b>More Actions &gt; Import</b>              | Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files. |

| Button   | Description   |
|--|---|
| <b>More Actions &gt; Import Provider Specific Data</b> | Opens the Import Provider Specific Data page that allows you to import provider—specific data from a file that you can specify by browsing. |
| <b>More Actions &gt; Export Dial Patterns</b>          | Opens the Export Dial Patterns page that allows you to export the dial patterns data as an XML file to a specified location.                |
| <b>More Actions &gt; Export Provider Specific Data</b> | Opens the Export Provider Specific Data page that allows you to export provider-specific data as an XML file to a specified location.       |
| <b>More Actions &gt; Export all data</b>               | Opens the Export all data page that allows you to export data for all the routing entities as a zipped file to a specified location.        |
| <b>Commit</b>  | Distributes the selected dial pattern to all the Session Manager instances in the enterprise.   |

## Dial Pattern Details field descriptions

Use this page to specify the dial pattern details.

### General section

| Name                  | Description  |
|-----------------------|--|
| <b>Pattern</b>        | Dial pattern to match. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.  |
| <b>Min</b>            | Minimum number of digits to be matched.  |
| <b>Max</b>            | Maximum number of digits to be matched.  |
| <b>Emergency Call</b> | <p>Indicate if it is an emergency call.</p> <p> <b>Note:</b><br/>Some of the important constraints on the use of this feature are as follows</p> <ul style="list-style-type: none"> <li>• Each location should be assigned to only one emergency dial number.</li> <li>• This emergency dial number must match the emergency dial number in the 96xx settings file for all SIP phones in the identified location. Failure to follow this guideline can result in users being unable to dial emergency numbers.</li> </ul> |
| <b>SIP Domain</b>     | Domain for which you want to restrict the dial pattern.  |
| <b>Notes</b>          | Other details that you wish to add.  |

### Locations and Routing Policies section

| Name                              | Description   |
|-----------------------------------|---|
| <b>Select check box</b>           | Use this check box to select and use the digit conversion for the incoming calls. |
| <b>Location Name</b>              | Name of the location to be associated to the dial pattern.                        |
| <b>Location Notes</b>             | Notes about the selected location.  |
| <b>Routing Policy Name</b>        | Name of the routing policy to be associated to the dial pattern.                  |
| <b>Routing Policy Disabled</b>    | Name of the routing policy that should not be used for the dial pattern.          |
| <b>Routing Policy Destination</b> | Destination of the routing policy.  |
| <b>Routing Policy Notes</b>       | Any other notes about the routing policy that you wish to add.                    |

### Denied Locations section

| Name                    | Description   |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select denied locations for the dial pattern match. |

| Button        | Description   |
|---------------|---|
| <b>Add</b>    | Adds locations, routing policies, or denied locations for the dial patterns.                            |
| <b>Remove</b> | Removes locations, routing policies, or denied locations for the dial patterns.                         |
| <b>Commit</b> | Saves the dial pattern details and distributes them to the Session Manager instances in the enterprise. |
| <b>Cancel</b> | Cancel changes to the dial pattern details and returns to the Dial Patterns page.                       |

### Related topics:

[Creating Dial Patterns](#) on page 1282

[Deleting Dial Patterns](#) on page 1283

### Pattern List field descriptions

Use this page to view the dial pattern details for associating with the routing policy

| Name           | Description   |
|----------------|---|
| <b>Pattern</b> | Dial pattern to match. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern. |
| <b>Min</b>     | Minimum number of digits to be matched.   |

| Name                  | Description  |
|-----------------------|--|
| <b>Max</b>            | Maximum number of digits to be matched.  |
| <b>Emergency Call</b> | Indicate if it is an emergency call.<br><br> <b>Note:</b><br>Some of the important constraints on the use of this feature are as follows <ul style="list-style-type: none"> <li>• Each location should be assigned to only one emergency dial number.</li> <li>• This emergency dial number must match the emergency dial number in the 96xx settings file for all SIP phones in the identified location. Failure to follow this guideline can result in users being unable to dial emergency numbers.</li> </ul> |
| <b>Domain</b>         | Domain for which you want to restrict the dial pattern.  |
| <b>Notes</b>          | Other details that you wish to add.  |

| Button        | Description   |
|---------------|---|
| <b>Select</b> | Associate the selected pattern to the routing policy.                 |
| <b>Cancel</b> | Cancel the association of the selected pattern to the routing policy. |

## Bulk Import for Dial Patterns

Please follow these rules when creating an XML bulk import file:

- A dial pattern is identified by a combination of 5 elements below. This combination must be unique for each dial pattern.
  - <digitpattern>
  - <maxdigits>
  - <mindigits>
  - <sipdomainName>
  - <routingoriginationName>
- <sipdomainName> must refer to an existing domain with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the dial pattern.
- <routingpolicyNames> must refer to existing Routing Policies with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Dial pattern.
- <routingpolicyNames> must exist if <deny> is false.
- <routingpolicyNames> must exist if <deny> is true.

**Example:**

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<digitmapFullTOList>
  <DigitmapFullTO>
    <notes>this is a test</notes>
    <deny>true</deny>
    <digitpattern>123</digitpattern>
    <maxdigits>36</maxdigits>
    <mindigits>3</mindigits>
    <routingoriginName>New York</routingoriginName>
    <routingpolicyNames>toBerlin</routingpolicyNames>
    <sipdomainName>avaya.com</sipdomainName>
    <treatasemergency>true</treatasemergency>
  </DigitmapFullTO>
  <DigitmapFullTO>
    <notes>this is a test</notes>
    <deny>false</deny>
    <digitpattern>123</digitpattern>
    <maxdigits>36</maxdigits>
    <mindigits>3</mindigits>
    <routingoriginName>Berlin</routingoriginName>
    <routingpolicyNames>toBerlin</routingpolicyNames>
    <sipdomainName>avaya.com</sipdomainName>
    <treatasemergency>true</treatasemergency>
  </DigitmapFullTO>
</digitmapFullTOList>
```

---

## Regular Expressions

### About Regular Expressions

You can configure routing in Session Manager by creating regular expressions and associating them with a routing policy.

Regular expression syntax is based on Perl version 5.8.

The asterisk character "\*" matches any character string.

The dot character "." matches one character.

The backslash character "\" makes a character lose its special meaning, if any

Some examples are:

- For "www.sipentity.domain.com", use the string "www\\.sipentity\\.domain\\.com"
- For "192.14.11.22", use string "192\\.14\\.11\\.22".
- The routing policy with a regular expression `.*@.*\\.de` routes all calls requesting a domain in Germany (for example, name@company.de) to a Frankfurt Gateway.

## Creating Regular Expressions

The Regular Expressions screen enables you to create regular expressions and associate them with routing policies. You cannot save a regular expression unless it has a routing policy associated to it.

- 
1. On the System Manager console, select **Routing > Regular Expressions**.
  2. Click **New**. The Regular Expression Details screen is displayed.
  3. Enter the regular expression pattern in the **Pattern** field.
  4. Specify a rank order for the regular expression. A lower rank order indicates a higher priority.
  5. To deny routing for a matched regular expression pattern, select the **Deny** check box.
  6. To associate a routing policy for the matched pattern, click **Add** under the Routing Policy section.
  7. Select the required routing policies that you want associated with the Regular Expression by selecting the respective check boxes.
  8. Click **Select** to indicate that you have completed your selections.
  9. To remove an associated routing policy, select the routing policy and click **Remove**.
  10. Click **Commit**.
- 

## Modifying Regular Expressions

The Regular Expressions screen enables you to modify regular expressions and associate them with routing policies.

- 
1. On the System Manager console, select **Routing > Regular Expressions**. The Regular Expressions screen is displayed.
  2. Select a regular expression from the list and click **Edit**. The Regular Expression Details screen is displayed.
  3. Modify the regular expression pattern in the **Pattern** field, if required.
  4. If required, modify the rank order for the regular expression. A lower rank order indicates a higher priority.

5. To allow or deny routing for a matched regular expression pattern, select or clear the **Deny** check box.
6. To associate a routing policy for the matched pattern, click **Add** under the Routing Policy section.
7. Select the required routing policies that you want associated with the Regular Expression by selecting the respective check boxes.
8. Click **Select** to indicate that you have completed your selections.
9. To remove an associated routing policy, select the routing policy and click **Remove**.
10. Click **Commit**.



**Note:**

You cannot save a regular expression unless it has a routing policy associated to it.

---

## Deleting Regular Expressions

Deleting a regular expression deletes it from all of the routing policies that it is associated with.

- 
1. On the System Manager console, select **Routing > Regular Expressions**.
  2. To delete existing regular expressions, select the respective check boxes and click **Delete**.
  3. Click **Delete** on the confirmation page.
- 

## Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of the regular expression.

| Button        | Description   |
|---------------|---|
| <b>Delete</b> | Confirms the deletion of the regular expression and also deletes the regular expression from the routing policy that it is associated to. |
| <b>Cancel</b> | Cancels the deletion of the regular expression.   |

## Regular Expressions field descriptions

Use this page to create, modify, delete, and manage regular expressions.

| Button  | Description  |
|---|--|
| <b>Edit</b>   | Opens the Regular Expression Details page that you can use to modify the regular expressions.  |
| <b>New</b>  | Opens the Regular Expression Details page that you can use to create new regular expressions.  |
| <b>Duplicate</b>                                    | Creates a duplicate of the selected regular expression and assigns a new state to it.  |
| <b>Delete</b>                                       | Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the regular expression.                            |
| <b>More Actions &gt; Refresh all data</b>           | Refreshes all data. Any unsaved modifications are lost.  |
| <b>More Actions &gt; Import</b>                     | Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.                        |
| <b>More Actions &gt; Export Regular Expressions</b> | Opens the Export Regular Expressions page that allows you to export the regular expressions data as an XML file to a specified location. |
| <b>More Actions &gt; Export all data</b>            | Opens the Export all data page that allows you to export data for all entities as a zipped file to a specified location.                 |
| <b>Commit</b>                                       | Distributes the selected regular expressions to all the Session Manager instances in the enterprise.                                     |

## Regular Expression Details field descriptions

Use this page to specify the regular expression details.

### General

| Name           | Description  |
|----------------|--|
| <b>Pattern</b> | Regular expression pattern that Session Manager tries to match. Allowed characters are A-Z a-z 0-9 @ - _ and meta characters are - [ ] ( ) { }   ? : + * ^ \$ . \ . For example, <ul style="list-style-type: none"> <li>• miller@company.com</li> <li>• company.org</li> <li>• .*@company.com</li> </ul> |

| Name              | Description  |
|-------------------|--|
| <b>Rank Order</b> | Priority of the pattern. A lower rank order means higher priority. |
| <b>Deny</b>       | Denies routing for a matched regular expression pattern.           |
| <b>Notes</b>      | Additional notes about the regular expression pattern.             |

| Button        | Description  |
|---------------|--|
| <b>Add</b>    | Associates a routing policy for the matched pattern.                                       |
| <b>Remove</b> | Dissociates a routing policy from the matched pattern.                                     |
| <b>Commit</b> | Saves the regular expression and distributes it to the Session Managers in the enterprise. |
| <b>Cancel</b> | Cancels the creation or modification of the regular expression.                            |

## Regular Expression List field descriptions

Use this page to view the regular expression associated with the selected routing policy.

| Name                      | Description   |
|---------------------------|---|
| <b>Regular Expression</b> | Displays the regular expression to be used for the selected routing policy.   |
| <b>Rank Order</b>         | Priority of the regular expression. Lower rank order means a higher priority. |
| <b>Deny</b>               | Denies routing for a matched regular expression.                              |
| <b>Notes</b>              | Additional notes for the regular expression.                                  |

| Button        | Description  |
|---------------|--|
| <b>Select</b> | Associates the selected regular expression to a routing policy or dissociates it based on the Add or Remove option selected earlier. |
| <b>Cancel</b> | Cancels the association or dissociation of the regular expression.   |

## Bulk import for Regular Expressions

Please follow these rules when creating an XML bulk import file:

- The pattern of a Regular Expression referred to as <regexpmap> must be unique.
- <routingpolicyNames> must refer to an existing Routing Policy with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Regular Expression.
- Multiple Routing Policy entries (<routingpolicyNames>) can be configured for one Regular Expression.

### Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<regexpmapFullTOList>
  <RegexpmapFullTO>
    <notes>this is a test</notes>
    <deny>>false</deny>
    <pattern>*.com</pattern>
    <rankorder>0</rankorder>
    <routingpolicyNames>toBerlin</routingpolicyNames>
  </RegexpmapFullTO>
</regexpmapFullTOList>
```

---

## Defaults

### Modifying the default settings

You can use the Defaults screen to change the default values or ranges for parameters that are used by the other Routing menu options

These values are used as defaults values of admin personal settings when creating new Routing entities. Modifying these values does not change the values of already created entities .

1. On the System Manager console, select **Routing > Defaults**. The Personal Settings screen is displayed.
2. Under **Adaptations**, specify the minimum and maximum number of characters for pattern matching. The default minimum and maximum values are 1 and 36 respectively.
3. Under **Dial Patterns**, specify the minimum and maximum length for dial pattern. These values are used by the **Dial Patterns** option. The default minimum and maximum values are 1 and 36 respectively.

4. Under **Entity Links**, specify the port number to be used as a listen port. The default port is 5060.
5. Under **Domain Management**, specify a domain suffix.
6. Under **SIP Entities**, specify the following:
  - a. Select the default SIP entity type from the **Type** drop-down menu. The default type is Session Manager.
  - b. Select the default time zone from the **Time Zone** pull-down menu. The default time zone is America/Denver.
  - c. Select the default transport protocol for ports. The default protocol is TLS.
  - d. With entity links from both the Session Manager instances, checking the **Override Port & Transport with DNS SRV** check box on the SIP entity form indicates that both the Port and Protocol (Transport) on the SIP entity form are ignored.
    - If you select the check box, the port and transport administered in the local host name resolution table is used, which could override the entity link.
    - If the FQDN is not in the local table and DNS is consulted, if you have not selected the check box, only an A-Record lookup is done in DNS to resolve the host name to an IP address. Transport and port specified in the entity link are used. If you selected the check box, a full DNS lookup (as described in RFC 3263) is done, and the transport and port specified in the entity link could be overridden.
7. Under **Time Ranges**, specify the default start time and end time for the time range. The default is to use a 24-hour time range, that is, the start time is 00:00 hours and the end time is 23:59 hours.
8. Under **Application Settings**, select the **Show warning message** check box to get a warning message if you try to navigate to another page when a page has unsaved data or when data import is in progress.
9. Click **Apply** to save the changes.

---

**Related topics:**

[Default Settings field descriptions](#) on page 1294

## Default Settings field descriptions

Use this page to specify default settings for all the Routing menus on the right-hand side pane and to save them as your default personal settings.

| Name   | Description  |
|--|--|
| <b>Adaptations</b>                                 |  |
| <b>Matching Pattern Min Length</b>                 | Minimum length of pattern matched for adaptations. The minimum value can be 1.   |
| <b>Matching Pattern Max Length</b>                 | Maximum length of pattern matched for adaptations. The maximum value can be 36.  |
| <b>Dial Patterns</b>                               |  |
| <b>Dial Pattern Min Length</b>                     | Minimum length of dial pattern to be matched. The minimum value can be 1.  |
| <b>Dial Pattern Max Length</b>                     | Maximum length of dial pattern to be matched. The maximum value can be 36.   |
| <b>Entity Links</b>                                |  |
| <b>Listen Port</b>                                 | Number of the port to be used for entity links. The default port is 5060.  |
| <b>Default Transport Protocol for Entity Links</b> | The default transport protocol that the entity links use, such as TLS, TCP, or UDP. The default is TLS.  |
| <b>Domain Management</b>                           |  |
| <b>Suffix</b>                                      | The default suffix to be used for the domain name.   |
| <b>SIP Entities</b>                                |  |
| <b>Type</b>  | Type of the SIP entity, such as ASM, CM, Trunk, Gateway, and so on. The default is ASM.  |
| <b>Time Zone</b>                                   | Default time zone to be used for the entity link.  |
| <b>Default Transport Protocol for Ports</b>        | Default transport protocol to be used by the ports. The default is TLS.  |
| <b>Use DNS Routing</b>                             | Select check box to use DNS routing.   |
| <b>Time Ranges</b>                                 |  |
| <b>Time Range Start Time</b>                       | Start time for the time range. Default is 00:00  |
| <b>Time Range End Time</b>                         | End time for the time range. Default is 23:59.   |
| <b>Application Settings</b>                        |  |
| <b>Show warning message</b>                        | Displays a warning message if you try to navigate to another page when the displayed page has unsaved data or if a data import is on progress. |

| Button                  | Description   |
|-------------------------|---|
| <b>Restore Defaults</b> | Restores vendor defaults.                             |
| <b>Revert</b>           | Reverts to settings before the last applied settings. |

| Button | Description                                      |
|--------|--|
| Apply  | Saves and applies the modified default settings. |

**Related topics:**

[Modifying the default settings](#) on page 1293

# Chapter 13: Managing System Manager Data

---

## Administering backup and restore

---

### Backup and Restore

The backup and restore functions are executed on the System Manager. These functions allow you to backup and restore configuration data for the System Manager and all of the Session Manager instances. All of the configuration data for the entire system is kept centrally on the System Manager. This means that individual backups of the Session Manager instances are not needed. After a restore operation, the restored configuration data is automatically propagated to the Session Manager instances.

Associated actions include configuring data retention rules for specifying how long the backup files should remain on the system, and modifying logger and appender information.

---

### Viewing list of backup files

---

On the System Manager console, click **System Manager Data > Backup and Restore** in the left navigation pane.

---

#### Result

The Backup and Restore page displays the list of backup files.

## Creating a data backup on a local computer

---

1. On the System Manager console, click **System Manager Data > Backup and Restore** in the left navigation pane.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local**.
4. In the **File name** field, enter the file path and name of the backup file that you want to create.
5. Click **Now**.

---

### Result

If the backup is successful, the Backup and Restore page displays a message Backup created successfully!!.

---

## Scheduling a data backup on a local computer

---

1. On the System Manager console, click **System Manager Data > Backup and Restore** in the left navigation pane.
  2. On the Backup and Restore page, click **Backup**.
  3. On the Backup page, Click **Local** option.
  4. In the **File name** field, enter the name of the backup file that you want to create.
  5. Click **Schedule**.
  6. Click **Commit**.
-

---

## Restoring a data backup from a local machine

- 
1. On the System Manager console, click **System Manager Data > Backup and Restore** in the left navigation pane.
  2. On the Backup and Restore page, click **Restore**.
  3. On the Restore page, click **Local**.
  4. In the **Select File Name** field, click the file name that you want to restore.
  5. Click **Restore**.
  6. On the Restore Confirmation page, click **Continue**.

---

### Result

After the backup data is successfully restored, the system logs you out of the System Manager console.

---

## Viewing data retention rules

---

On the System Manager console, click **System Manager Data > Data Retention** in the left navigation pane.

---

### Result

The Data Retention page displays the data retention rules.

### Related topics:

[Data Retention field descriptions](#) on page 1306

---

## Modifying data retention rules

- 
1. On the System Manager console, click **System Manager Data > Data Retention** in the left navigation pane.
  2. Click the option button to select a rule.

3. Click **Edit**.
4. Modify the value in the **Retention Interval (Days)** field.
5. Click **Update** to save the value.

---

**Related topics:**

[Data Retention field descriptions](#) on page 1306

---

## Accessing the Data Retention Rules service

1. Log in to the System Manager web interface as an administrator.
2. On the System Manager console, click **System Manager Data > Data Retention** in the left navigation pane.  
The system displays the Data Retention page.

---

## Viewing loggers for a log file

1. On the System Manager console, click **Events > Logs > Log Settings** in the left navigation pane.
2. On the Logging Configuration page, click a log file from the **Select Log File** field.

---

**Result**

You can view the loggers in the Logger List section.

**Related topics:**

[Logging Settings field descriptions](#) on page 1109

---

## Assigning an appender to a logger

The appender where logger logs the log messages.

- 
1. On the System Manager console, click **Events > Logs > Log Settings** in the left navigation pane.
  2. On the Log Settings page, select a log file from the **Select Log File** field.
  3. Click a logger in the **Logger List** section.
  4. Click **Edit**.
  5. On the Edit logger page, click **Attach** in the **Attached Appenders** section.
  6. On the Attach Appender page, click an appender in the **Select Appender** field.
  7. Click **Commit**.  
The appender is added to the selected logger and you can view the appender on the Log Settings page.

---

**Related topics:**

[Attach Appender field descriptions](#) on page 1114

---

## Editing a logger in a log file

You can set log levels for loggers which define as to what level of logging the logger logs.

- 
1. On the System Manager console, click **Events > Logs > Log Settings** in the left navigation pane.
  2. On the Log Settings page, select a log file from the **Select Log File** field.
  3. Click a logger in the **Logger List** section.
  4. Click **Edit**.
  5. On the Edit logger page, in the **Log Level** field select a log level.
  6. Click **Commit**.  
The log level is set for the selected logger.

---

**Related topics:**

[Edit Logger field descriptions](#) on page 1112

---

## Modifying an appender

1. On the System Manager console, click **Events > Logs > Log Settings** in the left navigation pane.
2. On the Logging Configuration page, click a log file from the **Select Log File** field.
3. Click a logger in the **Logger List** section.
4. Click **Edit**.
5. On the Edit logger page, click an appender in the **Attached Appendors** section.
6. Click **Edit**.
7. On the Edit Appender page modify the appender information.



**Note:**

You can modify information in the following fields: **Threshold Log Level**, **Max File Size**, **File Path**, and **Number Of Backup Files**.

8. Click **Commit**.

---

**Related topics:**

[Edit Appender field descriptions](#) on page 1113

---

## Removing an appender from a logger

1. On the System Manager console, click **Events > Logs > Log Settings** in the left navigation pane.
  2. On the Log Settings page, click a log file from the **Select Log File** field.
  3. Click a logger in the **Logger List** section.
  4. Click **Edit**.
  5. On the Edit logger page, click an appender in the **Attached Appendors** section.
  6. Click **Detach**.
-

---

## Backup And Restore field descriptions

Use this page to view the details of backup files.

| Name               | Description   |
|--------------------|---|
| <b>File Name</b>   | Name of the backup file.  |
| <b>Path</b>        | Path of the backup file.  |
| <b>Status</b>      | Status of the backup. The values are: <ul style="list-style-type: none"> <li>• SUCCESS</li> <li>• FAILED</li> </ul> |
| <b>Backup Time</b> | Time of backup.   |
| <b>Backup Mode</b> | The mode defines whether the backup is manual or automatic.   |
| <b>Backup Type</b> | The type defines whether the backup is a local or remote backup.  |
| <b>User</b>        | The user who has performed the backup.  |

| Button         | Description  |
|----------------|--|
| <b>Backup</b>  | Opens the Backup page. Use this page to back up data on a specified local or remote location.  |
| <b>Restore</b> | Opens the Restore page. Use this page to restore data to a specified local or remote location. |

---

## Backup field descriptions

Use this page to backup the System Manager data on a local or a remote location. You can also use this page to schedule a back up.

| Name        | Description   |
|-------------|---|
| <b>Type</b> | The type based on the location of the computer on which you want to back up the application data. The options are: <ul style="list-style-type: none"> <li>• <b>Local</b>: The data is backed up on a local machine.</li> <li>• <b>Remote</b>: The data is backed up on a remote machine.</li> </ul> |

The page displays the following fields when you choose to create a backup of System Manager data on a local computer.

| Name             | Description  |
|------------------|--|
| <b>File Name</b> | The name of the file that identifies the backup. If you specify only the filename, System Manager creates a backup file in the home directory of the specified user. If you want to create the backup file in a directory other than the home directory, specify a complete path including the filename. |

The page displays the following fields when you choose to create a backup of System Manager data on a remote computer.

| Name                      | Description   |
|---------------------------|---|
| <b>Remote Server IP</b>   | IP address of the remote server.                            |
| <b>Remote Server Port</b> | Port of the remote server.                                  |
| <b>User Name</b>          | User name for logging into the remote server.               |
| <b>Password</b>           | Password for logging into the remote server.                |
| <b>File Name</b>          | The path and name of the backup file.                       |
| <b>Use Default</b>        | Select this check box to use the default configured values. |

| Button          | Description   |
|-----------------|---|
| <b>Now</b>      | Backs up the data to the specified location immediately.                  |
| <b>Schedule</b> | Opens the Schedule Backup page. Use this page to schedule a back up.      |
| <b>Cancel</b>   | Closes the Backup page and takes you back to the Backup and Restore page. |

---

## Schedule Backup field descriptions

Use this page to schedule a job for backup of data by specifying the date and time of running the job.

### Job Details

| Name            | Description          |
|-----------------|----------------------|
| <b>Job Name</b> | The name of the job. |

### Job Frequency

| Name             | Description                           |
|------------------|---------------------------------------|
| <b>Task Time</b> | The date and time of running the job. |

| Name              | Description   |
|-------------------|---|
| <b>Recurrence</b> | The settings define whether the execution of the jobs is a recurring activity or a one time activity. In the case of a recurring job, the field also displays the time interval of recurrence. The options are: <ul style="list-style-type: none"> <li>• Execute task one time only.</li> <li>• Task are repeated.</li> </ul> |
| <b>Range</b>      | The settings define the number of recurrences or date after which the job stops to recur. The options are: <ul style="list-style-type: none"> <li>• No End Date</li> <li>• End After occurrences</li> <li>• End By Date</li> </ul>  |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Schedules the backup job.  |
| <b>Cancel</b> | Closes the Schedule Backup page and takes you back to the Backup Restore page. |

---

## Restore field descriptions

Use this page to restore the application data from a local or a remote location.

| Name        | Description   |
|-------------|---|
| <b>Type</b> | The type based on the location of the computer from which you want to restore the application data. The options are: <ul style="list-style-type: none"> <li>• <b>Local</b>: The data is restored from a local machine.</li> <li>• <b>Remote</b>: The data is restored from a remote machine.</li> </ul> |

The page displays the following fields, when you select **Local** as **Type**.

| Name                    | Description   |
|-------------------------|---|
| <b>File Name</b>        | The name of the backup file that you want to restore.       |
| <b>Select File Name</b> | Lists the name of the backup file that you want to restore. |

The page displays the following fields, when you select **Remote** as **Type**.

| Name                      | Description                   |
|---------------------------|-------------------------------|
| <b>Remote Server IP</b>   | IP address of the SCP server. |
| <b>Remote Server Port</b> | Port of the SCP server.       |

| Name        | Description   |
|-------------|---|
| User Name   | User name for logging in to the SCP server.                 |
| Password    | Password for logging in to the SCP server.                  |
| File Name   | The name of the backup file that you want to restore.       |
| Use Default | Select this check box to use the default configured values. |

| Button  | Description  |
|---------|--|
| Restore | Restores the data from the specified backup file.                          |
| Cancel  | Closes the Restore page and takes you back to the Backup and Restore page. |

---

## Data Retention field descriptions

Use this page to view and edit data retention rules.

| Name                      | Description  |
|---------------------------|--|
| Option button             | Click the option button to select a data retention rule. |
| Rule Name                 | Name of the rule.  |
| Rule Description          | A brief description about the data retention rule.       |
| Retention Interval (Days) | The number of days the data is retained.                 |

| Button | Description                                     |
|--------|---|
| Edit   | Modifies the selected rule.                     |
| Update | Updates the rule with changes made to the rule. |
| Cancel | Cancels the editing operation.                  |
| Apply  | Applies the selected rule.                      |

---

## Logging Settings field descriptions

Use this page to view and edit loggers defined in a log file.

### Log Configuration

| Name            | Description   |
|-----------------|---|
| Select Log File | The field lists the log files that you can configure. |

## Logger List

| Name                                     | Description  |
|--|--|
| <b>Logger</b>                            | The loggers in the selected log files.   |
| <b>Log level</b>                         | Log level defines as to what level of logging is set for the corresponding logger.                 |
| <b>Attached Appenders &gt; Name</b>      | Name of the appender.  |
| <b>Attached Appenders &gt; File Path</b> | The path of the file to which the appender logs the information.                                   |
| <b>Attached Appenders &gt; Facility</b>  | The process running on the machine that created the log message.                                   |
| <b>Attached Appenders &gt; host</b>      | The name of the syslog host where the log output is stored.  |
| <b>Show All</b>                          | Provides you an option to select the maximum number of logger records that you can view at a time. |

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the Edit Logger page that you can use to edit loggers. |

### Related topics:

[Viewing loggers for a log file](#) on page 1109

---

## Edit Logger field descriptions

Use this page to edit logger and appender information. You can also add and remove appenders from the loggers.

### Logger

| Name             | Description   |
|------------------|---|
| <b>Logger</b>    | The name of the logger.   |
| <b>Log level</b> | The level of logging for which the logger logs the information. |

### Attached Appender

| Name                       | Description   |
|----------------------------|---|
| <b>Appender</b>            | The name of the appender.   |
| <b>Threshold Log Level</b> | The threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level . |

| Name                     | Description   |
|--------------------------|---|
| <b>File Path</b>         | The path of the file where the appender logs the information.   |
| <b>Max File Size</b>     | The maximum size in KB, MB, and GB reserved for the appender file.  |
| <b># Backup Files</b>    | The number of log files that an appender can use to store log information if one log file becomes full. If all the backup files are full, the appender overwrites the previous backup files in the order the files are created. |
| <b>Facility</b>          | The process running on the machine for which log messages are created.  |
| <b>Host</b>              | The name of the syslog host that stores the log output.   |
| <b>Header</b>            | The header part of the syslog packet. The header part contains timestamp and host name information.   |
| <b>Facility Printing</b> | The printed message includes the facility name of the application.  |

| Button        | Description   |
|---------------|---|
| <b>Edit</b>   | Opens the Edit Appender page. Use this page to modify the appender information.   |
| <b>Attach</b> | Opens the Attach Appender page. Use this page to add an appender to the logger.   |
| <b>Detach</b> | Removes the selected appender from the logger.                                    |
| <b>Commit</b> | Saves the changes in the logger information to the database.                      |
| <b>Cancel</b> | Closes the Edit Logger page and takes you back to the Logging Configuration page. |

## Edit Appender field descriptions

Use this page to edit information of an appender.

| Name                       | Description  |
|----------------------------|--|
| <b>Logger</b>              | The name of the logger.<br> <b>Note:</b><br>You can only view this information.   |
| <b>Appender</b>            | The name of the appender.<br> <b>Note:</b><br>You can only view this information. |
| <b>Threshold Log Level</b> | The threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level .                                    |

| Name                  | Description   |
|-----------------------|---|
| <b>File Path</b>      | The path of the file where the appender logs the information.   |
| <b>Max File Size</b>  | The maximum KB, MB, and GB reserved for the appender file.  |
| <b># Backup Files</b> | The number of log files that an appender can use to store log information if one log file becomes full. If all the backup files are full, the appender overwrites the previous backup files in the order the files are created. |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Saves the changes to the database.                                    |
| <b>Cancel</b> | Closes Edit Appender page and takes you back to the Edit Logger page. |

---

## Attach Appender field descriptions

Use this page to assign an appender to the logger.

| Name                   | Description   |
|------------------------|---|
| <b>Logger</b>          | The name of the logger.   |
| <b>Log Level</b>       | The level of logging for which the logger logs the information. |
| <b>Select Appender</b> | The list of appenders that you can assign to the logger.        |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Assigns the appender to the logger.  |
| <b>Cancel</b> | Closes the <b>Attach Appender</b> page and takes you back to the Edit Logger page. |

## Managing data retention rules

---

### Accessing the Data Retention Rules service

---

1. Log in to the System Manager web interface as an administrator.
  2. On the System Manager console, click **System Manager Data** > **Data Retention** in the left navigation pane.  
The system displays the Data Retention page.
- 

### Data retention rules

---

You can configure data retention rules for specifying how long the backup files should remain on the system.

---

### Viewing data retention rules

---

On the System Manager console, click **System Manager Data** > **Data Retention** in the left navigation pane.

---

#### Result

The Data Retention page displays the data retention rules.

#### Related topics:

[Data Retention field descriptions](#) on page 1306

---

## Modifying data retention rules

- 
1. On the System Manager console, click **System Manager Data > Data Retention** in the left navigation pane.
  2. Click the option button to select a rule.
  3. Click **Edit**.
  4. Modify the value in the **Retention Interval (Days)** field.
  5. Click **Update** to save the value.
- 

### Related topics:

[Data Retention field descriptions](#) on page 1306

---

## Data Retention field descriptions

Use this page to view and edit data retention rules.

| Name                             | Description  |
|----------------------------------|--|
| <b>Option button</b>             | Click the option button to select a data retention rule. |
| <b>Rule Name</b>                 | Name of the rule.  |
| <b>Rule Description</b>          | A brief description about the data retention rule.       |
| <b>Retention Interval (Days)</b> | The number of days the data is retained.                 |

| Button        | Description                                     |
|---------------|---|
| <b>Edit</b>   | Modifies the selected rule.                     |
| <b>Update</b> | Updates the rule with changes made to the rule. |
| <b>Cancel</b> | Cancels the editing operation.                  |
| <b>Apply</b>  | Applies the selected rule.                      |

---

## Data Replication Service

---

### Data Replication Service

The Data Replication Service replicates data from the master database residing on the server.

The Data Replication Service supports the following two modes of replication:

- Replication in Repair mode: In repair mode, the Data Replication Service replicates all of the requested data from the master database to the database of the replica node. Repair should only be necessary if there is a post-install failure of the Data Replication Service.
- Automatic synchronization mode: After the database of the replica node is loaded with the requested data, the subsequent synchronizations of the master database and the replica database occur automatically. The Data Replication service replicates only the data that has been updated since the last replication. Automatic synchronization is a scheduled activity and occurs after each fixed interval of time as set in the configuration files.

The data from the master database is sent to the replica node in batches. Data Replication Service creates replication batches whenever the data in the master database is added, modified, and deleted.

You can perform the following activities using the Data Replication service:

- View replica nodes in a replica group.
- Replicate requested data from the System Manager master database to the database of the replica nodes if the databases are not synchronized

---

### Viewing replica groups

You can view all the replication groups that are created in System Manager.

---

On the System Manager console, click **System Manager Data** > **Replication** in the left navigation pane.

The system displays the Replica Groups page.

---

#### Result

The Replica Groups page displays the groups in a table.

**Related topics:**

[Replica Groups field descriptions](#) on page 1315

---

## Viewing replica nodes in a replica group

You can view the replica nodes in a group.

- 
1. On the System Manager console, click **System Manager Data** > **Replication** in the left navigation pane.  
The system displays the Replica Groups page.
  2. Select a replica group and click **View Replica Nodes**.  
Alternatively, you can click a replica group name displayed under the **Replica Group** column to view the replica nodes for that replica group.  
The Replica Nodes page displays the replica nodes for the select group.
- 

**Related topics:**

[Replica Nodes field descriptions](#) on page 1315

---

## Repairing a replica node

You can replicate data for a replica node whose database is not synchronized with the System Manager database. Repair is necessary if there is a post-install failure of the Data Replication Service.

- 
1. On the System Manager console, click **System Manager Data** > **Replication** in the left navigation pane.  
The system displays the Replica Groups page.
  2. Select a replica group for which you want repair the replica nodes from the table displaying replica groups and click **View Replica Nodes** or click the name of the replica node displayed in the **Replica Group** column.
  3. On the Replica Nodes page, select a replica node and click **Repair**.  
The **Synchronization Status** column displays the data replication status for the repairing replica node.
-

**Related topics:**

[Replica Nodes field descriptions](#) on page 1315

---

## Repairing all replica nodes in a replica group

You can replicate data for all the replica nodes that are in a group. You can perform this operation if replica nodes in a group are not synchronized with the System Manager database.

- 
1. On the System Manager console, click **System Manager Data** > **Replication** in the left navigation pane.  
The system displays the Replica Groups page.
  2. Select a replica group for which you want repair the replica nodes from the table displaying replica groups.
  3. Click **Repair**.  
The **Synchronization Status** column displays the data replication status for the replica group.
- 

---

## Viewing replication details for a replica node

You can view the batch related information such as total number of batches received, processed, and skipped for a replica node. The master database sends the requested data in batches to the replica node.

- 
1. On the System Manager console, click **System Manager Data** > **Replication** in the left navigation pane.  
The system displays the Replica Groups page.
  2. Select a replica group and click **View Replica Nodes**.  
The Replica Nodes page displays the replica nodes for the selected replica group in a table.
  3. Select a replica node and click **View Details**.  
The Data Replication page displays the replication details for the selected replica node.
- 

**Related topics:**

[Data Replication field descriptions](#) on page 1317

---

## Replica Groups field descriptions

You can use this page to:

- view all the replica groups in the enterprise. These replica groups are logical grouping of the replica nodes.
- replicate data requested by the replica node from the master database to the database of the replica nodes
- view the replication status of the replica groups

The page displays these fields when you All from the **Replica Group** field.

| Name                          | Description  |
|-------------------------------|--|
| <b>Select check box</b>       | You can use this check box to select a group.  |
| <b>Replica Group</b>          | Name of the replica group. This is a hyperlink. When you click a group, the Replica Nodes page opens and displays the replica nodes for that group.                                |
| <b>Synchronization Status</b> | Replication status of the replica group. The group displays out of synch status if any one of the replica computer database in the group and master database are not synchronized. |

| Button                    | Description   |
|---------------------------|---|
| <b>View Replica Nodes</b> | Opens the Replica Nodes page. You can use this page to view replica nodes for a selected group. |
| <b>Repair</b>             | Replicates data for a selected replica node that is not synchronized with the master nodes.     |

---

## Replica Nodes field descriptions

You can use this page to:

- View the replica nodes in a selected replica group which has requested data replication from the master database of System Manager
- View the replication status of replica nodes in a group

| Name                          | Description  |
|-------------------------------|--|
| <b>Select check box</b>       | You can use this check box to select a replica node. |
| <b>Replica Node Host Name</b> | The IP address of the replica node                   |
| <b>Product</b>                | Name of the product running on the replica node      |

| Name                                    | Description   |
|---|---|
| <p><b>Synchronization Status</b></p>    | <p>The synchronization status of the replica node. The following are the status for when you click the <b>Repair</b> button on the page to perform a data replication for a replica node:</p> <ul style="list-style-type: none"> <li>• Ready for Repair: This status indicates that database of the replica node is not synchronized with the master database.</li> <li>• Queued for Repair: This status indicates that replication request of the replica computer is in queue with other data replication requests. The color code of the status is yellow.</li> <li>• Repairing: This status indicates that the data replication process is in progress. The color code of the status is yellow.</li> <li>• Synchronized: This status indicates that the data requested by the replica node is successfully replicated from the master database to the database of the replica node. The color code of the status is green.</li> <li>• Synchronization Failure: This status indicates an error in data replication for the initial load. Resolving this issue requires manual intervention from the administrator.</li> </ul> <p>The system displays the following status during automatic replication of data from the master to the replica node:</p> <ul style="list-style-type: none"> <li>• Synchronizing: This status indicates that the data replication is in progress for the replica node. The color code of the status is yellow.</li> <li>• Synchronized: This status indicates that the data requested by the replica node is successfully replicated from the master database to the database of the replica node. The color code of the status is green.</li> </ul> |
| <p><b>Last Synchronization time</b></p> | <p>The last time when the data synchronization or replication happened for the replica node.</p>  |

| Button                                | Description   |
|---------------------------------------|---|
| <p><b>View Details</b></p>            | <p>Opens the Data Replication page. You can use this page to view the synchronization details for a replica node.</p> |
| <p><b>Repair</b></p>                  | <p>Replicates or synchronizes data from the master node to a selected replica node.</p>                               |
| <p><b>Remove</b></p>                  | <p>Removes the selected nodes from the group.</p>   |
| <p><b>Show All Replica Groups</b></p> | <p>Takes you back to the Replica Groups page.</p>   |

---

## Data Replication field descriptions

### General

| Name                             | Description  |
|----------------------------------|--|
| <b>Replica Node Group</b>        | Name of the group of the replica computer.   |
| <b>Replica Node Host Name</b>    | The IP address of the replica computer   |
| <b>Last Synchronization Time</b> | The last time and date when the data synchronization or replication happened for the replica node. |
| <b>Synchronization Status</b>    | The synchronization status of the replica computer.  |

### Synchronization Status

| Name                   | Description  |
|------------------------|--|
| <b>Pending Batches</b> | The batches for which data replication is pending. |

### Statistics

| Name                  | Description  |
|-----------------------|--|
| <b>Cause of Error</b> | A brief description of reason for failure to replicate or synchronize data |
| <b>Time of Error</b>  | The time when the error occurred.  |

---

## Managing scheduled jobs

---

### Scheduler

Scheduler is a schedule management service that provides the ability to monitor the tasks that are scheduled for execution. The scheduled tasks are of three types:

- **System scheduled:** The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but cannot delete the job.
- **Admin scheduled job:** The job that the administrator schedules for administering the application.
- **On-demand job:** The periodic jobs that the administrator may schedule to perform non-routine tasks.

You can browse the history of completed jobs. Using the Disable functionality, you can cancel all the executions scheduled for a task. The following are the important operations that you can perform using the Scheduler:

- View the pending and completed scheduled tasks
- Modify a task scheduled by an administrator or an On Demand Job
- Delete a scheduled task
- Schedule an On Demand Job
- Stop a running task
- Enable or Disable a task
- Search a scheduled task

---

### Accessing scheduler

1. Log in to the System Manager web interface as an administrator.
  2. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
-

---

## Viewing pending jobs

- 
1. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
  2. Click **Pending Jobs** in the left navigation pane.  
The Pending Jobs page displays the pending jobs.

---

### Related topics:

[Pending Jobs field descriptions](#) on page 1325

---

## Viewing completed jobs

- 
1. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
  2. Click **Completed Jobs** in the left navigation pane.  
The Completed Jobs page displays completed jobs.

---

### Related topics:

[Completed Jobs field descriptions](#) on page 1327

---

## Viewing details of a pending job

- 
1. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
  2. Click **Pending Jobs** in the left navigation pane.
  3. On the Pending Jobs page, select a pending job and click **View**.  
The Job Scheduling-View Job page displays the details of the selected job.
-

---

## Viewing details of a completed job

- 
1. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
  2. Click **Completed Jobs** in the left navigation pane.
  3. On the Completed Jobs page, select a completed job and click **View**.  
The Job Scheduling-View Job page displays the details of the selected job.
- 

---

## Viewing details of a pending job

- 
1. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
  2. Click **Pending Jobs** in the left navigation pane.
  3. On the Pending Jobs page, select a pending job and click **View**.  
The Job Scheduling-View Job page displays the details of the selected job.
- 

---

## Viewing logs for a job

Use this functionality to view logs for a pending and completed job.

- 
- 1.
  2. Perform one of the following steps:
    - To view logs for a pending job, perform the following steps:
      - i. Click **Pending Jobs** in the left navigation pane.
      - ii. On the Pending Jobs page, select a pending job and click **More Actions > View Log**.
    - To view logs for a completed job, perform the following steps:
      - i. Click **Completed Jobs** in the left navigation pane.

- ii. On the Completed Jobs page, select a completed job and click **More Actions > View Log**.

---

## Result

The log viewer displays the log details for the selected job.

---

## Viewing completed jobs

1. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
2. Click **Completed Jobs** in the left navigation pane.  
The Completed Jobs page displays completed jobs.

---

## Related topics:

[Completed Jobs field descriptions](#) on page 1327

---

## Filtering Jobs

1. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
2. Perform one of the following steps:
  - Click **Pending Jobs** in the left navigation pane and click **Filter: Enable** on the Pending Jobs page.
  - Click **Completed Jobs** in the left navigation pane and click **Filter: Enable** on the Completed Jobs page.

The page displays the **Filter: Enable** at the upper-right of the page.

3. Select type of the job from the field under the **Job Type** column.
4. Enter the name of job in the field under the **Job Name** field.
5. Select the status of the job from the field under the **Job Status** field.
6. Select the state of the job from the field under the **State** field.
7. Select the frequency of execution of the job from the field under the **Frequency** field.
8. Enter the scheduler of the job in the field under the **Scheduled By** column.



**Note:**

This field is displayed only for the completed jobs.

9. Click **Apply**.

---

## Result

The page displays jobs that match the filter criteria.

---

## Editing a job

1. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
2. Perform one of the following steps:

- To edit a pending job, perform the following steps:

- i. Click **Pending Jobs** in the left navigation pane.
- ii. On the Pending Jobs page, select a pending job and click **Edit**.



**Note:**

Alternatively, you can also click **View > Edit** to access the Job Scheduling-Edit Job page.

- To edit a completed job, perform the following steps:

- i. Click **Completed Jobs** in the left navigation pane.
- ii. On the Completed Jobs page, select a completed job and click **Edit**.



**Note:**

Alternatively, you can also click **View > Edit** to access the Job Scheduling-Edit Job page.

3. On the Job Scheduling-Edit Job page, modify the appropriate information and click **Commit** to save the changes.



**Note:**

You can modify information in the following fields: **Job Name**, **Job State** in the **Job Details** sections, and **Task Time**, **Recurrence**, **Range** in the **Job Frequency** section.

---

---

## Deleting a job

### Prerequisites

You must log in as an administrator to delete an administrator scheduled job.

Use this functionality to delete an obsolete job. You can delete an On demand and on demand and administrator scheduled job.

 **Note:**

You can remove only jobs that are of type Schedule On Demand.

- 
1. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
  2. Perform one of the following steps:
    - To remove a pending job, perform the following steps:
      - i. Click **Pending Jobs** in the left navigation pane.
      - ii. On the Pending Jobs page, select a pending job.

 **Note:**

If the job that you want to delete is currently running then you must stop the job. To stop the job, click **More Actions > Stop**.

 **Note:**

If the job that you want to delete is in the enabled state, disable the job.

- iii. Click **Delete**.
- To remove a competed job, perform the following steps:
  - i. Click **Completed Jobs** in the left navigation pane.
  - ii. On the Completed Jobs page, select a completed job .

 **Note:**

If the job that you want to delete is in the enabled state, disable the job.

- iii. Click **Delete**.
3. On the Delete Confirmation page, click **Ok**.

---

### Result

System Manager deletes the selected job from the database.

---

## Disabling a job

Use this functionality to make a job inactive.

- 
1. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
  2. Perform one of the following steps:
    - To disable a pending job, perform the following steps:
      - i. Click **Pending Jobs** in the left navigation pane.
      - ii. On the Pending Jobs page, select a pending job and click **More Actions > Disable**.
    - To disable a completed job, perform the following steps:
      - i. Click **Completed Jobs** in the left navigation pane.
      - ii. On the Completed Jobs page, select a completed job and click **More Actions > Disable**.
  3. On the Disable Confirmation page, click **Continue**.

---

### Result

The **State** of the selected job is changed to Disabled.

---

## Enabling a job

Use this functionality to make a job active.

- 
1. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
  2. Perform one of the following steps:

- To enable a pending job, perform the following steps:
  - i. Click **Pending Jobs** in the left navigation pane.
  - ii. On the Pending Jobs page, select a pending job and click **More Actions > Enable**.
- To enable a completed job, perform the following steps:
  - i. Click **Completed Jobs** in the left navigation pane.
  - ii. On the Completed Jobs page, select a completed job and click **More Actions > Enable**.

---

## Result

The **State** of the selected job is changed to Enabled.

---

## Stopping a Job

1. On the System Manager console, click the **System Manager Data > Scheduler** link in the left navigation pane.
2. Click **Pending Jobs** in the left navigation pane.
3. On the Pending Jobs page, select a pending job in the running state and click **More Actions > Stop**.
4. Click **Continue** on the Stop Confirmation page. Scheduler stops the selected job.

---

## Pending Jobs field descriptions

Use this page to view, edit and delete the scheduled jobs that are pending for execution.

| Name            | Description  |
|-----------------|--|
| <b>Job Type</b> | The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. Following are the job types: |

| Name                | Description  |
|---------------------|--|
|                     | <ol style="list-style-type: none"> <li>1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job.</li> <li>2. Admin scheduled job — The job that the administrator schedules for administering the application.</li> <li>3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.</li> </ol> |
| <b>Job Name</b>     | The name of the scheduled job.   |
| <b>Job Status</b>   | The current status of the pending job. The options are: <ol style="list-style-type: none"> <li>1. Pending Execution</li> <li>2. Running</li> </ol>   |
| <b>State</b>        | The state of a job indicates if the job is an active job. The options are: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>   |
| <b>Frequency</b>    | The time interval between two consecutive executions of the job.   |
| <b>Scheduled By</b> | The scheduler of the job.  |

| Button  | Description  |
|---|--|
| <b>View</b>                                     | Opens the Job Scheduling-View Job page that displays the details of the selected pending job.                        |
| <b>Edit</b>                                     | Opens the Job Scheduling-Edit Job page that you can use to modify the information of a selected pending job.         |
| <b>Delete</b>                                   | Opens the Delete Confirmation page that prompts you to confirm the deletion of the selected Jobs.                    |
| <b>More Actions &gt; View Log</b>               | Opens the Logging page that displays the logs for the selected pending jobs.   |
| <b>More Actions &gt; Stop</b>                   | Stops the selected job which is currently in running state.  |
| <b>More Actions &gt; Enable</b>                 | Changes the state of the selected pending job from inactive to active.   |
| <b>More Actions &gt; Disable</b>                | Opens the Disable Confirmation page that prompts you to confirm the disabling of the selected pending job.           |
| <b>More Actions &gt; Schedule On Demand Job</b> | Opens the Job Scheduling-On Demand Job page that you can use to schedule the selected pending job of type On Demand. |
| <b>Advanced Search</b>                          | Displays fields that you can use to specify the search criteria for searching a pending job.                         |

| Button                 | Description  |
|------------------------|--|
| <b>Filter: Enable</b>  | Displays fields under select columns that you can use to set filter criteria. This is a toggle button. |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.         |
| <b>Filter: Apply</b>   | Filters pending jobs based on the filter criteria.   |
| <b>Select: All</b>     | Selects all the pending jobs in the table displayed in the Job List section.                           |
| <b>Select: None</b>    | Clears the selection for the pending jobs that you have selected.                                      |
| <b>Refresh</b>         | Refreshes the pending job information.   |

### Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the upper-right corner of the page.

| Name            | Description  |
|-----------------|--|
| <b>Criteria</b> | <p>Displays the following three fields:</p> <ul style="list-style-type: none"> <li>• Drop-down 1 - The list of criteria that you can use to search the pending jobs.</li> <li>• Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field.</li> <li>• Field 3 – The value corresponding to the search criteria.</li> </ul> |

| Button        | Description  |
|---------------|--|
| <b>Clear</b>  | Clears the search value that you entered in the third field.   |
| <b>Search</b> | Searches the pending jobs based on the specified search conditions and displays the search results in the <b>Groups</b> section. |
| <b>Close</b>  | Cancel the search operation and hides the <b>Criteria</b> section.   |

### Related topics:

[Viewing pending jobs](#) on page 1319

---

## Completed Jobs field descriptions

Use this page to view and edit the completed jobs. In addition, you can also perform the following operations:

- Disable or Enable a job
- View a log
- Schedule and delete an on demand job

| Name                | Description  |
|---------------------|--|
| <b>Job Type</b>     | <p>The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the job types. Following are the job types:</p> <ol style="list-style-type: none"> <li>1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job.</li> <li>2. Admin scheduled job — The job that the administrator schedules for administering the application.</li> <li>3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.</li> </ol> |
| <b>Job Name</b>     | The name of the scheduled job.   |
| <b>Job Status</b>   | <p>The current status of the pending job. The options are:</p> <ol style="list-style-type: none"> <li>1. Status Unknown</li> <li>2. Interrupted</li> <li>3. Failed</li> <li>4. Successful</li> <li>5. Not Authorized</li> </ol>  |
| <b>Last Run</b>     | The date and time when the job was last run.   |
| <b>State</b>        | <p>The state of a job indicates if the job is an active. The options are:</p> <ul style="list-style-type: none"> <li>• Enabled: An active job.</li> <li>• Disabled: An inactive job.</li> </ul>  |
| <b>Frequency</b>    | The time interval between two consecutive executions of the job.   |
| <b>Scheduled By</b> | The scheduler of the job.  |

| Button                            | Description  |
|-----------------------------------|--|
| <b>View</b>                       | Opens the Job Scheduling-View Job page that displays the details and of the selected completed job.            |
| <b>Edit</b>                       | Opens the Job Scheduling-Edit Job page that you can use to modify the information of a selected completed job. |
| <b>Delete</b>                     | Opens the Delete Confirmation page that prompts you to confirm the deletion of the selected Jobs.              |
| <b>More Actions &gt; View Log</b> | Opens the Logging page that displays the logs for the selected completed jobs.                                 |

| Button  | Description  |
|---|--|
| <b>More Actions &gt; Enable</b>                 | Changes the state of the selected completed job from inactive to active.                                     |
| <b>More Actions &gt; Disable</b>                | Opens the Disable Confirmation page that prompts you to confirm the disabling of the selected completed job. |
| <b>More Actions &gt; Schedule On Demand Job</b> | Opens the Job Scheduling-On Demand Job page that you can use to schedule a On Demand job.                    |
| <b>Advanced Search</b>                          | Displays fields that you can use to specify the search criteria for searching a completed job.               |
| <b>Filter: Enable</b>                           | Displays fields under select columns that you can use to set filter criteria. This is a toggle button.       |
| <b>Filter: Disable</b>                          | Hides the column filter fields without resetting the filter criteria. This is a toggle button.               |
| <b>Filter: Apply</b>                            | Filters pending jobs based on the filter criteria.   |
| <b>Select: All</b>                              | Selects all the completed jobs in the table displayed in the Job List section.                               |
| <b>Select: None</b>                             | Clears the selection for the completed jobs that you have selected.  |
| <b>Refresh</b>                                  | Refreshes the completed job information.   |

### Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the upper-right corner of the page.

| Name            | Description  |
|-----------------|--|
| <b>Criteria</b> | <p>Displays the following three fields:</p> <ul style="list-style-type: none"> <li>• Drop-down 1 - The list of criteria that you can use to search the completed jobs.</li> <li>• Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field.</li> <li>• Field 3 – The value corresponding to the search criteria.</li> </ul> |

| Button        | Description  |
|---------------|--|
| <b>Clear</b>  | Clears the search value that you entered in the third field.   |
| <b>Search</b> | Searches the completed jobs based on the specified search conditions and displays the search results in the <b>Groups</b> section. |
| <b>Close</b>  | Cancel the search operation and hides the <b>Criteria</b> section.   |

### Related topics:

[Viewing completed jobs](#) on page 1319

## Job Scheduling-View Job field descriptions

Use this page to view the details and frequency of a job.

### Job Details

| Name              | Description  |
|-------------------|--|
| <b>Job Name</b>   | The name of the job.   |
| <b>Job Type</b>   | <p>The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. Following are the job types:</p> <ol style="list-style-type: none"> <li>1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job.</li> <li>2. Admin scheduled job — The job that the administrator schedules for administering the application.</li> <li>3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.</li> </ol> |
| <b>Job Status</b> | <p>The current status of the job. The options are:</p> <ol style="list-style-type: none"> <li>1. Running</li> <li>2. Pending</li> <li>3. Status Unknown</li> <li>4. Interrupted</li> <li>5. Failed</li> <li>6. Successful</li> <li>7. Not Authorized</li> </ol>  |
| <b>Job State</b>  | <p>The state of a job indicates whether the job is an active job or not. The options are:</p> <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>  |

### Job Frequency

| Name              | Description  |
|-------------------|--|
| <b>Task Time</b>  | The date and time of running the job.  |
| <b>Recurrence</b> | The settings define whether the execution of the jobs is a recurring activity or a one time activity. In case of a recurring job, the field also displays the frequency of recurrence. |

| Name         | Description   |
|--------------|---|
| <b>Range</b> | The number of recurrences or a date after which the job stops to recur. |

| Button          | Description  |
|-----------------|--|
| <b>View Log</b> | Opens the Logging page that you can use to view the logs for the selected job.               |
| <b>Edit</b>     | Opens the Job Scheduling-Edit Job page that you can use to edit the pending job information. |
| <b>Cancel</b>   | Closes the Job Scheduling-View Job page and returns to the Pending or Completed Jobs page.   |

## Job Scheduling-Edit Job field descriptions

Use this page to modify job details and frequency related information of a selected job.

### Job Details

| Name              | Description   |
|-------------------|---|
| <b>Job Name</b>   | The name of the job.  |
| <b>Job Type</b>   | <p>The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. Following are the job types:</p> <ol style="list-style-type: none"> <li>1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job.</li> <li>2. Admin scheduled job — The job that the administrator schedules for administering the application.</li> <li>3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.</li> </ol> <p> <b>Note:</b><br/>You can only view the information in this field.</p> |
| <b>Job Status</b> | <p>The current status of the job. The options are:</p> <ol style="list-style-type: none"> <li>1. Running</li> <li>2. Pending</li> <li>3. Status Unknown</li> <li>4. Interrupted</li> <li>5. Failed</li> </ol>   |

| Name                | Description  |
|---------------------|--|
|                     | 6. Successful<br>7. Not Authorized<br><br> <b>Note:</b><br>You can only view the information in this field. |
| <b>Job State</b>    | The state of a job indicates whether the job is an active job or not. The options are: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>                       |
| <b>Scheduled By</b> | The scheduler of the job.<br><br> <b>Note:</b><br>You can only view the information in this field.          |

### Job Frequency

| Name              | Description   |
|-------------------|---|
| <b>Task Time</b>  | The date and time of running the job. Use the calendar icon to select a date. The time is in the HH:MM:SS format followed by PM and AM.   |
| <b>Recurrence</b> | The settings define whether the execution of the jobs is a recurring activity or a one time activity. In case of a recurring job, the field displays the frequency of recurrence. |
| <b>Range</b>      | The number of recurrences or the date after which the job stops to recur.   |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Saves the changes to the database.   |
| <b>Cancel</b> | Closes the Job Scheduling-View Job page and returns to the Pending or completed Jobs page. |

## Job Scheduling-On Demand Job field descriptions

Use this page to schedule an on demand job.

### Job Details

| Name            | Description          |
|-----------------|----------------------|
| <b>Job Name</b> | The name of the job. |

## Job Frequency

| Name              | Description  |
|-------------------|--|
| <b>Task Time</b>  | The date and time of running the job.  |
| <b>Recurrence</b> | The settings define whether the execution of the jobs is a recurring activity or a one time activity. In case of a recurring job, the field also display the time interval of recurrence. The options are: <ul style="list-style-type: none"> <li>• Execute task one time only.</li> <li>• Task are repeated every day.</li> </ul> |
| <b>Range</b>      | The settings define the number of recurrences or date after which the job stops recurring. The options are: <ul style="list-style-type: none"> <li>• No End Date</li> <li>• End After occurrences</li> <li>• End By Date</li> </ul>  |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Schedules an On-Demand job.  |
| <b>Cancel</b> | Cancel the schedule an On Demand job operation and takes you back to the Pending or completed Jobs page. |

---

## Disable Confirmation field descriptions

Use this page to disable selected jobs.

| Name              | Description   |
|-------------------|---|
| <b>Job Type</b>   | The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. Following are the job types: <ol style="list-style-type: none"> <li>1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job.</li> <li>2. Admin scheduled job — The job that the administrator schedules for administering the application.</li> <li>3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.</li> </ol> |
| <b>Job Name</b>   | The name of the scheduled job.  |
| <b>Job Status</b> | The current status of the pending job. The options are:   |

| Name                | Description  |
|---------------------|--|
|                     | <ol style="list-style-type: none"> <li>1. Running</li> <li>2. Pending</li> <li>3. Status Unknown</li> <li>4. Interrupted</li> <li>5. Failed</li> <li>6. Successful</li> <li>7. Not Authorized</li> </ol>                       |
| <b>State</b>        | <p>The state of a job indicates whether the job is an active job or not. The options are:</p> <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>  |
| <b>Last Run</b>     | <p>The date and time when the job was last run successfully.</p> <p> <b>Note:</b><br/>The last run is applicable only for completed jobs.</p> |
| <b>Frequency</b>    | The time interval between two consecutive executions of the job.   |
| <b>Scheduled By</b> | The scheduler of the job.  |

| Button          | Description  |
|-----------------|--|
| <b>Continue</b> | Disables the job and cancels the next executions that are scheduled for the job.                   |
| <b>Cancel</b>   | Cancels the operation of disabling a job and takes you back to the Pending or completed Jobs page. |

---

## Stop Confirmation field descriptions

Use this page to stop a running job.

| Name            | Description  |
|-----------------|--|
| <b>Job Type</b> | The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. Following are the job types: |

| Name                | Description  |
|---------------------|--|
|                     | <ol style="list-style-type: none"> <li>1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job.</li> <li>2. Admin scheduled job — The job that the administrator schedules for administering the application.</li> <li>3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.</li> </ol> |
| <b>Job Name</b>     | The name of the scheduled job.   |
| <b>Job Status</b>   | The current status of the pending job. The jobs on this page have status Running.  |
| <b>State</b>        | The state of a job indicates if the job is an active job. All the jobs on this page are in the Enabled state.  |
| <b>Last Run</b>     | <p>The date and time when the job was last run successfully.</p> <p> <b>Note:</b><br/>The last run is applicable only for completed jobs.</p>   |
| <b>Frequency</b>    | The time interval between two consecutive executions of the job.   |
| <b>Scheduled By</b> | The scheduler of the job.  |

| Button          | Description  |
|-----------------|--|
| <b>Continue</b> | Stops the job.   |
| <b>Cancel</b>   | Cancels the operation of stopping a job and takes you back to the Pending Jobs page. |

---

## Delete Confirmation field descriptions

| Name            | Description  |
|-----------------|--|
| <b>Job Type</b> | <p>The type of job represented by an icon that corresponds to its type. The application uses different icons to represent the Job types. Following are the job types:</p> <ol style="list-style-type: none"> <li>1. System scheduled Job — The job scheduled for the normal operation of the application. The System Administrator can reschedule and stop a system schedule job, but can not delete the job.</li> <li>2. Admin scheduled job — The job that the administrator schedules for administering the application.</li> <li>3. On-demand job — The periodic jobs that the administrator may schedule to perform non-routine tasks.</li> </ol> |

| Name                | Description   |
|---------------------|---|
| <b>Job Name</b>     | The name of the scheduled job.  |
| <b>Job Status</b>   | The current status of the job.  |
| <b>State</b>        | The state of a job indicates if the job is an active job. The jobs on this page are in the disabled state.  |
| <b>Last Run</b>     | The date and time when the job was last run.<br><br> <b>Note:</b><br>The last run is applicable only for completed jobs. |
| <b>Frequency</b>    | The time interval between two consecutive executions of the job.  |
| <b>Scheduled By</b> | The scheduler of the job.   |

| Button          | Description   |
|-----------------|---|
| <b>Continue</b> | Deletes the selected job.   |
| <b>Cancel</b>   | Cancels the operation of deleting a job and takes you back to the Pending or completed Jobs page. |

---

## Setting service profiles for applications

---

### About Service Profile Management

The Service Profile Management Service provides a configuration repository for the System Manager services. The Service Profile Management service is responsible for storing configuration data for the System Manager services and notifying the services of configuration changes. You can perform the following operations using the Service Profile Management service:

- Store configuration data for services
- View a profile of a service
- Edit a profile of a service

---

### Edit global feature profiles

This topic is about the global feature profiles that Service Profile Manager maintained in System Manager. You must log in as administrator to edit the global profiles.

Following is the global feature profile for System Manager:

[Edit Profile System Manager field descriptions](#) on page 1337

---

## View global feature profiles

This topic is about the global feature profiles that Service Profile Manager maintained in System Manager.

Following is the global feature profile for System Manager:

[View Profile System Manager field descriptions](#) on page 1338

---

## Edit Profile System Manager field descriptions

### applicationMetadata

| Name           | Description                              |
|----------------|--|
| Version Detail | The build version of the System Manager. |

### database

| Name           | Description                                      |
|----------------|--|
| connection_url | Complete URL for connecting to the database      |
| hostname       | Name of the computer that hosted the database    |
| jdbc_class     | Name of the database driver implementation class |
| password       | Password for accessing the database              |
| port           | Port for the database connection                 |
| user           | Name of the database user                        |
| vendor         | Name of the database                             |

| Button | Description   |
|--------|---|
| Commit | Saves changes to the database                           |
| Cancel | Takes you back to the View Profile: System Manager page |

### Related topics:

[Edit global feature profiles](#) on page 1336

---

## View Profile System Manager field descriptions

### applicationMetadata

| Name           | Description                             |
|----------------|---|
| Version Detail | The build version of the System Manager |

### database

| Name           | Description                                      |
|----------------|--|
| connection_url | The complete URL for connecting to the database  |
| hostname       | Name of the computer that hosted the database    |
| jdbc_class     | Name of the database driver implementation class |
| password       | Password for accessing the database              |
| port           | Port for the database connection                 |
| user           | Name of the database user                        |
| vendor         | Name of the database                             |

| Button | Description                                |
|--------|--|
| Edit   | Opens the Edit Profile System Manager page |
| Done   | Closes the page.                           |

### Related topics:

[View global feature profiles](#) on page 1337

---

## Edit software feature profiles

This topic is about the software feature profiles that Service Profile Manager maintains for global feature profiles in System Manager. You must log in as an administrator to modify the software feature profiles.

Following are the software feature profiles for the System Manager global feature profile:

[Edit Profile:Licenses field descriptions](#) on page 1340

[Edit Profile:Alarming UI field descriptions](#) on page 1341

[Edit Profile:IAM field descriptions](#) on page 1355

[Edit Profile: System Manager Element Manager field descriptions](#) on page 1363

[Edit Profile:Logging field descriptions](#) on page 1365

[Edit Profile:Scheduler field descriptions](#) on page 1369

[Edit Profile:SNMP field descriptions](#)

[Edit Common Console Profile field descriptions](#) on page 1371

[Edit Profile: Communication System Management Configuration field descriptions](#) on page 1372

[Edit Profile: User Bulk Import Profile field descriptions](#) on page 1378

[Edit Profile: Role Bulk Import Profile field descriptions](#) on page 1374

[Edit Profile Enterprise Directory Synchronization field descriptions](#) on page 1344

---

## View software feature profiles

This topic is about the software feature profiles that Service Profile Manager maintains for global feature profiles in System Manager.

Following are the software feature profiles for the System Manager global feature profile:

[View Profile:Licenses field descriptions](#) on page 1339

[View Profile:Alarming UI field descriptions](#) on page 1341

[View Profile:IAM field descriptions](#) on page 1348

[View Profile: System Manager Element Manager field descriptions](#) on page 1361

[View Profile:Logging field descriptions](#) on page 1364

[View Profile:Scheduler field descriptions](#) on page 1368

[View Profile:SNMP field descriptions](#) on page 1370

[View Common Console Profile field descriptions](#) on page 1372

[View Profile: Communication System Management Configuration field descriptions](#) on page 1373

[View Profile: Role Bulk Import Profile field descriptions](#) on page 1376

[View Profile: User Bulk Import Profile field descriptions](#) on page 1379

[Edit Profile Enterprise Directory Synchronization field descriptions](#) on page 1344

---

## View Profile:Licenses field descriptions

Use this page to view the parameters in the WebLM profile.

| Name   | Description   |
|--|---|
| <b>WebLM.Usages.UsageCount</b>                 | This count represents the number of usage reports the server must maintain and display for each WebLM server.   |
| <b>WebLM.LicenseAllocation.Backup.FileSize</b> | This property specifies the size of the license allocation backup file in MB. Allocate an integer to this property like 1 or 10. A decimal value like 1.5 is not valid. |

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the Edit Profile:Licenses (WebLM) page. Use this page to edit the parameters in the WebLM profile. |
| <b>Done</b> | Closes the View Profile:Licenses (WebLM) page.   |

**Related topics:**

- [View software feature profiles](#) on page 1339
- [View Profile: User Bulk Import Profile field descriptions](#) on page 1379
- [View Profile: Agent Management field descriptions](#) on page 1381
- [View Profile: Alarm Management field descriptions](#) on page 1383
- [View Profile: Event processor field descriptions](#) on page 1384
- [View Profile : Data Transport Config field descriptions](#) on page 1385
- [View Profile: Data Transport Static Config field descriptions](#) on page 1388

---

## Edit Profile:Licenses field descriptions

Use this page to edit the parameters in the WebLM profile.

| Name   | Description   |
|--|---|
| <b>WebLM.Usages.UsageCount</b>                 | This count represents the number of usage reports the server must maintain and display for each WebLM server.   |
| <b>WebLM.LicenseAllocation.Backup.FileSize</b> | This property specifies the size of the license allocation backup file in MB. Allocate an integer to this property like 1 or 10. A decimal value like 1.5 is not valid. |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Saves the changes to the database.   |
| <b>Cancel</b> | Cancels the edit profile operation and takes you back to the View Profile:Licenses (WebLM) page. |

**Related topics:**

[Edit software feature profiles](#) on page 1338

[Edit Profile:Logging Service field descriptions](#) on page 1367

---

## Edit Profile:Alarming UI field descriptions

Use this page to edit the parameters in the Alarming profile.

**Color Codes**

| Name                 | Description                                 |
|----------------------|---|
| <b>Cleared</b>       | The color code for alarms that are cleared. |
| <b>Critical</b>      | The color code for critical alarms.         |
| <b>Informational</b> | The color code for informational alarms.    |
| <b>Intermediate</b>  | The color code for the intermediate alarms. |
| <b>Major</b>         | The color code for the major alarms.        |
| <b>Minor</b>         | The color code for the minor alarms.        |
| <b>Warning</b>       | The color code for the warning alarms.      |

**Auto Refresh**

| Name                            | Description  |
|---------------------------------|--|
| <b>Time Interval (millisec)</b> | The time interval in milliseconds after which the Alarming module refreshes the alarms on the Alarming page. |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Saves the changes to the database.  |
| <b>Cancel</b> | Cancels the edit profile operation and takes you back to the View Profile:Alarming UI page. |

**Related topics:**

[Edit software feature profiles](#) on page 1338

[Edit Profile:Logging Service field descriptions](#) on page 1367

---

## View Profile:Alarming UI field descriptions

Use this page to view the parameters in the Alarming profile.

## Color Codes

| Name                 | Description                                 |
|----------------------|---|
| <b>Cleared</b>       | The color code for cleared alarms.          |
| <b>Critical</b>      | The color code for critical alarms.         |
| <b>Informational</b> | The color code for informational alarms.    |
| <b>Intermediate</b>  | The color code for the intermediate alarms. |
| <b>Major</b>         | The color code for the major alarms.        |
| <b>Minor</b>         | The color code for the minor alarms.        |
| <b>Warning</b>       | The color code for the warning alarms.      |

## Auto Refresh

| Name                            | Description  |
|---------------------------------|--|
| <b>Time Interval (millisec)</b> | The time interval in milliseconds after which the Alarming module refreshes the alarms on the Alarming page. |

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the Edit Profile:Alarming UI page. Use this page to edit the parameters in the Alarming Profile. |
| <b>Done</b> | Closes the View Profile:Alarming UI page.  |

### Related topics:

[View software feature profiles](#) on page 1339

[View Profile: User Bulk Import Profile field descriptions](#) on page 1379

[View Profile: Agent Management field descriptions](#) on page 1381

[View Profile: Alarm Management field descriptions](#) on page 1383

[View Profile: Event processor field descriptions](#) on page 1384

[View Profile : Data Transport Config field descriptions](#) on page 1385

[View Profile: Data Transport Static Config field descriptions](#) on page 1388

---

## View Profile Enterprise Directory Synchronization field descriptions

Use this page to view the parameters and their values configured for synchronizing users with active directory.

## Active Directory Mapping

| Name                  | Description   |
|-----------------------|---|
| <b>Abort on Error</b> | The values are true and false. If set to true, the synchronization task will stop on the first error and no additional users will be synchronized. This should be set to false for normal operation.  |
| <b>Base DN</b>        | The point in the Active Directory tree where the search should begin. The value should be a valid LDAP DN. For example, if the targeted Container in AD is "Users" and Domain of the "Active Directory" machine is "pansv.platform.avaya.com", the Base DN value is "CN=Users,DC=pansv,DC=platform,DC=avaya,DC=com" |
| <b>IP Address</b>     | IP address of the Active Directory.   |
| <b>LDAP Port</b>      | Port number of the LDAP server. 389 is the default port mentioned for Active directory. Change as per the requirement   |
| <b>Login</b>          | Login id of the user which has access to everything in Active Directory.<br><br> <b>Note:</b><br>This is an Active Directory user and not the System Manager administrator.  |
| <b>Password</b>       | Password of the user mentioned in <b>Login</b> field.   |
| <b>SSL Enabled</b>    | The values are true and false values. If set to true, an SSL connection to the Active Directory server will be established. This will require that a certificate from the Active Directory server has been imported into System Manager and that SSL has been enabled on the Active Directory server.               |

## Maintenance

It is recommended not to change these values.

| Name                         | Description  |
|------------------------------|--|
| <b>DSE Location</b>          | This field specifies the path of the DSE installation. The DSE is run as a separate Java process and the UPM Server needs to know where DSE is located within the file system so that it can start jobs when the scheduler fires. The location is set by the installer but may need to be updated in the case of a load-to-load upgrade (end customers should not need to change this). The location should be the same as the shell variable \$MGMT_HOME with "upm/sync-engine" appended to it. |
| <b>DSE Logging Level</b>     | This is the logging level used by the Maxware/SAP Data Synchronization Engine (third party) that is used. The range of values are 0 to 6 with 0 meaning no logging and 6 meaning debug level logging. This represents how much logging will appear in the file \$AVAYA_LOG/mgmt/upm/IdIPAddress where IPAddress is the internet address of the Active Directory server. This would only be changed when troubleshooting a problem.   |
| <b>DSE Stack Trace Level</b> | This value is for the Maxware DSE log mentioned above. It represents the level of stack trace included in any exceptions the Maxware DSE encounters.   |

| Name                | Description  |
|---------------------|--|
|                     | Values are 0 (none), 1 (show only topmost entry), and 2 (show full stack trace). This would only be changed when troubleshooting a problem.  |
| <b>Log Location</b> | This represents the directory where the Maxware DSE logs mentioned above will be stored. It should be the same as the shell environment variable \$AVAYA_LOG with "mgmt/upm" appended to it.   |
| <b>Sync All</b>     | The values are true and false. If set to true, the Maxware DSE will ignore any existing delta information it stores internally and re-synchronize all users that match the current LDAP filter. Setting this to true could result in information being lost in the SMGR database for existing enterprise users, such as group associations and role assignments. It should only be set to true if the customer is unable to reconcile major synchronization issues between the enterprise and SMGR. When set to true, any existing users in the SMGR database that match an enterprise user will be deleted and re-added as if they were a new user. |

 **Note:**

All the values except Sync All are string values with no specific validation. Sync All is defined as a Boolean type and subject to any default validation performs on its value.

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the Edit Profile Enterprise Directory Synchronization page. Use this page to edit the values of the Active Directory synchronization parameters. |
| <b>Done</b> | Closes the View Profile Enterprise Directory Synchronization page.   |

## Edit Profile Enterprise Directory Synchronization field descriptions

Use this page to modify the value of parameters that define settings for active directory synchronization.

### Active Directory Mapping

| Name                  | Description   |
|-----------------------|---|
| <b>Abort on Error</b> | The values and true or false. If set to true, the synchronization task will stop on the first error and no additional users will be synchronized. This should be set to false for normal operation.   |
| <b>Base DN</b>        | The point in the Active Directory tree where the search should begin. The value should be a valid LDAP DN. For example, if the targeted Container in AD is "Users" and Domain of the "Active Directory" machine is "pansv.platform.avaya.com", the Base DN value is CN=Users,DC=pansv,DC=platform,DC=avaya,DC=com |

| Name               | Description   |
|--------------------|---|
| <b>IP Address</b>  | IP address of the Active Directory.   |
| <b>LDAP Port</b>   | Port number of the LDAP server. 389 is the default port mentioned for Active directory. Change as per the requirement   |
| <b>Login</b>       | Login id of the user which has access to everything in Active Directory.<br><br> <b>Note:</b><br>This is an Active Directory user and not the System Manager administrator.  |
| <b>Password</b>    | Password of the user mentioned in <b>Login</b> field.   |
| <b>SSL Enabled</b> | The values are true and false values. If set to true, an SSL connection to the Active Directory server will be established. This will require that a certificate from the Active Directory server has been imported into System Manager and that SSL has been enabled on the Active Directory server. |

## Maintenance

It is recommended not to change these values.

| Name                         | Description  |
|------------------------------|--|
| <b>DSE Location</b>          | This field specifies the path of the DSE installation. The DSE is run as a separate Java process and the UPM Server needs to know where DSE is located within the file system so that it can start jobs when the scheduler fires. The location is set by the installer but may need to be updated in the case of a load-to-load upgrade (end customers should not need to change this). The location should be the same as the shell variable \$MGMT_HOME with "upm/sync-engine" appended to it. |
| <b>DSE Logging Level</b>     | This is the logging level used by the Maxware/SAP Data Synchronization Engine (third party) that is used. The range of values are 0 to 6 with 0 meaning no logging and 6 meaning debug level logging. This represents how much logging will appear in the file \$AVAYA_LOG/mgmt/upm/IdIPAddress where IPAddress is the internet address of the Active Directory server. This would only be changed when troubleshooting a problem.   |
| <b>DSE Stack Trace Level</b> | This value is for the Maxware DSE log mentioned above. It represents the level of stack trace included in any exceptions the Maxware DSE encounters. Values are 0 (none), 1 (show only topmost entry), and 2 (show full stack trace). This would only be changed when troubleshooting a problem.   |
| <b>Log Location</b>          | This represents the directory where the Maxware DSE logs mentioned above will be stored. It should be the same as the shell environment variable \$AVAYA_LOG with "mgmt/upm" appended to it.   |
| <b>Sync All</b>              | The values are true and false. If set to true, the Maxware DSE will ignore any existing delta information it stores internally and re-synchronize all users that match the current LDAP filter. Setting this to true could result in information being lost in the SMGR database for existing enterprise users, such as group associations and role assignments. It should only be set to true if the customer is unable to reconcile major synchronization issues between the enterprise        |

| Name | Description  |
|------|--|
|      | and SMGR. When set to true, any existing users in the SMGR database that match an enterprise user will be deleted and re-added as if they were a new user. |

 **Note:**

All the values except Sync All are string values with no specific validation. Sync All is defined as a Boolean type in SPM and subject to any default validation SPM performs on its value. All values are required fields.

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Saves the changes to the database.   |
| <b>Cancel</b> | Cancels the edit profile operation and takes you back to the View Profile Enterprise Directory Synchronization page. |

**Related topics:**

[Synchronizing users with Active Directory](#) on page 1346

---

## Synchronizing users with Active Directory

Synchronizing users with Active Directory is a two step process as

1. Configure directory synchronization profile
2. Schedule task for synchronizing user

- 
1. On the System Manager console, click **System Manager Data > Settings > SMGR > Enterprise Directory Synchronization** in the left navigation pane.
  2. On the View Profile:Enterprise Directory Synchronization page, click **Edit**.
  3. On the Edit Profile:Enterprise Directory Synchronization page, enter the appropriate information in the LDAP connection section.  
All are required fields. You must enter an appropriate information in these fields.  
You are recommended to keep the default values displayed in the Active Directory Mapping and Maintenance sections.
  4. Click **Commit** .
-

## Next steps

1. On the System Manager console, click **System Manager Data > Scheduler > Pending Jobs**.
2. On the Pending Jobs job, select the Directory Sync job from the table displaying pending jobs.
3. Click **More Actions > Schedule On Demand Job**.
4. Enter the name of the job in the Job Details section and frequency related information in the Job Frequency section.
5. Click **commit**.



### Note:

After the job is successfully run, click **Users > Manage Users** and verify synchronized user. The **Job Status** column displays the status of the Job on the Completed Jobs page. Click **System Manager Data > Scheduler > Completed Jobs** to access the Completed Jobs page.

### Related topics:

[Edit Profile Enterprise Directory Synchronization field descriptions](#) on page 1344

---

## System Manager security authentication mechanism

System Manager (SMGR) includes an Identity and Access Management (IAM) service that defines the authentication mechanism that SMGR will use to authenticate its users.

Users of System Manager are administrators who perform provisioning or maintenance tasks on the Avaya solution. IAM authenticates all the requests received by it for System Manager and after the successful authentication, IAM forwards the requests to System Manager.

IAM can authenticate users against the following:

- System Manager's User Profile Manager (UPM) Database
- LDAP (for example, Active Directory)
- ADIUS/RSA SecurID
- SAML

### User Profile Manager (UPM) DATABASE

IAM uses the System Manager database to authenticate a user. To authenticate a user, IAM searches the System Manger database for the login name of the user in the loginName column and compares the password entered for the login name with the password in the userPassword column.

The value entered in userPassword field is not a clear-text password. It is a digest of the password and some salt. This digest is created by UPM for the default users at the time of installation as well as when creating new users using UPM service.

After the installation of System Manger, the following two users exist: system and admin created at installation time. Additional users can be created by using the UPM service from the System Manager console.

### LDAP AND ACTIVE DIRECTORY

You can configure System Manager to use the Lightweight Directory Access Protocol (LDAP) to authenticate user logins. Following is the list of supported directories:

- MS Active Directory
- SUN LDAP 5.2
- OpenLDAP

### RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. See RFC 2865 for more information. System Manager supports FreeRADIUS.

### SAML

Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions).

SAML 2.0 is the only authentication method available on System Manager that supports Web Single Sign-On (Web SSO).SAML version 2.0 is supported with System Manager. Browser or POST for SAML 2.0 is supported for Web Single Sign-On (Web SSO).

#### Related topics:

[View Profile:IAM field descriptions](#) on page 1348

[Edit Profile:IAM field descriptions](#) on page 1355

---

## View Profile:IAM field descriptions

Use this page to view the parameters in the IAM profile.

### SAML

| Name                                | Description  |
|-------------------------------------|--|
| <b>SAML_ARTIFACT_RESOLUTION_URL</b> | The URL to contact for resolving artifacts to SAML assertions. If the SSL/TLS connection is required, this should point to the HTTPS URL of the server.                                      |
| <b>SAML_AUTHN_REQ_GET_OR_POST</b>   | When sending a redirect URL to the user for authentication, an authentication request is also sent. The sent HTML gets posted automatically and the Idp receives the authentication request. |

| Name                           | Description  |
|--------------------------------|--|
|                                | When doing this, the form method can be either GET or POST. Some IdPs require one of these explicitly.   |
| <b>SAML_BINDING</b>            | The binding for SAML. This binding is mentioned in the Authentication request sent to the Idp as an indication of the binding that the IdP must use when sending the assertion back. The values are: <ul style="list-style-type: none"> <li>• POST</li> <li>• Artifacts</li> </ul>   |
| <b>SAML_COMPRESS_AUTHN_REQ</b> | The parameter specifies whether or not to compress the authentication request when sending to the IdP. Use this option when the SAML_AUTHN_REQ_GET_OR_POST option is GET.  |
| <b>SAML_HTTP_AUTH_USERNAME</b> | The user name to be used at the HTTP level for BASIC authentication when using the artifact resolution by contacting the SAML_ARTIFACT_RESOLUTION_URL.   |
| <b>SAML_IDP_ALIAS</b>          | Following are two ways in which this parameter can be used for the signature verification: . <ul style="list-style-type: none"> <li>• If a value is provided for this parameter , then the signature is verified to have been created using the certificate pointed to by this alias</li> <li>• When the signature element in the assertion does not identify the certificate used for creating the signature, then the certificate pointed to by this alias is used.</li> </ul> |
| <b>SAML_IDP_LOGIN_URL</b>      | The URL to which the authentication request is sent.   |
| <b>SAML Need Signature</b>     | The value specifies whether or not the authentication requests need to be signed. The default value is false.  |
| <b>SAML_NEED_SSL</b>           | If the URL for SAML_ARTIFACT_RESOLUTION_URL is HTTPS, then SAML_NEED_SSL must be set to true. If SSL/TLS connection is required between IAM and SAML IdP, then this should be set to TRUE  |
| <b>SAML_PROVIDER_ID</b>        | ID of the Identity provider that provides the authentication service.  |

| Name                             | Description   |
|----------------------------------|---|
| <b>SAML_SIGNATURE_ALIAS</b>      |   |
| <b>SAML_SP_NAME</b>              | The configuration name at the IdP that uniquely identifies this instance of IAM.  |
| <b>SAML_URL_ENCODE_AUTHN_REQ</b> | The value indicates whether or not to URL-encode the authentication request when sending to the IdP. This option is used when the SAML_AUTHN_REQ_GET_OR_POST option is GET. |
| <b>SAML_VERIFY_SIGNATURE</b>     | The value indicates whether or not to verify the signatures in the assertions. The parameter accepts a boolean value.   |

**COMMON**

| Name                                  | Description  |
|---------------------------------------|--|
| <b>AUTHENTICATION_MECHANISM</b>       | <p>Determines the type of server to use. The values are:</p> <ul style="list-style-type: none"> <li>• UPM: Avaya UPM Database</li> <li>• LDAP: An LDAP or AD type server</li> <li>• RADIUS: Radius type server</li> <li>• SAML: the server to be used can act as a SAML ID</li> </ul>  |
| <b>AUTHENTICATION_MODE</b>            | <p>Determines the type of password to be used for authentication. The values are:</p> <ul style="list-style-type: none"> <li>• COMMUNICATIONS: Used for SIP authentication</li> <li>• NON-COMMUNICATIONS: Used for non-SIP authentication (for example, web access)</li> </ul> <p> <b>Note:</b><br/>Administrators are not expected to change this.</p> |
| <b>BASIC_OR_DIGEST_AUTHENTICATION</b> | <p>Determines if the digest authentication needs to be used. The values are:</p> <ul style="list-style-type: none"> <li>• DIGEST: Used for SIP authentication</li> <li>• BASIC: Must be used for all non-SIP based authentications</li> </ul>  |

| Name                                | Description   |
|-------------------------------------|---|
|                                     |  <b>Note:</b><br>Administrators are not expected to change this.   |
| <b>DIGEST_NONCE_PRIVATE_KEY</b>     | key used to create the NONCE value in the DIGEST mode.  |
| <b>DIGEST_NONCE_VALIDITY_PERIOD</b> | Value determines if a NONCE given by the client is still valid in the DIGEST mode. This should be given in milliseconds.  |
| <b>NUMBER_OF_ACTIVE_SESSIONS</b>    | Number of active sessions that each user may have at any given time. This parameter accepts an integer value. For example, 10 means that a particular user is allowed to login through 10 different browser instances at the same time. |
| <b>REALM_NAME</b>                   | Realm name to be used for SIP digest authentication. This parameter accepts a string value. For example, sipUsers@domain.com  |

## CONSOLE

| Name                                      | Description  |
|---|--|
| <b>LOGIN_PAGE_URI</b>                     | Determines the URL users are forwarded to for authentication.<br><br> <b>Note:</b><br>Administrators are recommended not to change the value of this parameter. |
| <b>LOGIN_SYSTEM_ERROR_REDIRECT_URL</b>    | Determines whether to redirect the user to a specific URL page if a system error occurs. The parameter accepts a boolean value: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>  |
| <b>LOGIN_SYSTEM_ERROR_REDIRECT_TO_URL</b> | Used in conjunction with <b>LOGIN_SYSTEM_ERROR_REDIRECT_URL</b> when <b>LOGIN_SYSTEM_ERROR_REDIRECT_URL</b> is set to TRUE. This is the specific URL the user is redirected to on encountering system errors.                                      |

## LDAP

| Name                           | Description   |
|--------------------------------|---|
| <b>LDAP_BASE_DN</b>            | The base DN value to be used. The complete DN used for the authentication is LDAP_USERNAME_PREFIX + "=" + name entered by user + "," + LDAP_BASE_DN.  |
| <b>LDAP_PRIMARY_HOST</b>       | The hostname or IP address of the primary LDAP/AD Server.   |
| <b>LDAP_PRIMARY_PORT</b>       | The port number of the primary LDAP/AD server.  |
| <b>LDAP_PRIMARY_SSL_REQD</b>   | Enables or Disables TLS/SSL connection between IAM module and the primary LDAP server. This parameter accepts boolean value. <ul style="list-style-type: none"> <li>• True: Enables TLS/SSL connection between the IAM module and the primary LDAP server</li> <li>• False: Disables TLS/SSL connection between the IAM module and the primary LDAP server</li> </ul> |
| <b>LDAP_SECONDARY_HOST</b>     | This parameter specifies hostname or IP address of the LDAP secondary host. Authentication is done against this LDAP/AD Server, if the Primary LDAP/AD server specified above is unreachable.   |
| <b>LDAP_SECONDARY_SSL_REQD</b> | This parameter specifies whether you can establish a TLS/SSL connection between the IAM module and the LDAP/AD server. The parameter accepts boolean value: <ul style="list-style-type: none"> <li>• True</li> <li>• False</li> </ul>   |
| <b>LDAP_USERNAME_PREFIX</b>    | The prefix for the username. The complete DN for the authentication is LDAP_USERNAME_PREFIX+ "=" + name entered by user + "," + LDAP_BASE_DN.   |

## DB

| Name                     | Description   |
|--------------------------|---|
| <b>DB_CONNECTION_URL</b> | The JDBC specific connection URL. You can request JDBC vendor to provide information on configuring the parameter. For example, <ul style="list-style-type: none"> <li>• For Oracle: jdbc:oracle:thin:@192.147.7.215:1521:avayadb, where</li> </ul> |

| Name                       | Description  |
|----------------------------|--|
|                            | <p>192.147.7.215 is the IP address of the database server and avayadb is the SID of the UPM database.</p> <ul style="list-style-type: none"> <li>For PostgreSQL: jdbc:postgresql://192.147.7.215/avayadb, where 192.147.7.215 is the IP address of the database server, and avayadb is the database name.</li> </ul> <p> <b>Note:</b><br/>If SSL is required when connecting to the database, then the connection URL will look different. Please refer DB_SSL_NEEDED parameter for more information.</p> |
| <b>DB_DRIVER_CLASSNAME</b> | <p>The JDBC driver class to be used for obtaining the database connection. This class is given by the database vendor. Note that the JAR file containing this class must be present in the system classpath – for example, \$JBOSS_HOME/server/&lt;&lt;serverName&gt;&gt;/lib folder. For example,</p> <ul style="list-style-type: none"> <li>For Oracle: oracle.jdbc.driver.OracleDriver</li> <li>For PostgreSQL: org.postgresql.Driver</li> </ul>  |
| <b>DB_JNDI_NAME</b>        | <p>JNDI name of the datasource object configured in the J2EE server. This datasource must point to the Avaya UPM DB.</p> <p> <b>Note:</b><br/>Administrators are strongly recommended not to change the value of this parameter after a successful installation of database.</p>   |
| <b>DB_PASSWORD</b>         | Password for connecting to the database.   |
| <b>DB_SCHEMA_NAME</b>      | Name of the schema used for creating the Avaya UPM tables.   |
| <b>DB_SSL_NEEDED</b>       | Indicates whether or not SSL needs to be used for connecting to the database. This parameter accepts a boolean value.  |
| <b>DB_USERNAME</b>         | Unique name that identifies the user when connecting to the database.  |

## Radius

| Name                            | Description   |
|---------------------------------|---|
| <b>RADIUS_NUM_RETRIES</b>       | The number of times the client should attempt to connect to the Radius server if the server does not respond. |
| <b>RADIUS_PRIMARY_AUTH_PORT</b> | The port number the primary the Radius server uses to receive RADIUS authentication requests.                 |

| Name                                  | Description   |
|---------------------------------------|---|
| <b>RADIUS_PRIMARY_HOST</b>            | Hostname or IP address of the primary Radius server for authentication. For example, IP address such as 192.168.111.23 or "hostname.rnd.avaya.com"  |
| <b>RADIUS_PRIMARY_SHARED_SECRET</b>   | The secret key that is used to sign RADIUS data packets to ensure they are coming from a trusted source. The Radius Server's clients configuration must be associated with this shared secret.  |
| <b>RADIUS_SECONDARY_AUTH_PORT</b>     | The port number on which the server listens for RADIUS authentication requests. Set this parameter when you use a secondary Radius server for fail over, and have provided a value for <b>RADIUS_SECONDARY_HOST</b> .   |
| <b>RADIUS_SECONDARY_HOST</b>          | The host name or IP address of the secondary Radius server that is used for fail over. Authentication is done against this Radius Server, if the Primary Radius server specified is not reachable.  |
| <b>RADIUS_SECONDARY_SHARED_SECRET</b> | The secret key configured in the secondary Radius Server's client configuration. This key will be used to sign RADIUS data packets to ensure they are coming from a trusted source. This must be provided if <b>RADIUS_SECONDARY_HOST</b> is provided for failover. |
| <b>RADIUS_SERVER</b>                  | The vendor name for the Radius Server. This value helps in loading the dictionary for the Radius Server. Attributes corresponding to this vendor name should be present in the AvayaRadiusClient.dict.  |
| <b>RADIUS_TIMEOUT</b>                 | The number of seconds to wait for the Radius Server to respond before the client times out the server   |

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the Edit Profile: IAM page. Use this page to edit the parameters in the IAM profile. |
| <b>Done</b> | Closes the View Profile: IAM page.   |

**Related topics:**

[View software feature profiles](#) on page 1339

[System Manager security authentication mechanism](#) on page 1347

[View Profile: User Bulk Import Profile field descriptions](#) on page 1379

[View Profile: Agent Management field descriptions](#) on page 1381

[View Profile: Alarm Management field descriptions](#) on page 1383

[View Profile: Event processor field descriptions](#) on page 1384

[View Profile : Data Transport Config field descriptions](#) on page 1385

[View Profile: Data Transport Static Config field descriptions](#) on page 1388

---

## Edit Profile:IAM field descriptions

Use this page to edit the parameters in the IAM profile.

### SAML

| Name                                     | Description   |
|--|---|
| <b>SAML_ARTIFACT_RESOLUTION_URL</b>      | The URL to contact for resolving artifacts to SAML assertions. If the SSL/TLS connection is required, this should point to the HTTPS URL of the server.   |
| <b>SAML_AUTHN_REQ_GET_OR_POST</b>        | When sending a redirect URL to the user for authentication, an authentication request is also sent. The sent HTML gets posted automatically and the Idp receives the authentication request. When doing this, the form method can be either GET or POST. Some IdPs require one of these explicitly. |
| <b>SAML_BINDING</b>                      | The binding for SAML. This binding is mentioned in the Authentication request sent to the Idp as an indication of the binding that the IdP must use when sending the assertion back. The values are: <ul style="list-style-type: none"> <li>• POST</li> <li>• Artifacts</li> </ul>                  |
| <b>SAML_COMPRESS_AUTHN_REQ</b>           | The parameter specifies whether or not to compress the authentication request when sending to the IdP. Use this option when the SAML_AUTHN_REQ_GET_OR_POST option is GET.   |
| <b>SAML HTTP Authentication Password</b> | Password corresponding to the username given in SAML_HTTP_AUTH_USERNAME   |
| <b>SAML_HTTP_AUTH_USERNAME</b>           | The user name to be used at the HTTP level for BASIC authentication when using the artifact   |

| Name                             | Description   |
|----------------------------------|---|
|                                  | resolution by contacting the SAML_ARTIFACT_RESOLUTION_URL.  |
| <b>SAML_IDP_ALIAS</b>            | <p>Following are two ways in which this parameter can be used for the signature verification: .</p> <ul style="list-style-type: none"> <li>• If a value is provided for this parameter , then the signature is verified to have been created using the certificate pointed to by this alias</li> <li>• When the signature element in the assertion does not identify the certificate used for creating the signature, then the certificate pointed to by this alias is used.</li> </ul> |
| <b>SAML_IDP_LOGIN_URL</b>        | The URL to which the authentication request is sent.  |
| <b>SAML Need Signature</b>       | The value specifies whether or not the authentication requests need to be signed. The default value is false.   |
| <b>SAML_NEED_SSL</b>             | If the URL for SAML_ARTIFACT_RESOLUTION_URL is HTTPS, then SAML_NEED_SSL must be set to true. If SSL/TLS connection is required between IAM and SAML IdP, then this should be set to TRUE   |
| <b>SAML_PROVIDER_ID</b>          | ID of the Identity provider that provides the authentication service.   |
| <b>SAML_SIGNATURE_ALIAS</b>      |   |
| <b>SAML_SP_NAME</b>              | The configuration name at the IdP that uniquely identifies this instance of IAM.  |
| <b>SAML_URL_ENCODE_AUTHN_REQ</b> | The value indicates whether or not to URL-encode the authentication request when sending to the IdP. This option is used when the SAML_AUTHN_REQ_GET_OR_POST option is GET.   |
| <b>SAML_VERIFY_SIGNATURE</b>     | The value indicates whether or not to verify the signatures in the assertions. The parameter accepts a boolean value.   |

**COMMON**

| Name                            | Description   |
|---------------------------------|---|
| <b>AUTHENTICATION_MECHANISM</b> | Determines the type of server to use. The values are: |

| Name                                  | Description  |
|---------------------------------------|--|
|                                       | <ul style="list-style-type: none"> <li>• UPM: Avaya UPM Database</li> <li>• LDAP: An LDAP or AD type server</li> <li>• RADIUS: Radius type server</li> <li>• SAML: the server to be used can act as a SAML ID</li> </ul>   |
| <b>AUTHENTICATION_MODE</b>            | <p>Determines the type of password to be used for authentication. The values are:</p> <ul style="list-style-type: none"> <li>• COMMUNICATIONS: Used for SIP authentication</li> <li>• NON-COMMUNICATIONS: Used for non-SIP authentication (for example, web access)</li> </ul> <p> <b>Note:</b><br/>Administrators are not expected to change this.</p> |
| <b>BASIC_OR_DIGEST_AUTHENTICATION</b> | <p>Determines if the digest authentication needs to be used. The values are:</p> <ul style="list-style-type: none"> <li>• DIGEST: Used for SIP authentication</li> <li>• BASIC: Must be used for all non-SIP based authentications</li> </ul> <p> <b>Note:</b><br/>Administrators are not expected to change this.</p>                                |
| <b>DIGEST_NONCE_PRIVATE_KEY</b>       | key used to create the NONCE value in the DIGEST mode.   |
| <b>DIGEST_NONCE_VALIDITY_PERIOD</b>   | Value determines if a NONCE given by the client is still valid in the DIGEST mode. This should be given in milliseconds.   |
| <b>NUMBER_OF_ACTIVE_SESSIONS</b>      | Number of active sessions that each user may have at any given time. This parameter accepts an integer value. For example, 10 means that a particular user is allowed to login through 10 different browser instances at the same time.  |
| <b>REALM_NAME</b>                     | Realm name to be used for SIP digest authentication. This parameter accepts a string value. For example, sipUsers@domain.com   |

## CONSOLE

| Name                | Description  |
|---------------------|--|
| <b>NHI_USERNAME</b> | The Non Human Interface user name. The default value is NHI. |

## LDAP

| Name                           | Description   |
|--------------------------------|---|
| <b>LDAP_BASE_DN</b>            | The base DN value to be used. The complete DN used for the authentication is LDAP_USERNAME_PREFIX + "=" + name entered by user + "," + LDAP_BASE_DN.  |
| <b>LDAP_PRIMARY_HOST</b>       | The hostname or IP address of the primary LDAP/AD Server.   |
| <b>LDAP_PRIMARY_PORT</b>       | The port number of the primary LDAP/AD server.  |
| <b>LDAP_PRIMARY_SSL_REQD</b>   | Enables or Disables TLS/SSL connection between IAM module and the primary LDAP server. This parameter accepts boolean value. <ul style="list-style-type: none"> <li>• True: Enables TLS/SSL connection between the IAM module and the primary LDAP server</li> <li>• False: Disables TLS/SSL connection between the IAM module and the primary LDAP server</li> </ul> |
| <b>LDAP_SECONDARY_HOST</b>     | This parameter specifies hostname or IP address of the LDAP secondary host. Authentication is done against this LDAP/AD Server, if the Primary LDAP/AD server specified above is unreachable.   |
| <b>LDAP Secondary Port</b>     | If AUTHENTICATION_MECHANISM is LDAP and there is a secondary LDAP server to be used as fallback when the primary is not available, then enter the port of the secondary LDAP server.  |
| <b>LDAP_SECONDARY_SSL_REQD</b> | This parameter specifies whether you can establish a TLS/SSL connection between the IAM module and the LDAP/AD server. The parameter accepts boolean value: <ul style="list-style-type: none"> <li>• True</li> <li>• False</li> </ul>   |
| <b>LDAP_USERNAME_PREFIX</b>    | The prefix for the username. The complete DN for the authentication is LDAP_USERNAME_PREFIX+ "=" + name entered by user + "," + LDAP_BASE_DN.   |

**DB**

| Name                       | Description   |
|----------------------------|---|
| <b>DB_CONNECTION_URL</b>   | <p>The JDBC specific connection URL. You can request JDBC vendor to provide information on configuring the parameter. For example,</p> <ul style="list-style-type: none"> <li>• For Oracle:<br/>jdbc:oracle:thin:@192.147.7.215:1521:avayadb, where 192.147.7.215 is the IP address of the database server and avayadb is the SID of the UPM database.</li> <li>• For PostgreSQL: jdbc:postgresql://192.147.7.215/avayadb, where 192.147.7.215 is the IP address of the database server, and avayadb is the database name.</li> </ul> <p> <b>Note:</b><br/>If SSL is required when connecting to the database, then the connection URL will look different. Please refer DB_SSL_NEEDED parameter for more information.</p> |
| <b>DB_DRIVER_CLASSNAME</b> | <p>The JDBC driver class to be used for obtaining the database connection. This class is given by the database vendor. Note that the JAR file containing this class must be present in the system classpath – for example, \$JBOSS_HOME/server/&lt;&lt;serverName&gt;&gt;/lib folder. For example,</p> <ul style="list-style-type: none"> <li>• For Oracle: oracle.jdbc.driver.OracleDriver</li> <li>• For PostgreSQL: org.postgresql.Driver</li> </ul>   |
| <b>DB_JNDI_NAME</b>        | <p>JNDI name of the datasource object configured in the J2EE server. This datasource must point to the Avaya UPM DB.</p> <p> <b>Note:</b><br/>Administrators are strongly recommended not to change the value of this parameter after a successful installation of database.</p>   |
| <b>DB_PASSWORD</b>         | Password for connecting to the database.  |
| <b>DB_SCHEMA_NAME</b>      | Name of the schema used for creating the Avaya UPM tables.  |
| <b>DB_SSL_NEEDED</b>       | Indicates whether or not SSL needs to be used for connecting to the database. This parameter accepts a boolean value.   |
| <b>DB_USERNAME</b>         | Unique name that identifies the user when connecting to the database.   |

## Radius

| Name                                  | Description  |
|---------------------------------------|--|
| <b>RADIUS_NUM_RETRIES</b>             | The number of times the client should attempt to connect to the Radius server if the server does not respond.  |
| <b>RADIUS_PRIMARY_AUTH_PORT</b>       | The port number the primary the Radius server uses to receive RADIUS authentication requests.  |
| <b>RADIUS_PRIMARY_HOST</b>            | Hostname or IP address of the primary Radius server for authentication. For example, IP address such as 192.168.111.23 or "hostname.rnd.avaya.com"   |
| <b>RADIUS_PRIMARY_SHARED_SECRET</b>   | The secret key that is used to sign RADIUS data packets to ensure they are coming from a trusted source. The Radius Server's clients configuration must be associated with this shared secret.   |
| <b>RADIUS_SECONDARY_AUTH_PORT</b>     | The port number on which the server listens for RADIUS authentication requests. Set this parameter when you use a secondary Radius server for fail over, and have provided a value for <b>RADIUS_SECONDARY_HOST</b> .  |
| <b>RADIUS_SECONDARY_HOST</b>          | The host name or IP address of the secondary Radius server that is used for fail over. Authentication is done against this Radius Server, if the Primary Radius server specified is not reachable.   |
| <b>RADIUS_SECONDARY_SHARED_SECRET</b> | The secret key configured in the secondary Radius Server's client configuration. This key will be used to sign RADIUS data packets to ensure they are coming from a trusted source. This must be provided if RADIUS_SECONDARY_HOST is provided for failover. |
| <b>RADIUS_SERVER</b>                  | The vendor name for the Radius Server. This value helps in loading the dictionary for the Radius Server. Attributes corresponding to this vendor name should be present in the AvayaRadiusClient.dict.   |
| <b>RADIUS_TIMEOUT</b>                 | The number of seconds to wait for the Radius Server to respond before the client times out the server  |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Saves the changes to the database.  |
| <b>Cancel</b> | Cancels the edit profile operation and takes you back to the View Profile:IAM page. |

**Related topics:**

[Edit software feature profiles](#) on page 1338

[System Manager security authentication mechanism](#) on page 1347

[Edit Profile:Logging Service field descriptions](#) on page 1367

---

## View Profile: System Manager Element Manager field descriptions

Use this page to view the parameters in the System Manager Element Manager profile.

**PEM-Container**

| Name                                | Description  |
|-------------------------------------|--|
| <b>Backup Directory</b>             | The name of the directory on the Database server where Element Manager creates the backup archives.<br><br> <b>Note:</b><br>The database user should have write privileges on this directory.          |
| <b>Database Utilities Path</b>      | The name of the directory on the Database server that contains the PostgreSQL backup/restore utilities.<br><br> <b>Note:</b><br>The database user should have execute permissions on these utilities. |
| <b>Database Type</b>                | Type of the database. For example, Oracle, Postgres.   |
| <b>Database server</b>              | Host name of the database server.  |
| <b>Database Super-User Password</b> | Database super user password.  |
| <b>Database Port</b>                | Port number for database server.   |
| <b>Database SCP Port</b>            | Port on the database server on which the SSH server is running.  |
| <b>Database Super-User</b>          | Database super user. This user should be able to open a SSH connection to the DB.  |
| <b>Disk Space Allocated (GB)</b>    | Disk space allocated for backup archives.  |

| Name   | Description  |
|--|--|
| <b>Disk Space Threshold (%)</b>                  | This is the percentage of the <b>diskSpaceAllocated</b> property. When this percentage is reached, an alarm is generated. So, if the <b>diskSpaceAllocated</b> is 100 MB and <b>diskSpaceThreshold</b> is 90 percent, an alarm is generated when the disk space occupied by the backup archives reaches 90 MB. |
| <b>Job Interface URL</b>                         | Lookup URL for the Element Manager.  |
| <b>Maximum Backup Files</b>                      | The maximum number of backup files that you can create. Once maximum limit is reached, the backup archives are rotated.  |
| <b>Maximum Data Retention Limit (days)</b>       | The maximum data retention limit that can be set for any data retention rule in days.  |
| <b>Maximum size for log data stored</b>          | The maximum size for log data stored. This is the upper limit on the number of records on the log_store table.   |
| <b>Maximum Transaction Timeout Limit (Hours)</b> | The maximum transaction timeout limit in hours   |
| <b>Remote Utility Directory</b>                  | Directory on the database server that contains the Element Manager backup/restore utilities.   |
| <b>Scheduler URL</b>                             | The URL for accessing the Scheduler.   |
| <b>Remote Server Password</b>                    | Password for accessing the scp server.   |
| <b>Remote Server Port</b>                        | Port for the scp server.   |
| <b>Remote server</b>                             | Host name of the scp server.   |
| <b>Remote Server User</b>                        | User name for accessing the secure access server.  |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Edit Profile:IMSM Element Manager page. Use this page to edit the parameters in the IMSM Element Manager Profile. |
| <b>Done</b> | Closes the View Profile:IMSM Element Manager page.  |

**Related topics:**

- [View software feature profiles](#) on page 1339
- [View Profile: User Bulk Import Profile field descriptions](#) on page 1379
- [View Profile: Agent Management field descriptions](#) on page 1381
- [View Profile: Alarm Management field descriptions](#) on page 1383
- [View Profile: Event processor field descriptions](#) on page 1384
- [View Profile : Data Transport Config field descriptions](#) on page 1385
- [View Profile: Data Transport Static Config field descriptions](#) on page 1388

## Edit Profile: System Manager Element Manager field descriptions

Use this page to edit the parameters in the System Manager Element Manager profile.

### PEM-Container

| Name                                       | Description  |
|--|--|
| <b>Backup Directory</b>                    | The name of the directory on the Database server where Element Manager creates the backup archives.<br><br> <b>Note:</b><br>The database user should have write privileges on this directory.                                 |
| <b>Database Utilities Path</b>             | The name of the directory on the Database server that contains the PostgreSQL backup/restore utilities.<br><br> <b>Note:</b><br>The database user should have execute permissions on these utilities.                         |
| <b>Database Type</b>                       | Type of the database. For example, Oracle, Postgres.   |
| <b>Database server</b>                     | Host name of the database server.  |
| <b>Database Super-User Password</b>        | Database super user password.  |
| <b>Database Port</b>                       | Port number for database server.   |
| <b>Database SCP Port</b>                   | Port on the database server on which the SSH server is running.  |
| <b>Database Super-User</b>                 | Database super user. This user should be able to open a SSH connection to the DB.  |
| <b>Disk Space Allocated (GB)</b>           | Disk space allocated for backup archives.  |
| <b>Disk Space Threshold (%)</b>            | This is the percentage of the <b>diskSpaceAllocated</b> property. When this percentage is reached, an alarm is generated. So, if the <b>diskSpaceAllocated</b> is 100 MB and <b>diskSpaceThreshold</b> is 90 percent, an alarm is generated when the disk space occupied by the backup archives reaches 90 MB. |
| <b>Job Interface URL</b>                   | Lookup URL for the Element Manager.  |
| <b>Maximum Backup Files</b>                | The maximum number of backup files that you can create. Once maximum limit is reached, the backup archives are rotated.  |
| <b>Maximum Data Retention Limit (days)</b> | The maximum data retention limit that can be set for any data retention rule in days.  |

| Name   | Description  |
|--|--|
| <b>Maximum size for log data stored</b>          | The maximum size for log data stored. This is the upper limit on the number of records on the log_store table. |
| <b>Maximum Transaction Timeout Limit (Hours)</b> | The maximum transaction timeout limit in hours   |
| <b>Remote Utility Directory</b>                  | Directory on the database server that contains the Element Manager backup/restore utilities.                   |
| <b>Scheduler URL</b>                             | The URL for accessing the Scheduler.   |
| <b>Remote Server Password</b>                    | Password for accessing the scp server.   |
| <b>Remote Server Port</b>                        | Port for the scp server.   |
| <b>Remote server</b>                             | Host name of the scp server.   |
| <b>Remote Server User</b>                        | User name for accessing the secure access server.  |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Saves the changes to the database.  |
| <b>Cancel</b> | Cancel the edit profile operation for IMSM Element Manager and takes you back to the View Profile: IMSM Element Manager page. |

**Related topics:**

[Edit software feature profiles](#) on page 1338

[Edit Profile:Logging Service field descriptions](#) on page 1367

## View Profile:Logging field descriptions

Use this page to view the parameters in the Logging profile.

### Log Severity Levels

| Name             | Description   |
|------------------|---|
| <b>Alert</b>     | The color code for the log messages that are logged under the Alert severity level.     |
| <b>Critical</b>  | The color code for the log messages that are logged under the Critical severity level.  |
| <b>Emergency</b> | The color code for the log messages that are logged under the Emergency severity level. |
| <b>Error</b>     | The color code for the log messages that are logged under the Error severity level.     |

| Name                 | Description   |
|----------------------|---|
| <b>Informational</b> | The color code for the log messages that are logged under the Informational severity level. |
| <b>Notice</b>        | The color code for the log messages that are logged under the Notice severity level.        |
| <b>Warning</b>       | The color code for the log messages that are logged under the Notice severity level.        |

## Auto Refresh

| Name                              | Description   |
|-----------------------------------|---|
| <b>auto_refresh_time_interval</b> | The time interval in milliseconds after which the log messages are auto refreshed on the Logging page . |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Edit Profile:Logging page. Use this page to edit the parameters in the Logging profile. |
| <b>Done</b> | Closes the View Profile:Logging page.   |

## Related topics:

[View software feature profiles](#) on page 1339

[View Profile: User Bulk Import Profile field descriptions](#) on page 1379

[View Profile: Agent Management field descriptions](#) on page 1381

[View Profile: Alarm Management field descriptions](#) on page 1383

[View Profile: Event processor field descriptions](#) on page 1384

[View Profile : Data Transport Config field descriptions](#) on page 1385

[View Profile: Data Transport Static Config field descriptions](#) on page 1388

---

## Edit Profile:Logging field descriptions

Use this page to edit the parameters in the Logging profile.

### Log Severity Levels

| Name            | Description  |
|-----------------|--|
| <b>Alert</b>    | The color code for the log messages that are logged under the Alert severity level.    |
| <b>Critical</b> | The color code for the log messages that are logged under the Critical severity level. |

| Name                 | Description   |
|----------------------|---|
| <b>Emergency</b>     | The color code for the log messages that are logged under the Emergency severity level.     |
| <b>Error</b>         | The color code for the log messages that are logged under the Error severity level.         |
| <b>Informational</b> | The color code for the log messages that are logged under the Informational severity level. |
| <b>Notice</b>        | The color code for the log messages that are logged under the Notice severity level.        |
| <b>Warning</b>       | The color code for the log messages that are logged under the Notice severity level.        |

### Auto Refresh

| Name                              | Description   |
|-----------------------------------|---|
| <b>auto_refresh_time_interval</b> | The time interval in milliseconds after which the log messages are auto refreshed on the Logging page . |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | Saves the changes to the database.   |
| <b>Cancel</b> | Cancel the edit profile operation and takes you back to the View Profile:Logging page. |

---

## View Profile:Logging Service field descriptions

Use this page to view the parameters and their corresponding values that specify the default settings for log harvesting service.

| Name                                | Description  |
|-------------------------------------|--|
| <b>Max time interval to wait</b>    | The maximum time interval for which the system waits between a request and a response for harvesting a log file from a remote System Manager computer. You can specify a time interval between 1800000 milliseconds to maximum value of 7200000 milliseconds. The default value is 7200000 milliseconds. |
| <b>Size of the File Buffer</b>      | The value in this field is the buffer size for the files displayed to the log harvesting user interface. The minimum size of the file buffer is 10000 bytes and maximum value is 5000000 bytes.  |
| <b>Size of the LRU buffer cache</b> | The value in this field is the size of the cache. The files that you view or search are temporarily stored in the cache. If you open a file after the cache becomes full, the least recently used file is removed from   |

| Name  | Description  |
|---|--|
|   | the cache and the new file is stored in the cache. The system takes less time to open and display a file that is in cache.   |
| <b>Directory path for harvested files</b>                               | The directory where all the harvested files are stored. The default path is <code>/var/log/Avaya/mgmt/downloads</code> .   |
| <b>Number of Lines in a Log Browser page (Requires Service Restart)</b> | The value is the maximum number of lines that you can view on the log browser page for a harvested log file.   |
| <b>Maximum allowed size of harvest directory</b>                        | The maximum size of the harvested files directory. The value of minimum size of the harvested directory is 1 GB and maximum size can be 10 GB.   |
| <b>No. of files for File rotation</b>                                   | The maximum number of harvested files that the system can store before the oldest file is overwritten by the new harvested file. You can set 10 as minimum number of files and 9999999 as maximum number of files. |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Edit Logging Service Profile page. Use this page to edit the values of the log harvesting parameters. |
| <b>Done</b> | Closes the View Logging Service Profile page.   |

---

## Edit Profile:Logging Service field descriptions

Use this page to modify the value of parameters that define settings for log harvesting.

| Name                                | Description   |
|-------------------------------------|---|
| <b>Max time interval to wait</b>    | The maximum time interval for which the system waits between a request and a response for harvesting a log file from a remote System Manager computer. You can specify a time interval between 1800000 milliseconds to maximum value of 7200000 milliseconds. The default value is 7200000 milliseconds.  |
| <b>Size of the File Buffer</b>      | The value in this field is the buffer size for the files displayed to the log harvesting user interface. The minimum size of the file buffer is 10000 bytes and maximum value is 5000000 bytes.   |
| <b>Size of the LRU buffer cache</b> | The value in this field is the size of the cache. The files that you view or search are temporarily stored in the cache. If you open a file after the cache becomes full, the least recently used file is removed from the cache and the new file is stored in the cache. The system takes less time to open and display a file that is in the cache. |

| Name  | Description  |
|---|--|
| <b>Directory path for harvested files</b>                               | The directory where all the harvested files are stored. The default path is /var/log/Avaya/mgmt/downloads.   |
| <b>Number of Lines in a Log Browser page (Requires Service Restart)</b> | The value is the maximum number of lines that you can view on the log browser page for a harvested log file.   |
| <b>Maximum allowed size of harvest directory</b>                        | The maximum size of the harvested files directory. The value of minimum size of the harvested directory is 1 GB and maximum size can be 10 GB.   |
| <b>No. of files for File rotation</b>                                   | The maximum number of harvested files that the system can store before the oldest file is overwritten by the new harvested file. You can set 10 as minimum number of files and 9999999 as maximum number of files. |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Saves the changes to the database.  |
| <b>Cancel</b> | Cancels the edit profile operation and takes you back to the View Profile:Logging Service page. |

**Related topics:**

[Edit software feature profiles](#) on page 1338

## View Profile:Scheduler field descriptions

Use this page to view the parameters in the Scheduler profile.

### PropertyContainer

| Name                  | Description   |
|-----------------------|---|
| <b>pe_noof_retry</b>  | A count that defines the number of attempts to start the scheduler MBEAN. |
| <b>Pe_retry_delay</b> | Delay in time in seconds between each retry.                              |

### Container

| Name                   | Description   |
|------------------------|---|
| <b>smm_context_str</b> | Constant that holds the name of the environment property for specifying the initial context factory to use. |

| Name                  | Description   |
|-----------------------|---|
|                       |  <b>Note:</b><br>This parameter is currently not in use.   |
| <b>smm_credential</b> | Credential for connecting to the secured Java Naming and Directory Interface (JNDI).<br><br> <b>Note:</b><br>This parameter is currently not in use. |
| <b>smm_principal</b>  | User name for secured Java Naming and Directory Interface (JNDI).   |
| <b>smm_url</b>        | The PROVIDER_URL which gives the server name and port on which a service is running.<br><br> <b>Note:</b><br>This parameter is currently not in use. |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Edit Profile:Scheduler page. Use this page to edit the parameters in the Scheduler profile. |
| <b>Done</b> | Closes the View Profile:Scheduler page.   |

**Related topics:**

[View software feature profiles](#) on page 1339

[View Profile: User Bulk Import Profile field descriptions](#) on page 1379

[View Profile: Agent Management field descriptions](#) on page 1381

[View Profile: Alarm Management field descriptions](#) on page 1383

[View Profile: Event processor field descriptions](#) on page 1384

[View Profile : Data Transport Config field descriptions](#) on page 1385

[View Profile: Data Transport Static Config field descriptions](#) on page 1388

---

## Edit Profile:Scheduler field descriptions

Use this page to edit the parameters in the Scheduler profile.

**PropertyContainer**

| Name                  | Description   |
|-----------------------|---|
| <b>pe_noof_retry</b>  | A count that defines the number of attempts to start the scheduler MBEAN. |
| <b>Pe_retry_delay</b> | Delay in time in seconds between each retry.                              |

## Container

| Name                   | Description  |
|------------------------|--|
| <b>smm_context_str</b> | Constant that holds the name of the environment property for specifying the initial context factory to use.<br><br> <b>Note:</b><br>This parameter is currently not in use. |
| <b>smm_credential</b>  | Credential for connecting to the secured Java Naming and Directory Interface (JNDI).<br><br> <b>Note:</b><br>This parameter is currently not in use.                        |
| <b>smm_principal</b>   | User name for secured Java Naming and Directory Interface (JNDI).  |
| <b>smm_url</b>         | The PROVIDER_URL which gives the server name and port on which a service is running.<br><br> <b>Note:</b><br>This parameter is currently not in use.                        |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Saves the changes to the database.  |
| <b>Cancel</b> | Cancels the edit profile operation and takes you back to the View Profile:Scheduler page. |

### Related topics:

[Edit software feature profiles](#) on page 1338

[Edit Profile:Logging Service field descriptions](#) on page 1367

---

## View Profile:SNMP field descriptions

Use this page to view the parameters in the SNMP profile.

### Avaya IM System Manager subagent attributes

| Name                          | Description   |
|-------------------------------|---|
| <b>Master Agent IPAddress</b> | IP address of machine on which master agent is running.   |
| <b>Master Agent TCP Port</b>  | The connection between master agent and subagent is established via a TCP port using AgentX protocol. This port has to be configured with both the master agent and the subagent so that the master agent |

| Name                       | Description   |
|----------------------------|---|
|                            | starts listening on the configured TCP port and then the subagent establishes connection with the master agent via this port. |
| <b>Sub Agent IPAddress</b> | IP address of machine on which sub agent is deployed  |

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the Edit Profile:SNMP page. Use the page to edit the parameters in the SNMP profile. |
| <b>Done</b> | Closes the View Profile: SNMP page.  |

**Related topics:**

[View software feature profiles](#) on page 1339

[View Profile: User Bulk Import Profile field descriptions](#) on page 1379

[View Profile: Agent Management field descriptions](#) on page 1381

[View Profile: Alarm Management field descriptions](#) on page 1383

[View Profile: Event processor field descriptions](#) on page 1384

[View Profile : Data Transport Config field descriptions](#) on page 1385

[View Profile: Data Transport Static Config field descriptions](#) on page 1388

---

## Edit Common Console Profile field descriptions

Use this page to edit the common console profile.

| Name                          | Description   |
|-------------------------------|---|
| <b>Global session timeout</b> | Timeout period for global session. By default, the timeout period for global session is 30 minutes. The range is minimum -30 minutes and maximum - 480 minutes. |
| <b>Number of rows</b>         | Number of rows to be displayed in table. The default count is 15 . The range of minimum rows is 15 and maximum rows is 100.                                     |

| Button        | Description                         |
|---------------|-------------------------------------|
| <b>Commit</b> | Saves the changes to the database.  |
| <b>Cancel</b> | Cancels the edit profile operation. |

**Related topics:**

[Edit software feature profiles](#) on page 1338

[Edit Profile:Logging Service field descriptions](#) on page 1367

## View Common Console Profile field descriptions

Use this page to view the common console profile.

| Name                          | Description   |
|-------------------------------|---|
| <b>Global session timeout</b> | Timeout period for global session. By default, the timeout period for global session is 30 minutes. The range is minimum -30 minutes and maximum - 480 minutes. |
| <b>Number of rows</b>         | Number of rows to be displayed in table. The default count is 15 . The range of minimum rows is 15 and maximum rows is 100.                                     |

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the Edit Profile: Common Console page. Use this page to edit the parameters in the Common Console profile. |
| <b>Done</b> | Closes the View Profile: Common Console page.  |

### Related topics:

[View software feature profiles](#) on page 1339

[View Profile: User Bulk Import Profile field descriptions](#) on page 1379

[View Profile: Agent Management field descriptions](#) on page 1381

[View Profile: Alarm Management field descriptions](#) on page 1383

[View Profile: Event processor field descriptions](#) on page 1384

[View Profile : Data Transport Config field descriptions](#) on page 1385

[View Profile: Data Transport Static Config field descriptions](#) on page 1388

## Edit Profile: Communication System Management Configuration field descriptions

Use this page to edit the parameters in the Communication System Management Configuration profile.

### General Properties

| Name                      | Description   |
|---------------------------|---|
| <b>application_prefix</b> | The default value in this field is CSM. This application prefix appears as the prefix in the Communication System Management job names. |

## Telephony

| Name                                      | Description   |
|---|---|
| <b>incremental_sync_interval_in_hours</b> | The time between every incremental synchronization. By default, the value for the incremental_sync_interval_in_hours field is 24. |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Saves the changes to the database.  |
| <b>Cancel</b> | Cancels the edit profile operation and takes you back to the Edit Profile:Communication System Management Configuration page. |

### Related topics:

[Edit software feature profiles](#) on page 1338

[Edit Profile:Logging Service field descriptions](#) on page 1367

---

## View Profile: Communication System Management Configuration field descriptions

Use this page to edit the parameters in the Communication System Management Configuration profile.

### General Properties

| Name                      | Description   |
|---------------------------|---|
| <b>application_prefix</b> | The default value in this field is CSM. This application prefix appears as the prefix in the Communication System Management job names. |

## Telephony

| Name                                      | Description   |
|---|---|
| <b>incremental_sync_interval_in_hours</b> | The time between every incremental synchronization. By default, the value for the incremental_sync_interval_in_hours field is 24. |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Edit Profile:Communication System Management Configuration page. Use this page to edit the parameters in the Scheduler profile. |
| <b>Done</b> | Closes the Edit Profile:Communication System Management Configuration page.   |

**Related topics:**

- [View software feature profiles](#) on page 1339
- [View Profile: User Bulk Import Profile field descriptions](#) on page 1379
- [View Profile: Agent Management field descriptions](#) on page 1381
- [View Profile: Alarm Management field descriptions](#) on page 1383
- [View Profile: Event processor field descriptions](#) on page 1384
- [View Profile : Data Transport Config field descriptions](#) on page 1385
- [View Profile: Data Transport Static Config field descriptions](#) on page 1388

## Edit Profile: Role Bulk Import Profile field descriptions

Use this page to modify the value of parameters that define settings for bulk importing role records.

### Role Bulk Import Module

| Name                                      | Description  |
|---|--|
| <p><b>Default Error Configuration</b></p> | <p>The value in this field specifies what action the system performs when an error is encountered during bulk importing roles record in the system. The options are:</p> <ul style="list-style-type: none"> <li>• True: When this parameter is set to true, the system skips the erroneous record in the input file and continue to import other records. This is the default value.<br/>If this parameter is set to true, the <b>Continue processing other records</b> option is set as the default option for the <b>Select error configuration</b> field on the Import Roles page.</li> <li>• False: When this parameter is set to false, the system aborts the importing process on encountering the first error in the input file.<br/>If this parameter is set to false, the <b>Abort on first error</b> option is set as default option for the <b>Select error configuration</b> field on the Import Roles page.</li> </ul> <p>To access the Import Roles page, click <b>Groups &amp; Roles &gt; More Actions &gt; Import Roles</b>.</p> |
| <p><b>Schedule Job</b></p>                | <p>The value in this field specifies the default scheduling option for importing a roles job. The options are:</p> <ul style="list-style-type: none"> <li>• True: When this parameter is set to true, the system run the bulk importing roles job immediately. This is the default value.<br/>If this parameter is set to true, the <b>Run immediately</b> option is set as the default option for the <b>Schedule job</b> field on the Import Roles page.</li> <li>• False: When this parameter is set to false, you can set the date and time of running the bulk importing roles job.</li> </ul>  |

| Name   | Description   |
|--|---|
|  | <p>If this parameter is set to false, the <b>Schedule later</b> option is set as the default option for the <b>Schedule job</b> field on the Import Roles page.</p> <p>To access the Import Roles page, click <b>Groups &amp; Roles &gt; More Actions &gt; Import Roles</b>.</p>  |
| <b>Maximum Number of Error records to be displayed</b> | <p>The value in this field specifies the maximum number of error records that the Job Details page can display for a role importing job that has failed.</p> <p>To access the Job Details page, click <b>Groups &amp; Roles &gt; More Actions &gt; Import Roles &gt; View Job</b>.<br/>Select a failed job from the table before you click <b>View Job</b>.</p>   |
| <b>Maximum Number of Job records to be displayed</b>   | <p>The value in this field specifies the maximum number of job records that the system displays on the Import Roles page.</p>   |
| <b>Default Action for a matching record</b>            | <p>The value specifies a default action that the system performs when the system finds a matching record in the database while bulk importing roles. The options are:</p> <ul style="list-style-type: none"> <li>• 0: When you set 0 for this parameter, the system does not import role records from the input file that already exists in the database.<br/>If you enter 0, the <b>Skip</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Roles page..</li> <li>• 1: When you set 1 for this parameter, the system appends the records for an attribute.<br/>If you enter 1, the <b>Merge</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Roles page..</li> <li>• 2: When you set the value of this parameter to 2, the system replaces the record with the record in the input file if a matching record is found.<br/>If you enter 2, the <b>Replace</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Roles page.</li> <li>• 3: When you set the value of this parameter to 3, the system deletes the records from the database that matches the records in the input file.<br/>If you enter 3, the <b>Delete</b> option is set as the default option for the <b>If a matching record already exists</b> field.</li> </ul> <p>To access the Import Roles page, click <b>Groups &amp; Roles &gt; More Actions &gt; Import Roles</b>.</p> |

| Button        | Description                        |
|---------------|------------------------------------|
| <b>Commit</b> | Saves the changes to the database. |

| Button | Description   |
|--------|---|
| Cancel | Cancels the edit profile operation and takes you back to the Edit Profile: Role Bulk Import Profile page. |

## View Profile: Role Bulk Import Profile field descriptions

Use this page to view the parameters and their corresponding values that specify bulk import settings for importing roles records.

### Role Bulk Import Module

| Name                               | Description  |
|------------------------------------|--|
| <b>Default Error Configuration</b> | <p>The value in this field specifies what action the system performs when an error is encountered during bulk importing roles record in the system. The options are:</p> <ul style="list-style-type: none"> <li>• True: When this parameter is set to true, the system skips the erroneous record in the input file and continue to import other records. This is the default value.<br/>If this parameter is set to true, the <b>Continue processing other records</b> option is set as the default option for the <b>Select error configuration</b> field on the Import Roles page.</li> <li>• False: When this parameter is set to false, the system aborts the importing process on encountering the first error in the input file.<br/>If this parameter is set to false, the <b>Abort on first error</b> option is set as default option for the <b>Select error configuration</b> field on the Import Roles page.</li> </ul> <p>To access the Import Roles page, click <b>Groups &amp; Roles &gt; More Actions &gt; Import Roles</b>.</p> |
| <b>Schedule Job</b>                | <p>The value in this field specifies the default scheduling option for importing a roles job. The options are:</p> <ul style="list-style-type: none"> <li>• True: When this parameter is set to true, the system run the bulk importing roles job immediately. This is the default value.<br/>If this parameter is set to true, the <b>Run immediately</b> option is set as the default option for the <b>Schedule job</b> field on the Import Roles page.</li> <li>• False: When this parameter is set to false, you can set the date and time of running the bulk importing roles job.<br/>If this parameter is set to false, the <b>Schedule later</b> option is set as the default option for the <b>Schedule job</b> field on the Import Roles page.</li> </ul> <p>To access the Import Roles page, click <b>Groups &amp; Roles &gt; More Actions &gt; Import Roles</b>.</p>  |

| Name   | Description   |
|--|---|
| <b>Maximum Number of Error records to be displayed</b> | <p>The value in this field specifies the maximum number of error records that the Job Details page can display for a role importing job that has failed.</p> <p>To access the Job Details page, click <b>Groups &amp; Roles &gt; More Actions &gt; Import Roles &gt; View Job</b>.</p> <p>Select a failed job from the table before you click <b>View Job</b>.</p>  |
| <b>Maximum Number of Job records to be displayed</b>   | <p>The value in this field specifies the maximum number of job records that the system displays on the Import Roles page.</p>   |
| <b>Default Action for a matching record</b>            | <p>The value specifies a default action that the system performs when the system finds a matching record in the database while bulk importing roles. The options are:</p> <ul style="list-style-type: none"> <li>• 0: When you set 0 for this parameter, the system does not import role records from the input file that already exists in the database.<br/>If you enter 0, the <b>Skip</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Roles page..</li> <li>• 1: When you set 1 for this parameter, the system appends the records for an attribute.<br/>If you enter 1, the <b>Merge</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Roles page..</li> <li>• 2: When you set the value of this parameter to 2, the system replaces the record with the record in the input file if a matching record is found.<br/>If you enter 2, the <b>Replace</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Roles page.</li> <li>• 3: When you set the value of this parameter to 3, the system deletes the records from the database that matches the records in the input file.<br/>If you enter 3, the <b>Delete</b> option is set as the default option for the <b>If a matching record already exists</b> field.</li> </ul> <p>To access the Import Roles page, click <b>Groups &amp; Roles &gt; More Actions &gt; Import Roles</b>.</p> |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Edit Profile:Role Bulk Import Profile page. You can use this page to modify the values set for the role bulk import parameters. |

## Edit Profile: User Bulk Import Profile field descriptions

Use this page to modify the value of parameters that define settings for bulk importing users records.

### User Bulk Import Module

| Name  | Description   |
|---|---|
| <p><b>Default Error Configuration</b></p>                     | <p>The value in this field specifies what action the system performs when an error is encountered during bulk importing users record in the system. The options are:</p> <ul style="list-style-type: none"> <li>• True: When this parameter is set to true, the system skips the erroneous record in the input file and continue to import other records. This is the default value.<br/>If this parameter is set to true, the <b>Continue processing other records</b> option is set as the default option for the <b>Select error configuration</b> field on the Import Users page.</li> <li>• False: When this parameter is set to false, the system aborts the importing process on encountering the first error in the input file.<br/>If this parameter is set to false, the <b>Abort on first error</b> option is set as default option for the <b>Select error configuration</b> field on the Import Users page.</li> </ul> <p>To access the Import Users page, click <b>Manage Users &gt; More Actions &gt; Import Users</b></p> |
| <p><b>Enable Error File Generation</b></p>                    | <p>The value in this field specifies the error file generation options for an importing users job. The options are:</p> <ul style="list-style-type: none"> <li>• True: When this parameter is set to true, the system generates an error file for a failed import.</li> <li>• False: When this parameter is set to false, the system does not generate an error file for a failed import.</li> </ul>  |
| <p><b>Maximum Number of Error records to be displayed</b></p> | <p>The value in this field specifies the maximum number of error records that the Job Details page can display for a user importing job that has failed to import user records completely or partially.<br/>To access the Import Users page, click <b>Manage Users &gt; More Actions &gt; Import Users &gt; View Job</b><br/>Select a failed job from the table before you click <b>View Job</b></p>  |
| <p><b>Maximum Number of Job records to be displayed</b></p>   | <p>The value in this field specifies the maximum number of job records that the system displays on the Import Users page.</p>   |

| Name  | Description  |
|---|--|
| <b>Default Action for a matching record</b> | <p>The value specifies a default action that the system performs when the system finds a matching record in the database while bulk importing users. The options are:</p> <ul style="list-style-type: none"> <li>• 0: When you set 0 for this parameter, the system does not import user records from the input file that already exists in the database. If you enter 0, the <b>Skip</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Users page..</li> <li>• 1: When you set 1 for this parameter, the system appends the records for an attribute. If you enter 1, the <b>Merge</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Users page..</li> <li>• 2: When you set the value of this parameter to 2, the system replaces the record with the record in the input file if a matching record is found. If you enter 2, the <b>Replace</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Users page.</li> <li>• 3: When you set the value of this parameter to 3, the system deletes the records from the database that matches the records in the input file. If you enter 3, the <b>Delete</b> option is set as the default option for the <b>If a matching record already exists</b> field.</li> </ul> <p>To access the Import Users page, click <b>Manage Users &gt; More Actions &gt; Import Users</b></p> |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Edit Profile:User Bulk Import Profile page. You can use this page to modify the values set for the user bulk import parameters. |

## View Profile: User Bulk Import Profile field descriptions

Use this page to view the parameters and their corresponding values that specify the default settings for bulk importing user records.

## User Bulk Import Module

| Name  | Description   |
|---|---|
| <p><b>Default Error Configuration</b></p>                     | <p>The value in this field specifies what action the system performs when an error is encountered during bulk importing users record in the system. The options are:</p> <ul style="list-style-type: none"> <li>• True: When this parameter is set to true, the system skips the erroneous record in the input file and continue to import other records. This is the default value.<br/>If this parameter is set to true, the <b>Continue processing other records</b> option is set as the default option for the <b>Select error configuration</b> field on the Import Users page.</li> <li>• False: When this parameter is set to false, the system aborts the importing process on encountering the first error in the input file.<br/>If this parameter is set to false, the <b>Abort on first error</b> option is set as default option for the <b>Select error configuration</b> field on the Import Users page.</li> </ul> <p>To access the Import Users page, click <b>Manage Users &gt; More Actions &gt; Import Users</b></p> |
| <p><b>Enable Error File Generation</b></p>                    | <p>The value in this field specifies the error file generation options for an importing users job. The options are:</p> <ul style="list-style-type: none"> <li>• True: When this parameter is set to true, the system generates an error file for a failed import.</li> <li>• False: When this parameter is set to false, the system does not generate an error file for a failed import.</li> </ul>  |
| <p><b>Maximum Number of Error records to be displayed</b></p> | <p>The value in this field specifies the maximum number of error records that the Job Details page can display for a user importing job that has failed to import user records completely or partially.</p> <p>To access the Import Users page, click <b>Manage Users &gt; More Actions &gt; Import Users &gt; View Job</b><br/>Select a failed job from the table before you click <b>View Job</b></p>   |
| <p><b>Maximum Number of Job records to be displayed</b></p>   | <p>The value in this field specifies the maximum number of job records that the system displays on the Import Users page.</p>   |
| <p><b>Default Action for a matching record</b></p>            | <p>The value specifies a default action that the system performs when the system finds a matching record in the database while bulk importing users. The options are:</p> <ul style="list-style-type: none"> <li>• 0: When you set 0 for this parameter, the system does not import user records from the input file that already exists in the database.<br/>If you enter 0, the <b>Skip</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Users page..</li> <li>• 1: When you set 1 for this parameter, the system appends the records for an attribute.</li> </ul>  |

| Name | Description   |
|------|---|
|      | <p>If you enter 1, the <b>Merge</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Users page..</p> <ul style="list-style-type: none"> <li>• 2: When you set the value of this parameter to 2, the system replaces the record with the record in the input file if a matching record is found.<br/>If you enter 2, the <b>Replace</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Users page.</li> <li>• 3: When you set the value of this parameter to 3, the system deletes the records from the database that matches the records in the input file.<br/>If you enter 3, the <b>Delete</b> option is set as the default option for the <b>If a matching record already exists</b> field.</li> </ul> <p>To access the Import Users page, click <b>Manage Users &gt; More Actions &gt; Import Users</b></p> |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Edit Profile:User Bulk Import Profile page. You can use this page to modify the values set for the user bulk import parameters. |

**Related topics:**

[View software feature profiles](#) on page 1339

[View Profile: Agent Management field descriptions](#) on page 1381

[View Profile: Alarm Management field descriptions](#) on page 1383

[View Profile: Event processor field descriptions](#) on page 1384

[View Profile : Data Transport Config field descriptions](#) on page 1385

[View Profile: Data Transport Static Config field descriptions](#) on page 1388

---

## View Profile: Agent Management field descriptions

Use this page to view the parameters and their values that are set for managing agents.

| Name                            | Description  |
|---------------------------------|--|
| <b>Alarm aging keep time</b>    | This field is not used for System Manager.   |
| <b>Enterprise auto download</b> | The value in this field specifies whether to enable or disable enterprise auto downloading. The default value is false.<br>If the value is set to true, the enterprise downloads the base rules for all registered agents. |

| Name                                     | Description  |
|--|--|
| <b>Enterprise customer reference</b>     | The customer reference for the Enterprise. For example, Avaya. A value in this field is required only if polling to upstream enterprise is enabled.  |
| <b>Enterprise heartbeat interval</b>     | The time in seconds between heartbeats for Enterprise to Enterprise communication. A value in this field is required only if polling to upstream enterprise is enabled.  |
| <b>Enterprise heartbeat threshold</b>    | The heartbeat threshold in seconds for the Enterprise. A value in this field is required only if polling to upstream enterprise is enabled.  |
| <b>Enterprise platform name</b>          | The value in this field specifies a fully-qualified DataTransport address of the host Enterprise.<br>For example: The value of this field will be "avaya.com., Enterprise-dtxjbss01", if the OrganizationFQDN value is "avaya.com." and SpiritPlatformQualifier value is "Enterprise-dtxjbss01".<br>A value in this field is required only if polling to upstream enterprise is enabled.         |
| <b>Enterprise tenancy support</b>        | This field is for tenancy support of SAL. This field is not used for System Manager.   |
| <b>Enterprise upstream platform name</b> | The value specifies a fully-qualified Data Transport address of the upstream enterprise.<br>For example: The value of this field is "avaya.com., Enterprise-dtxapp06", if the Connection.AvayaTest.FQDN value is "avaya.com." and Connection.AvayaTest.PlatformQualifier value is "Enterprise-dtxapp06".<br>A value in this field is required only if polling to upstream enterprise is enabled. |
| <b>Enterprise upstream polling</b>       | The value in this field specifies whether polling upstream enterprise is enabled or not. The default value is false.<br>A false value disables upstream Enterprise polling or Cascading Enterprise.  |
| <b>Inventory aging keep time</b>         | This field is not used for System Manager.   |
| <b>Inventory change keep time</b>        | This field is not used for System Manager.   |
| <b>Out Of Service delete time</b>        | This field is not used for System Manager.   |

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the Edit Profile: Agent Management page. Use this page to edit the parameters in the Agent Management profile. |

| Button | Description                                     |
|--------|---|
| Done   | Closes the View Profile: Agent Management page. |

**Related topics:**

[View software feature profiles](#) on page 1339

[View Profile: User Bulk Import Profile field descriptions](#) on page 1379

[View Profile: Alarm Management field descriptions](#) on page 1383

[View Profile: Event processor field descriptions](#) on page 1384

[View Profile : Data Transport Config field descriptions](#) on page 1385

[View Profile: Data Transport Static Config field descriptions](#) on page 1388

---

## View Profile: Alarm Management field descriptions

Use this page to view the parameters and their values that are set for managing alarms generated by System Manager and its components.

| Name                                   | Description  |
|--|--|
| <b>Email from address</b>              | The value is the e-mail address of the alarm manager.<br>For example: alarmgr@avaya.com  |
| <b>Email hostname</b>                  | The value is the name of the SMTP e-mail host.<br>For example, "306181anex4.global.avaya.com"  |
| <b>Email to addresses</b>              | The values are comma separated list of e-mail addresses to which alarms are forwarded.   |
| <b>Email user id</b>                   | The value is the e-mail address of the user.   |
| <b>Federation member platform name</b> | A fully qualified data transport address to which alarms are forwarded.<br>For example, the value of this field will be "avaya.com., Enterprise-dtxapp06", if the Connection.AvayaTest.FQDN value is "avaya.com." and Connection.AvayaTest.PlatformQualifier value is "Enterprise-dtxapp06". |
| <b>NMS forward</b>                     | The value specifies whether alarms are to be forwarded to Network Management System (NMS). The default value is false.<br>If set to true, the SAL forwards the alarms to the NMS   |
| <b>NMS urls</b>                        | A comma separated list of NMS (Network Management System) URLs.<br>For example, "[155.184.73.11:162]"<br>There are no default values from SAL Enterprise and you need to update them later.  |
| <b>SPIRIT ui url</b>                   | The URL for accessing theala SAL Web interface for viewing a specific alarm.   |
| <b>Trouble ticket url</b>              | The URL for accessing the Trouble Ticket Web interface.  |

| Name | Description   |
|------|---|
|      |  <b>Note:</b><br>Do not change this value. |

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the Edit Profile: Alarm Management page. Use this page to edit the parameters in the Alarm Management profile. |
| <b>Done</b> | Closes the View Profile: Alarm Management page.  |

**Related topics:**

[View software feature profiles](#) on page 1339

[View Profile: User Bulk Import Profile field descriptions](#) on page 1379

[View Profile: Agent Management field descriptions](#) on page 1381

[View Profile: Event processor field descriptions](#) on page 1384

[View Profile : Data Transport Config field descriptions](#) on page 1385

[View Profile: Data Transport Static Config field descriptions](#) on page 1388

---

## View Profile: Event processor field descriptions

Use this page to view the parameters and their values that are set for managing events.

| Name                             | Description  |
|----------------------------------|--|
| <b>EP mechanism class name 1</b> | This field is not used for System Manager.   |
| <b>EP mechanism XSD type</b>     | <p>The value in this field specifies event processor uses a set of XML rule configuration files to describe the rules to be used to process events. The event processor uses a different processing mechanisms as indicated by the type of rule listed in a rule configuration file. A mapping between the XSD types describes rules and the java classes used to implement the rule processing mechanisms is required. For every concrete XSDType used to implement a processingMechanismConfigurationType, the event processor must have a mapping to an available java class. The XSDType: Java Class mappings are done by creating sets of matching pair entries in the &lt;Attributes &gt; element below:</p> <ol style="list-style-type: none"> <li>1. The first is a &lt;string&gt; element with a name of "EPMechanismXSDType.N" where N is a positive integer. The value of the entry indicates the full URI of the type name, including the namespace.</li> <li>2. The second is an &lt;string&gt; element named "EPMechanismClassName.N" where N matches the appropriate</li> </ol> |

| Name                        | Description   |
|-----------------------------|---|
|                             | EPMechanismXSDType entry. The Event Processor will incrementally search for XSDType->Class mappings, beginning with an "N" of 1 and working incrementally positive until it can't find a type or class for the current N.</string></string ></Attributes> |
| <b>EP transport address</b> | This field is not used for System Manager.  |

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the Edit Profile: Event processor page. Use this page to edit the parameters in the Event processor profile. |
| <b>Done</b> | Closes the View Profile: Event processor page.   |

**Related topics:**

[View software feature profiles](#) on page 1339

[View Profile: User Bulk Import Profile field descriptions](#) on page 1379

[View Profile: Agent Management field descriptions](#) on page 1381

[View Profile: Alarm Management field descriptions](#) on page 1383

[View Profile : Data Transport Config field descriptions](#) on page 1385

[View Profile: Data Transport Static Config field descriptions](#) on page 1388

---

## View Profile : Data Transport Config field descriptions

Use this page to view the parameters and their values that are set for data transport configuration.

| Name  | Description   |
|---|---|
| <b>Connection Avaya production FQDN</b>               | The value is a fully qualified domain name of the target Enterprise for a connection. This may identify a customer, Business Partner or Avaya itself. For example, avaya.com, company.com   |
| <b>Connection Avaya production keyAlias</b>           | The value specifies the alias of a key in the keyStore to be used for client authentication in HTTPS sessions when communicating with an upstream server. Typically used when Avaya is the upstream server.<br>This is an optional field.   |
| <b>Connection Avaya production platform qualifier</b> | The value is a logical name for the target enterprise, that applies irrespective of primary or backup.<br>The primary and backup are a part of the same organization. Components use this name to address the Enterprise Server pair. This name must match the name that the Enterprise Servers have assigned to themselves locally or else the connection is rejected. |

| Name   | Description  |
|--|--|
| <b>Connection Avaya production primary URL</b> | The value is a primary URL of the platform   |
| <b>Connection Avaya production useProxy</b>    | The value specifies whether to use proxies for this platform or not. The values are true or false.   |
| <b>Connection set</b>                          | The set of connections that this SAL data transport will open. Each connection must have PlatformName, TargetFQDN, and PrimaryURL elements. Connections can optionally also have BackupURL elements.   |
| <b>Https session timeout</b>                   | The value specifies the maximum duration of HTTPS authentication sessions before they need to be re-negotiated.  |
| <b>Max message exchange size</b>               | <p>The value specifies maximum size of the messages data transport attempts to send or receive in one bundle. The following are the units of size:</p> <ul style="list-style-type: none"> <li>• B for bytes</li> <li>• M for megabytes</li> <li>• k for kilobytes</li> </ul> <p> <b>Note:</b><br/>Avaya recommends you not to change the default value unless there is need.</p> |
| <b>Max queue memory</b>                        | <p>The value specifies the maximum amount of memory on disk that the queue can occupy. The following are the units of memory:</p> <ul style="list-style-type: none"> <li>• B for bytes</li> <li>• M for megabytes</li> <li>• k for kilobytes</li> </ul> <p> <b>Note:</b><br/>Avaya recommends you not to change the default value unless there is need.</p>                     |
| <b>Max send transaction time</b>               | <p>The value specifies the maximum amount of time spent in a transaction when trying to send upstream.</p> <p> <b>Note:</b><br/>Avaya recommends you not to change the default value unless there is need.</p>  |
| <b>Organization FQDN</b>                       | The value specifies a fully qualified domain name that uniquely identifies the business organization that the SAL Platform resides in.   |

| Name                                | Description   |
|-------------------------------------|---|
| <b>Polling interval</b>             | <p>The time between polling for messages from each enterprise platform. Specify 0 to turn polling off.</p> <p>The following are the units:</p> <ul style="list-style-type: none"> <li>• h for Hours</li> <li>• m for Minutes</li> </ul> <p>The Agent polls because there is no way to connect directly from Avaya to the customer. Connections may only be initiated from the customer side. A component in the Enterprise can just send a message. The message is queued until either a message or a polling request is received from the destination Agent and the queued message is sent back to the Agent in the HTTPS reply.</p> |
| <b>Proxy address</b>                | The domain name or IP address of the proxy to use.  |
| <b>Proxy password</b>               | The password to use with the proxy. They are stored in a plain text.  |
| <b>Proxy port</b>                   | The port of the proxy server.   |
| <b>Proxy type</b>                   | The type of proxy based on whether the proxy supports HTTP or SOCKS.  |
| <b>Proxy use authentication</b>     | <p>The value specifies whether an authentication is required to access the proxy server.</p> <p>The values are true and false. If the value is true, an authentication is required to access the server.</p>  |
| <b>Proxy user</b>                   |   |
| <b>Server status reset interval</b> | <p>The time between the server marking an URL as unreachable and reattempting to connect to that URL.</p> <p>The following are the units of time:</p> <ul style="list-style-type: none"> <li>• h for hours</li> <li>• m for minutes</li> <li>• s for seconds</li> </ul>   |
| <b>SAL platform qualifier</b>       | A logical name for the target Enterprise, that applies irrespective of primary or backup. Implicitly, the primary and backup are a part of the same organization. Components use this name to address the Enterprise Server pair. This name must match the name that the Enterprise Servers have assigned to themselves locally or else the connection will be rejected.  |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Edit Profile: Data Transport Config page. Use this page to edit the parameters in the Data Transport Configuration profile. |
| <b>Done</b> | Closes the View Profile: Data Transport Config page.  |

**Related topics:**

[View software feature profiles](#) on page 1339

[View Profile: User Bulk Import Profile field descriptions](#) on page 1379

[View Profile: Agent Management field descriptions](#) on page 1381

[View Profile: Alarm Management field descriptions](#) on page 1383

[View Profile: Event processor field descriptions](#) on page 1384

[View Profile: Data Transport Static Config field descriptions](#) on page 1388

---

## View Profile: Data Transport Static Config field descriptions

Do not change any values in the fields displayed on this page. Any change is likely to break the SAL Agent application.

**Related topics:**

[View software feature profiles](#) on page 1339

[View Profile: User Bulk Import Profile field descriptions](#) on page 1379

[View Profile: Agent Management field descriptions](#) on page 1381

[View Profile: Alarm Management field descriptions](#) on page 1383

[View Profile: Event processor field descriptions](#) on page 1384

[View Profile : Data Transport Config field descriptions](#) on page 1385

# Chapter 14: Managing Users

---

## Managing users

---

### Manage users, public contacts and shared address

#### Manage users

User Profile Management is a shared management service that provides a central user administration. Centralized administration reduces the need for replicating a user's data across multiple products.

#### Manage public contacts

You can manage public contacts for the users in the enterprise.

#### Manage shared address

You can manage shared address for the users in the enterprise. These addresses are common address that can be shared by all the users in the enterprise.

---

## User Management

User Profile Management is a shared management service that provides a central user administration. Centralized administration reduces the need for replicating a user's data across multiple products. Following is the list of important operations that you can perform using the User Management shared service:

- Add a user profile
- View, modify and delete an existing user profile
- Assign and remove permission, roles, groups, address, contacts for users
- Bulk Import users and their attributes from a file
- Search for a user

A system administrator can only add, modify, and delete the user profiles.

---

## Users in Management Console

Access to the Management Console web interface requires a valid user name and password. Avaya recommends that you create a limited number of accounts and ensure that the passwords they use are secure.

Users with login privileges can add, modify, and delete accounts on the Management Console. To obtain a user account and password to the console, see your system administrator.

---

## Viewing details of a user

### Prerequisites

You must have permission to view the details of the selected user.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select a user.
  3. Click **View** to view the selected user account.  
You can view details of only one user account at a time.

---

### Related topics:

[User Profile View field descriptions](#) on page 1571

---

## Modifying user accounts

You must have permission to modify the user. The **Edit button** for modifying a user details is not available if you select a user for which you do not have the permission to modify the details.

### Prerequisites

Permission to modify the user

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select a user.

You can edit only one user account at one time.

3. To edit a user account, perform one of the following steps:
  - Click **Edit**.
  - Click **View > Edit**.
4. Modify the information and click **Commit** to save the changes to the database.

---

**Related topics:**

[User Profile Edit field descriptions](#) on page 1577

---

## Creating a new user profile

Use this functionality to create a new user profile.

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. On the User Management page, click **New**.
3. On the New User Profile page, enter the appropriate information click **Commit**.  
The field names that are marked with \* are mandatory fields. You must enter valid information in these fields for the successful creation of the user.

---

**Related topics:**

[Assigning roles to a user](#) on page 1394

[Assigning groups to a user](#) on page 1396

[Adding a mailing address of the user](#) on page 1400

[Creating a new communication profile](#) on page 1560

[New User Profile field descriptions](#) on page 1586

[Adding a contact in the Default Contact list](#) on page 1595

[Adding a private contact for a user](#) on page 1602

---

## Creating duplicate users

Using this feature you can create a new user account by copying the information from an existing user account. This feature does not copy the confidential information such as, addresses, private contacts, contact members in the contact list, password, and login name of the source user.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select the user account that you want to duplicate.
  3. Click **Duplicate**.
  4. On the User Profile Duplicate page, enter the appropriate information and click **Commit**.
- 

---

## Creating a user on communication management system

- 
1. Create a new user profile which is duplicate of profile 18.
  2. Give permissions to access the shell.
  3. Add any additional permissions
  4. Create a user with this profile.  
Use this user as login in RTS
- 

---

## Removing user accounts

When you remove a user, the system marks the user as deleted and stores them in a list of deleted users. Removing a user removes the roles associated with the user but retains the contacts, addresses, communication profiles of the user.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select a user from the table and click **Delete**.
  3. On the User Delete Confirmation page, click **Delete**.

 **Note:**

This operation marks the deleted users as deleted and stores them in the database in a list of deleted users.

---

---

## Filtering users

You can filter users by:

- Status of the user
- Name of the user
- E164 Handle
- Login Name of the user
- 

You may apply one or more filters to view users that match the filter criteria.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, click **Filter: Enable**.  
You can find the button at the upper-right corner of the table displaying users.
  3. Select the status of the user from the drop-down under the **Status** column.
  4. Enter the name of the user in the field under the **Name** column.  
To filter login names starting with a letter, enter the letter in the field. You can enter multiple letters to filter names that start with these entered letters.
  5. Enter the login name in the field under the **Login Name** column.  
To filter login names starting with a letter, enter the letter in the field. You can enter multiple letters to filter login names that start with these entered letters.
  6. Enter the E164 handle of the user in the field under the **E164 Handle** column.
  7. Click **Apply**.  
To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.  
To clear the filter criteria, click **Clear**.

---

### Result

The table displays only those users that match the filter criteria.

---

## Searching for users

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, click **Advanced Search** displayed at the upper-right corner of the page.
  3. In the Criteria section, do the following:
    - a. Select the search criterion from the first field.
    - b. Select the operator from the second field.
    - c. Enter the search value in the third field.

If you want to add another search condition, click **+** and repeat sub steps a through c listed in step 4.

If you want to delete a search condition, click **-**. This button is available if there are more than one search condition.

4. Click **Search**.

---

### Result

The page displays the users that match the value specified for the search criteria.

---

## Assigning roles to a user

To provide access to resources, you need to assign roles to the user accounts.

 **Note:**

You can also assign roles to the users using the Roles service provided by System Manager. To access the Roles service, click **Groups & Roles > Roles**.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Perform one of the following steps:
    - To assign roles to a new user, click **New**.

- To assign roles to an existing user, select the user and click **Edit** or **View > Edit**.
3. On the User Profile Edit or New User Profile page, click the **Roles** link displayed at the top of the page along with other links.
  4. Click **Assign Roles**.
  5. On the Assign Roles page, select the roles from the **Available Roles** section.
  6. Click **Select** to assign the roles to the selected user.
  7. Click **Commit** to assign roles to the selected users.
- 

---

## Assigning roles to multiple users

To provide access to resources, you need to assign roles to the user accounts.

 **Note:**

You can also assign roles to the users using the Roles service provided by System Manager. To access the Roles service, click **Groups & Roles > Roles**.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select the users and click **More Actions > Assign Roles**.
  3. On the Assign Roles page, select the roles from the **Available Roles** section.
  4. Click **Commit** to assign the roles to the selected users.
- 

---

## Removing roles from a user

You can use this feature to remove roles from a user. You must have permissions to modify the attributes of the user.

 **Note:**

You can also remove roles from the users using the Roles service provided by System Manager. To access the Roles service, click **Groups & Roles > Roles**.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Perform one of the following steps:
    - If you are creating a new user account and you have already assigned a role, then click **New > Roles**.
    - If you are removing a role in the edit mode, on the User Management page, select a user and click **Edit > Roles**.
    - If you are removing a role in the view mode, on the User Management page, select a user and click **View > Edit > Roles**.
  3. Select roles and click **Unassign Roles** to remove the assigned roles.
- 

---

## Assigning groups to a user

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Perform one of the following steps:
    - To assign groups to a new user, click **New**.
    - To assign groups to an existing user, select the user and click **Edit** or **View > Edit**.
  3. On the User Profile Edit page or New User Profile page, click the Group Membership link displayed at the top of the page along with other links.
  4. Click **Add To Group** in the Group Membership section.
  5. On the Assign Groups page, select the groups from the **Available Groups** section.
  6. Click **Select** to assign the groups to the user.
  7. Click **Commit**.
- 

### Related topics:

- [Creating a new user profile](#) on page 1391
- [Assigning roles to a user](#) on page 1394
- [Assigning roles to a user](#) on page 1394
- [Adding a mailing address of the user](#) on page 1400
- [Adding a mailing address of the user](#) on page 1400

[Creating a new communication profile](#) on page 1560

[Creating a new communication profile](#) on page 1560

[Adding a contact in the Default Contact list](#) on page 1595

[Adding a contact in the Default Contact list](#) on page 1595

[Adding a private contact for a user](#) on page 1602

[Adding a private contact for a user](#) on page 1602

---

## Assigning groups to multiple users

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select the users and click **More Actions > Add To Group**.
  3. On the Assign Groups page, select the groups from the **Available Groups** section.
  4. Click **Commit** to assign groups to the selected users.
- 

---

## Removing a user from groups

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Perform one of the following steps:
    - If you are creating a new user account and you have already assigned a group, then click **New > Group Membership**.
    - If you are removing a group in the edit mode, on the User Management page, select a user and click **Edit > Group Membership**.
    - If you are removing a group in the view mode, on the User Management page, select a user and click **View > Edit > Group Membership**.
  3. Select the groups and click **Remove From Group** to remove the user from the selected groups.
-

---

## Viewing deleted users

When you remove a user from the User Management page using the Delete functionality, the User Management page removes the user temporarily and stores this users as Deleted Users. You can use the Viewing deleted users functionality to view temporarily deleted users .

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the Users page, click **More Actions > Show Deleted Users**.
- 

---

## Restoring a deleted user

You can use this feature to restore the user that you deleted using the delete feature.

### Prerequisites

You must have permission to restore the selected deleted user.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, click **More Actions > Show Deleted Users**.
  3. Select the user that you want to restore and click **Restore**.
  4. On the User Restore Confirmation page, click **Restore**.
  5. On the User Profile Edit page, enter the password in the **Password** field.
  6. In the **Confirm Password** field, enter the same password that you entered in step 5.
  7. Click **Commit**.
- 

---

## Deleting the deleted users

When you use this feature to delete a user, it deletes the user permanently from the database.

## Prerequisites

You must have permission to delete the selected user.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, click **More Actions > Show Deleted Users**.
  3. Select the users that you want to delete and click **Delete**.
  4. On the User Delete Confirmation page, click **Delete**.



**Note:**

This operation permanently deletes the users from the database.

---

---

## Assigning users to roles

- 
1. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  2. On the Manage Roles page, select a user role and click **More Actions > Assign Roles to Users**.
  3. On the Assign Users page, select the users displayed in the **Select Users** section.
  4. Click **Commit**.
- 

---

## Removing users from roles

- 
1. Log in to the Avaya Aura™ System Manager web interface as an administrator.
  2. On the System Manager console, click **Groups & Roles > Roles** in the left navigation pane.
  3. On the Manage Roles page, select one or more user roles and click **More Actions > UnAssign User Roles**.

4. On the UnAssign Roles page, select the users displayed in the Select Users section.
  5. Click **Commit**.
- 

---

## Managing addresses

### Adding a mailing address of the user

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Perform one of the following steps:
    - On the Users page, click **New > Identity > Address > New**.
    - On the User Management page, select a user and click **Edit > Identity > Address > New**.
    - On the User Management page, select a user and click **View > Edit > Identity > Address > New**.
  3. Enter the appropriate information.
  4. Click **Commit**.
- 

#### Related topics:

[Add Address field descriptions](#) on page 1402

### Modifying a mailing address

You can use this feature to modify the mailing address of the user.



#### Note:

You can not modify a shared address using this feature.

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. Perform one of the following steps:

- Select a user and click **Edit > Identity > Address > Edit**.
  - Select a user and click **View > Edit > Identity > Address > Edit**.
3. On the **Edit Address** page, modify the information.
  4. Click **Commit**.

---

**Related topics:**

[Edit Address field descriptions](#) on page 1403

## Deleting a mailing address

You can use this feature to delete a private mailing address from the database. If the mailing address that you want to delete is a shared mailing address, the system removes the mailing address from the user's mailing address list and not from the database.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Perform one of the following steps:
    - If you are on the New User Profile page or on the User Profile Duplicate page and have added a mailing address , then navigate to **Identity > Address** .
    - On the User Management page, select a user and click **Edit > Identity > Address** .
    - On the Users page, select a user and click **View > Edit > Identity > Address** .
  3. Select the mailing address and click **Delete**.

---

## Choosing a shared address

Use this feature to choose a shared address for the user from a set of common addresses. You can use the Shared Addresses feature to add, modify and delete a shared address.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Perform one of the following steps:
    - On the User Management page, click **New**.

- If you are in the editing a user account, on the User Management page, select a user and click **Edit**.
  - If you are viewing information of an user, on the User Management page, select a user and click **View > Edit**.
3. On the New User Profile page or the User Profile Edit page, click **Identity > Address > Choose Shared Address**.
  4. On the Choose Address page, select one or more shared addresses.
  5. Click **Select**.
  6. Click **Commit**.

If you are choosing a shared address for a new user, ensure that you have entered valid information in all the mandatory fields on the New User Profile page before you click **Commit**. If you fail to enter valid information in a mandatory field, the system displays an error message.

**Related topics:**

[Choose Address field descriptions](#) on page 1403

## Add Address field descriptions

Use this page to add the mailing address of the user.

| Name                 | Description  |
|----------------------|--|
| <b>Name</b>          | The unique label that identifies the address.  |
| <b>Address Type:</b> | The type that identifies whether mailing address is a home or office address.  |
| <b>Building</b>      | The name of the building.  |
| <b>Room</b>          | The number or name of the room.  |
| <b>Street</b>        | The name of the street.  |
| <b>Locality Name</b> | The name of the city or town.  |
| <b>Postal Code</b>   | The postal code or zip code used by postal services to route mail to a destination. In the United States this is the Zip code. |
| <b>Province</b>      | The full name of the province.   |
| <b>Country</b>       | The name of the country.   |

| Button     | Description                           |
|------------|---------------------------------------|
| <b>Add</b> | Adds the mailing address of the user. |

| Button | Description                        |
|--------|------------------------------------|
| Cancel | Cancels the add address operation. |

**Related topics:**

[Adding a mailing address of the user](#) on page 1400

[Adding a postal address of a private contact](#) on page 1605

[Adding a shared address](#) on page 1671

[Modifying a shared address](#) on page 1671

**Edit Address field descriptions**

Use this page to add the mailing address of the user.

| Name                 | Description  |
|----------------------|--|
| <b>Name</b>          | The unique label that identifies the address.  |
| <b>Address Type:</b> | The type that identifies whether mailing address is a home or office address.  |
| <b>Building</b>      | The name of the building.  |
| <b>Room</b>          | The number or name of the room.  |
| <b>Street</b>        | The name of the street.  |
| <b>Locality Name</b> | The name of the city or town.  |
| <b>Postal Code</b>   | The postal code or zip code used by postal services to route mail to a destination. In the United States this is the Zip code. |
| <b>Province</b>      | The full name of the province.   |
| <b>Country</b>       | The name of the country.   |

| Button | Description                           |
|--------|---------------------------------------|
| Add    | Adds the mailing address of the user. |
| Cancel | Cancels the add address operation.    |

**Related topics:**

[Modifying a mailing address](#) on page 1400

[Modifying a postal address of a private contact](#) on page 1605

**Choose Address field descriptions**

Use this page to choose a shared address for the user.

| Name                 | Description   |
|----------------------|---|
| <b>Name</b>          | The unique label that identifies the address.   |
| <b>Address Type</b>  | The type of address. The values are: <ul style="list-style-type: none"> <li>• Office</li> <li>• Home</li> </ul> |
| <b>Street</b>        | The name of the street.   |
| <b>Locality Name</b> | The name of the city or town.   |
| <b>Postal Code</b>   | The postal code used by postal services to route mail to a destination. In United States this is Zip code.      |
| <b>Province</b>      | The full name of the province.  |
| <b>Country</b>       | The name of the country.  |

| Button        | Description   |
|---------------|---|
| <b>Select</b> | Adds the selected mailing address as the shared contact for the user account. |
| <b>Cancel</b> | Cancel the choose address operation.  |

**Related topics:**

[Choosing a shared address](#) on page 1401

[Choosing a shared address for a private contact](#) on page 1606

## Managing bulk importing and exporting

### Bulk importing and exporting

System Manager provides bulk importing and exporting of user profiles and global settings. You need to provide an XML file as input file for importing the data. While exporting, the data is exported to an XML file. The System Manager database stores the imported user profiles and global settings data.

The following are the user attributes that you can bulk import and export:

- Identity Data
- Communication Profile Set
- Handles
- Communication profiles (Station Data, Messaging Data, and Session Manager Data)

The following are the global settings attributes that you can bulk import and export:

- Public Contact Lists
- Shared Addresses
- System Presence access control list (ACLs)

### Key features of Bulk Import and Export

- Supports bulk import and export of 100000 user profiles in multiple files.



#### Note:

It is observed that the bulk import of 5000 users in a single input XML file of 600 MB achieves the performance rate of 60 records per minute.

- Maintains logs of records that failed to import and require manual intervention
- Supports scheduling of bulk import jobs from the System Manager console
- Provides various configuration options if a record to be imported matches an existing record in the database. You can configure to skip, replace, merge or delete of a matching record which already exists and re-import data.
- Supports downloading of failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and re-import them in to the database.

## Bulk importing users

Use this functionality to bulk import users with their attributes from an XML file. The bulk importing of the users functionality provides you the options to:

- abort or continue the import process when the import user operation encounters first error in the user input file.
- skip importing the users that already exist in the database. Use this option when you want to import new users and retain the existing users.
- replace the users in the database with the new users from the imported file.
- update and merge the user attributes data from the imported file to the existing data.
- delete the user records from the database that match the records in the input XML file.

See the “XML Schema Definition for bulk importing users” and “Sample XML for bulk importing users” sections in the “List of XML Schema Definitions and Sample XMLs for bulk Import” topic for details on the user imported attributes.

See the “XML Schema Definition for bulk deleting users” and “Sample XML for bulk deleting users” sections in the “List of XML Schema Definitions and Sample XMLs for bulk Import” topic for details on the user imported attributes.

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. Click **More Actions > Import Users**.
3. On the Import Users page, enter the complete path of the file in the **Select file** field. You can also use the **Browse** button to select a file.
4. Choose one of the error configuration options:
  - Abort on first error
  - Continue processing other records
5. Click **Complete**.
6. Choose one of the import options:
  - Click **Skip**.
  - Click **Replace**.
  - Click **Merge**.
  - Click **Delete**.
7. Click **Import**.

 **Note:**

Communication Manager Synchronization operation and Bulk Import of users should not overlap in time. If Bulk Import of users is in progress and Communication Manager Synchronization is started, the current records being processed will fail. After the synchronization is complete, the remaining bulk import records will be processed successfully. You have to re-import the records that have failed during synchronization.

---

### Related topics:

[Encrypting the passwords in the user import file using BulkImportEncryptionUtil running on Windows operating system](#) on page 1410

[Encrypting the passwords in the user import file using BulkImportEncryptionUtil running on Linux Operating System](#) on page 1411

[List of XML Schema Definitions and Sample XMLs for bulk Import](#) on page 1420

[List of XML Schema Definitions and Sample XMLs for bulk Import](#) on page 1420

[Attribute details defined in the Import user XSD](#) on page 1503

[Attribute details defined in the Delete User XSD](#) on page 1513

[Attribute details defined in the Endpoint profile XSD](#) on page 1514

[Attribute details defined in the Messaging communication profile XSD](#) on page 1541

[Attribute details defined in the Session Manager communication profile XSD](#) on page 1550

## Exporting users in bulk

With System Manager you can export users in bulk from the System Manager database. This utility is in the `$MGMT_HOME/upm/bulkexport` directory, where `MGMT_HOME` is an environment variable that represents the System Manager HOME path.

- 
1. Go to the command prompt.
  2. Change the directory to `$MGMT_HOME/upm/bulkexport/exportutility`. `MGMT_HOME` is an environment variable that represents the System Manager HOME path.
  3. Run the `# sh exportUpmUser.sh [-u] <user> [-p] <password> ... [OPTIONS]` command.

Here, `-u` (username) and `-p` (password) are the mandatory parameters. Optional parameters include:

- `-f` file name prefix of the file that you want to export
- `-r` number of records per file
- `-d` location of the file that you want to export
- `-s` start index of record
- `-e` number of records to be exported
- `-t` job scheduling time (YYYY:MM:DD:HH:MM:SS), if you do not specify this parameter, the present job runs immediately

You can modify the optional parameters by changing the `$MGMT_HOME/upm/bulkexport/exportutility/bulkexportconfig.properties` file, where `MGMT_HOME` is an environment variable that represents the System Manager HOME path.

For example, `# sh exportUpmUsers.sh -u <user> -p <password> -f userExport -r 1000 -s 0 -e 1000`

Refer the “XML Schema Definition for bulk importing users” section in the “List of XML Schema Definitions and Sample XMLs for bulk Import” topic for details on the attributes that are available for bulk exporting users.

While exporting users records if the number of exported records exceeds the limit of records that an XML file can hold, the system creates multiple XML files. These files are packaged together in a zip file.

- The system generates a zip file that contains the exported users records in an XML file.

- Password fields are not exported.

---

**Related topics:**

- [Making bulk export user data compatible for user partial import](#) on page 1409
- [List of XML Schema Definitions and Sample XMLs for bulk Import](#) on page 1420
- [List of XML Schema Definitions and Sample XMLs for bulk Import](#) on page 1420
- [Attribute details defined in the Import user XSD](#) on page 1503
- [Attribute details defined in the Delete User XSD](#) on page 1513
- [Attribute details defined in the Endpoint profile XSD](#) on page 1514
- [Attribute details defined in the Messaging communication profile XSD](#) on page 1541
- [Attribute details defined in the Session Manager communication profile XSD](#) on page 1550

## Bulk importing user attributes partially for a user

You can bulk import only the selected user attributes data for one or more users existing in the database. The bulk importing of the users functionality provides the options to:

1. abort or continue the import process when the User Management application encounters first error in the user input file.
2. replace the existing data in the user attributes with the new data from the imported file. For example, you can replace the existing contact list for a user with a new contact list
3. merge and update the data of the user attributes with the data from the imported file. For example, you can add a new contact in the list of contacts for the user and update the name of the user.

Refer to the “XML Schema Definition for partially importing users” and “Sample XML for partially importing users” sections in the “List of XML Schema Definitions and Sample XMLs for bulk Import” topic for details on the user imported attributes.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Click **More Actions > Import Users**.
  3. On the Import Users page, enter the file name in the **Select file** field.  
You can also use the **Browse** button to select a file.
  4. Choose one of the error configuration options:
    - Click **Abort on first error**.
    - Click **Continue processing other records**.
  5. Choose **Partial**.
  6. Choose one of the options if a matching record is found:

- Click **Replace**.
  - Click **Merge**.
7. Click **Import**.

---

### Related topics:

[List of XML Schema Definitions and Sample XMLs for bulk Import](#) on page 1420

[List of XML Schema Definitions and Sample XMLs for bulk Import](#) on page 1420

[Attribute details defined in the Import user XSD](#) on page 1503

[Attribute details defined in the Delete User XSD](#) on page 1513

[Attribute details defined in the Endpoint profile XSD](#) on page 1514

[Attribute details defined in the Messaging communication profile XSD](#) on page 1541

[Attribute details defined in the Session Manager communication profile XSD](#) on page 1550

## Making bulk export user data compatible for user partial import

Perform the following steps on the user export xml file to provision for partial import of users. You can generate the xml file when you bulk export users.

- 
1. After you export the users in bulk and generate the xml file, perform the following steps:

- a. Locate the following content in the generated XML file:

```
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:ns3="http://xml.avaya.com/schema/import1"
xmlns:ns4="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd">
```

- b. Modify `tns:users` to `tns:deltaUserList`.
- c. Remove `tns="http://xml.avaya.com/schema/import"`.
- d. Modify `ns4="http://xml.avaya.com/schema/deltaImport"` to `tns="http://xml.avaya.com/schema/deltaImport"`
- e. Modify `xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">` to `xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport userdeltaimport.xsd ">`

After you perform the substeps from b to e, the content referred in step a changes to:

```
<tns:deltaUserList xmlns:ns3="http://xml.avaya.com/schema/import1"
xmlns:tns="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
```

```
userdeltaimport.xsd ">
```

2. Replace All `<tns:user>` , `</tns:user>` , `<tns:users>` and `</tns:users >` with `<tns:userDelta>`, `</tns:userDelta>` , `<tns:deltaUserList>` and `</tns:deltaUserList>` respectively.

---

#### Related topics:

[Exporting users in bulk](#) on page 1407

## Encrypting the passwords in the user import file using BulkImportEncryptionUtil running on Windows operating system

A utility called BulkImportEncryptionUtil is a program that encrypts the “userPassword” and “commPassword” fields in the user import input file. This utility is a standalone java program and you can run this utility on any machine on which Java program is installed.

### Prerequisites

JDK 1.6 installed on your computer. If the computer does not have JDK 1.6 installed, use the <http://java.sun.com/javase/downloads/index.jsp> URL to download JDK 1.6.

1. Extract the contents of the `um_bulkimport-encryptUtil.zip` file from `$MGMT_HOME/upm/utilities` into a local folder.

The `um_bulkimport-encryptUtil.zip` file contains the following files:

- `um_bulkimport-encryptUtil.jar`
- `log4j.jar` and script files
- `um_bulkimport-encryptUtil.bat`
- `um_bulkimport-encryptUtil.sh`
- `Readme.txt`

2. Go to the command prompt and type `um_bulkimport-encryptUtil.bat <import|deltaimport> <xmlfilename> <basenamespaceprefix> <deltanamespaceprefix>`, where:

- `import | deltaimport` specifies whether the input xml file has data for complete import or partial import. For complete import this option value is "import" and for partial import this option value is "deltaimport".
- `xmlfilename` is the name of the XML file with complete path of the XML file that contains the data for importing the users data
- `basenamespaceprefix` is the namespace prefix in the input XML file. In the following example, `tns` is the value for the `basenamespaceprefix` parameter.

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd" >
```

- `deltanamespaceprefix` is the namespace prefix given in the partial import file. Specify this parameter if you are performing a partial import. In the following example, `deltanamespaceprefix` value is "delta" and `basenamespaceprefix` value is "tns".

```
<?xml version="1.0" encoding="UTF-8"?>
<delta:deltaUserList
xmlns:delta="http://xml.avaya.com/schema/deltaImport"
xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd ">
```

## Encrypting the passwords in the user import file using BulkImportEncryptionUtil running on Linux Operating System

A utility called BulkImportEncryptionUtil is a program that encrypts the "userPassword" and "commPassword" fields in the user import input file. This utility is a standalone java program and you can run this utility on any computer on which Java program is installed.

### Prerequisites

JDK 1.6 installed on your computer. If the computer does not have JDK 1.6 installed, use the <http://java.sun.com/javase/downloads/index.jsp> URL to download JDK 1.6.

1. Extract the contents of the `um_bulkimport-encryptUtil.zip` file from `$MGMT_HOME/upm/utilities` into a local folder.

The `um_bulkimport-encryptUtil.zip` file contains the following files:

- `um_bulkimport-encryptUtil.jar`
- `log4j.jar` and script files
- `um_bulkimport-encryptUtil.bat`
- `um_bulkimport-encryptUtil.sh`
- `Readme.txt`

2. Go to the command prompt and type `um_bulkimport-encryptUtil.sh <import|deltaimport> <xmlfilename> <basenamespaceprefix> <deltanamespaceprefix>`, where:

- `import | deltaimport` specifies whether the input xml file has data for complete import or partial import. For complete import this option value is "import" and for partial import this option value is "deltaimport".

- **xmlfilename** is the name of the XML file with complete path of the XML file that contains the data for importing the users data
- **basenamespaceprefix** is the namespace prefix in the input XML file. In the following example, **tns** is the value for the **basenamespaceprefix** parameter.

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd" >
```

- **deltanamespaceprefix** is the namespace prefix given in the partial import file. Specify this parameter if you are performing a partial import. In the following example, **deltanamespaceprefix** value is "delta" and **basenamespaceprefix** value is "tns".

```
<?xml version="1.0" encoding="UTF-8"?>
<delta:deltaUserList
xmlns:delta="http://xml.avaya.com/schema/deltaImport"
xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd ">
```

---

## Scheduling a user importing job

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. Click **More Actions > Import Users**.
3. On the Import Users page, in the **Select file** field enter the name of the file along with the path.  
You can also use the **Browse** button to select a file.
4. Choose one of the following error configuration options:
  - **Abort on first error**
  - **Continue processing other records**
5. Choose one of the options if a matching record is found:
  - **Skip**
  - **Merge**
  - **Replace**
  - **Delete**
6. In the Job Schedule section:

- a. Click **Schedule Later**.  
If you want to run the user importing job immediately, click **Run immediately**.  
Selecting this option makes the scheduling related fields unavailable.
  - b. Enter the date in the **Date** field.  
You can use the calendar icon to select a date.
  - c. In the **Time** field, enter time in hours, minutes and second format.
  - d. From the **Time Zone** field, select the time zone.
7. Click **Import**.

---

## Result

The page displays the scheduled job in the Manage Jobs section.

## Aborting a user importing job on first error

An importing process may encounter errors at the time of importing users. Use this feature to abort the importing process on encountering the first error during importing users from the input file.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Click **More Actions > Import Users**.
  3. On the Import Users page, enter the file name in the **Select file** field.  
You can also use the **Browse** button to select a file.
  4. Click **Abort on First Error** to choose error configuration options.
  5. Choose or enter the appropriate information for remaining fields.
  6. Click **Import**.
- 

## Canceling a user importing job

### Prerequisites

You can only cancel a job which is in PENDING EXECUTION or in RUNNING state.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Click **More Actions > Import Users**.
  3. On the Import Users page, select a job from the table in the Job List section.
  4. Click **Cancel Job**.
- 

## Deleting an importing job

### Prerequisites

You can only delete the jobs that are successful.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Click **More Actions > Import Users**.
  3. On the Import Users page, select a job from the table in the Job List section.
  4. Click **Delete Job**.
- 

## Viewing a user importing job in Scheduler

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Click **More Actions > Import Users**.
  3. On the Import Users page, select a job from the table in the Manage Jobs section.
  4. Click the link displayed in the **Scheduled Job** column.
- 

### Result

The Scheduler page displays the details of the Job. You can perform operations on the job that the Scheduler supports for the job.

## Viewing details of an user importing job

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Click **More Actions > Import Users**.
  3. On the Import Users page, select one job from the table in the Manage Jobs section.
  4. Click **View Job**.

---

### Result

The Job Detail page displays the details of the selected job.

## Bulk importing global user settings records

You can bulk import the global user settings from an XML file. The bulk importing of the global user settings feature provides you the options to:

- abort or continue the import process when the import operation encounters first error in the global user settings input file.
- skip importing the global user settings records that already exist in the database. Use this option when you want to import new global user settings records and retain the existing users.
- replace all the global user settings records in the database with the global user settings records from the imported file.
- update and merge the global user settings attributes data from the imported file to the existing data in the attributes.
- delete the global setting records from the database that matches the records in the input XML file.

See the “XML Schema Definition for bulk importing the global user settings” and “Sample XML for bulk importing global setting records” sections in the “List of XML Schema Definitions and Sample XMLs for bulk Import” topic for details on the global user settings imported attributes.

See the “XML Schema Definition for bulk deleting the global user settings” and “Sample XML for bulk deleting global setting records” sections in the “List of XML Schema Definitions and Sample XMLs for bulk Import” topic for details on the global user settings imported attributes.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Click **More Actions > Import Global Settings**.

3. On the Import Global Settings page, enter the complete path of the file in the **Select file** field.  
You can also use the **Browse** button to select a file.
4. Choose one of the error configuration options:
  - **Abort on first error**
  - **Continue processing other records**
5. Choose one of the import options:
  - **Skip**
  - **Replace**
  - **Merge**
  - **Delete**
6. Click **Import**.

---

**Related topics:**

[List of XML Schema Definitions and Sample XMLs for bulk Import](#) on page 1420

## Exporting global settings in bulk

You can export Global Settings in bulk from the System Manager database. You can find this utility in the `$MGMT_HOME/upm/bulkexport` directory. `MGMT_HOME` is an environment variable that represents the System Manager HOME path.

- 
1. Go to the shell prompt.
  2. Change the directory to `$MGMT_HOME/upm/bulkexport/exportutility`.  
`MGMT_HOME` is an environment variable that represents the System Manager HOME path.
  3. Run the `# sh exportUpmGlobalsettings.sh [-u] <user> [-p]< password> ... [OPTIONS] command`.  
Here, `-u` (username) and `-p` (password) are the mandatory parameters. Optional parameters include:  
Optional parameters include:
    - `-f` file name prefix of the file that you want to export
    - `-r` number of records per file
    - `-d` location of the file that you want to export
    - `-s` start index of record

- -e number of records that you want to export
- -t job scheduling time (YYYY:MM:DD:HH:MM:SS); if you do not specify this parameter, the job runs immediately
- -o global settings export filter, the default value is 0. The following is a list of values for the global settings export filter option:
  - 0: No Filter; 0 will be considered as start index value
  - 1: System Default Type filter
  - 2: Enforced users filter
  - 3: System Rule Type filter
  - 4: System ACL Entry Type filter
  - 5: Shared Address filter
  - 6: Public Contact filter

The optional arguments default values can be modified by changing the `$MGMT_HOME/upm/bulkexport/exportutility/bulkexportconfig.properties` file, where `MGMT_HOME` is an environment variable that represents the System Manager HOME path.

For example, # `sh exportUpmGlobalsettings.sh -u <user> -p <password> -f globalSettingExport -r 1000 -s 0 -e 1000 -o 1.`

Refer the “XML Schema Definition for bulk importing global setting records” section in the “List of XML Schema Definitions and Sample XMLs for bulk Import” topic for details on the attributes that are available for bulk exporting global settings.

While exporting global settings records if the number of exported records exceeds the limit of records that an XML file can hold, the system creates multiple XML files. These files are packaged together in a zip file.

The system generates a zip file that contains the exported global settings records in an XML file.

---

#### Related topics:

[List of XML Schema Definitions and Sample XMLs for bulk Import](#) on page 1420

## Scheduling a global user settings importing job

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. Click **More Actions > Import Global Settings**.

3. On the Import Global Settings page, in the **Select file** field, enter the name of the file along with the path.  
You can also use the **Browse** button to select a file.
4. Choose one of the following error configuration options:
  - **Abort on first error**
  - **Continue processing other records**
5. Choose one of the options if a matching record is found:
  - Click **Skip**.
  - Click **Merge**.
  - Click **Replace**.
  - Click **Delete**.
6. In the Job Schedule section:
  - a. Click **Schedule Later**.  
If you want to run the importing job immediately, click **Run immediately**.  
Selecting this option makes the scheduling related fields unavailable.
  - b. Enter the date in the **Date** field.  
You can use the calendar icon to select a date.
  - c. In the **Time** field, enter time in hours, minutes and second format.
  - d. From the **Time Zone** field, select the time zone.
7. Click **Import**.

---

## Result

The page displays the scheduled job in the Manage Jobs section.

## Viewing details of a global user settings importing job

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Click **More Actions > Import Global Settings**.
  3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
  4. Click **View Job**.
-

## Result

The Job Detail page displays the details of the selected job.

## Viewing a global user settings importing job in Scheduler

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. Click **More Actions > Import Global Settings**.
3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
4. Click the link displayed in the **Scheduled Job** column.

## Result

The Scheduler page displays the details of the Job. You can perform operations on the job that Scheduler supports for the job.

## Aborting a global user settings import job on first error

This functionality provides you an option to abort the import process when the import process encounters the first error in the input file while processing the global user settings records.

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. Click **More Actions > Import Global Settings**.
3. On the Import Global Settings page, enter the file name in the **Select file** field. You can also use the **Browse** button to select a file.
4. Click **Abort on First Error** to choose error configuration options.
5. Choose or enter the appropriate information for remaining fields.
6. Click **Import**.

## Deleting a global user settings importing job

### Prerequisites

You can only delete jobs that are successful.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Click **More Actions > Import Global Settings**.
  3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
  4. Click **Delete Job**.
- 

## Canceling a global user settings importing job

### Prerequisites

You can only cancel a job which is in PENDING EXECUTION or in RUNNING state.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Click **More Actions > Import Global Settings**.
  3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
  4. Click **Cancel Job**.
- 

## List of XML Schema Definitions and Sample XMLs for bulk Import

Following is the list of XML Schema Definition and XML code snippets for bulk importing users, global setting records, roles, elements, endpoint profiles, messaging profiles and Session Manager profiles:

[XML Schema Definition for bulk importing users](#) on page 1421

[Sample XML for bulk importing users with minimal attributes](#) on page 1432

[Sample XML for bulk importing users with all attributes](#) on page 1432

[XML Schema Definition for partially importing users](#) on page 1440

[Sample XML for partially importing users](#) on page 1441

[Sample XML for partially importing users](#) on page 1441

[Sample XML for bulk deleting users](#) on page 1444

[XML Schema Definition for bulk importing elements](#) on page 1445

[Sample XML for bulk importing elements](#) on page 1450

[XML Schema Definition for bulk importing Session Manager profiles](#) on page 1451

[Sample XML for bulk importing Session Manager profiles](#) on page 1451

[XML Schema Definition for bulk importing endpoint profiles](#) on page 1453

[Sample XML for bulk importing endpoint profiles](#) on page 1477

[XML Schema Definition for bulk importing messaging profiles](#) on page 1479

[Sample XML for bulk importing messaging profiles](#) on page 1486

[XML Schema Definition for bulk importing global setting records](#) on page 1487

[Sample XML for bulk importing global setting records](#) on page 1493

[XML Schema Definition for bulk deleting global setting records](#) on page 1497

[Sample XML for bulk deleting global setting records](#) on page 1498

[XML Schema Definition for bulk importing roles](#) on page 1498

[Sample XML for bulk importing roles](#) on page 1502

## XML Schema Definition for bulk importing users

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ext="http://
xml.avaya.com/schema/import" xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://xml.avaya.com/schema/import" version="1.0">
  <xs:annotation>
    <xs:documentation xml:lang="en">This Schema defines schema for bulk import
and export of Users. Root Element 'Users' represent collection of user (containing
1 or more users)</xs:documentation>
  </xs:annotation>
  <xs:element name="secureStore" type="tns:xmlSecureStore"/>
  <xs:element name="user" type="tns:xmlUser"/>
  <xs:element name="users">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="secureStore" type="tns:xmlSecureStore"
minOccurs="0"/>
        <xs:element name="user" type="tns:xmlUser" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="xmlUser">
    <xs:annotation>
      <xs:documentation xml:lang="en">
        ---authenticationType: This defines the type of authentication that
```

this user will undergo at runtime to obtain access to the system. Possible Values: BASIC, ENTERPRISE

- description: A text description of the user. Human readable description of this user instance.
- displayName: The localized name of a user to be used when displaying. It will typically be the localized full name. This value may be provisioned from the user's enterprise directory entry. If it does not exist, synchronization rules can be used to populate it for other fields e.g. Surname, GivenName, or LoginName.
- displayNameAscii: The full text name of the user represented in ASCII. It is used to support display (e.g. endpoints) that cannot handle localized text.
- dn: The distinguished name of the user. The DN is a sequence of relative distinguished names (RDN) connected by commas. An RDN is an attribute with an associated value in the form of attribute=value, normally expressed in a UTF-8 string format. The dn can be used to identify the user and may be used for authentication subject mapping. Note the dn is changeable.
- isDuplicatedLoginAllowed: A boolean indicator showing whether this user is allowed a duplicate concurrent logins. A true stipulates that the user is allowed to have duplicate logins. Default value is true.
- isEnabled: A boolean indicator showing whether or not the user is active. Users with AuthenticationType=Basic will fail if this value is false. This attribute can be used to disable access between login attempts. A running session's login will not be revocable. Alternatively the administrator can always modify the password to disable the user from logging in. A true stipulates this is an active user, a false used for a disabled user. Default value is false.
- isVirtualUser: A boolean indicator showing whether or not the record is being used for a non-human entity such as an application, service, software agent, etc. This is to be used where the entity will behave as a user and needs to have subset of the user profile populated. If the entity does not behave as a user and has a different trust relationship e.g. a trust certificate it should not be treated as a virtual user. A virtual user can represent an Avaya or external non-human entity. This attribute is provided as a convenience to track such accounts. A true stipulates this is a virtual users, a false is used for human users. Default value is false.
- givenName: The first name of the user.
- honorific: The personal title used to address a user. This is typically a social title and not the work title which is contained in the title attribute. This attribute can map to "PersonalTitle".
- loginName: This is the unique system login name given to the user. It can take the form of username@domain or just username. This may vary across customers. It can be used to help provision default user handles in the CSHandle table. The username is an alphanumeric value that must comply with the userinfo related portion of a URI as described in rfc2396. However, it is further restricted as ASCII characters with only the "\_" and "." special characters supported. This is the rfc2798 "uid" attribute.
- middleName: The middle name of the user
- managerName: Text name of the user's manager. This is a free formed field and does not require the user's manager to also be a user of the solution. This attribute was requested to support reporting needs.
- preferredGivenName: The preferred first name of the user.
- preferredLanguage: The individual's preferred written or spoken language. Values will conform to rfc4646 and the reader should refer to rfc4646 for syntax. This format uses the ISO standard Language (ISO-639) and region (ISO-3166) codes. In the absence of a value the client's locale should be used, if no value is set, en-US should be defaulted.
- source: Free format text field that identifies the entity that created this user record. The format of this field will be either a IP Address/Port or a name representing an enterprise LDAP or Avaya.
- sourceUserKey: The key of the user from the source system. If the source is an Enterprise Active Directory server, this value will be the objectGUID.
- status: This information is to help manage provisioning activities such as correcting or completing the provisioning of a user instance. It can also signify that approval is needed (PENDINGAUTHZ) before a user account is sufficiently configured to be a valid user (PROVISIONED). Possible Values:

```

AUTHPENDING;PENDINGAUTHZ;PROVISIONED
    ---suffix:The text appended to a name e.g. Jr., III.
    ---surname:The user's last name, also called the family name.
    ---timeZone:The preferred time zone of the user. For example:
"(-07:00) Mountain Time (US & Canada); Chihuahua, La Paz", "(+00:00) GMT : Dublin,
Edinburgh, Lisbon, London, Casablanca".
    ---title:The job function of a person in their organizational context.
    ---userName:This is the username portion of the loginName field.
It is an alphanumeric value that must comply with the userinfo related portion of a
URI as described in rfc2396. However, it is further restricted as ASCII characters
with only the "_" and "." special characters supported. This is the rfc2798 "uid"
attribute.
    ---userPassword:The encrypted password for this user's account.A
null password is used when the user is authenticated by the enterprise such as
with a separate source such as the enterprise LDAP.
    ---commPassword:The encrypted "subscriber" or communication password
with which the user logs can use to authentication with on to any CommProfile SIP
and non SIP. This attribute is meant to be a shared across different communication
profiles and thus different communication services.
    ---userType:This enumerates the possible primary user application
types. A User can be associated with multiple user types. Possible values are
ADMINISTRATOR;COMMUNICATION USER;AGENT;SUPERVISOR;RESIDENT EXPERT;SERVICE
TECHNICIAN;LOBBY PHONE
    ---roles:Text name of a role.This value needs to pre-exist in SMGR DB
    ---address:The address of the user.
    ---securityIdentity:The SecurityIdentity is used to hold any
additional identities for a user that can be used for authentication such as their
loginName, Kerberos account name, or their X509 certificate name.
    ---ownedContactLists:It is a collection of internal or external
contacts. ContactList is owned by a specific user and has a name that a unique name
within the context of its owner.
    ---ownedContacts:It represents a non Avaya application user (external)
contact. Contacts can be collected together along with User entities into a contact
list. Contacts can be created by an administrator or an end user.
    ---presenceUserDefault:These are personal rules that are set by
presentities to define how much presence information can be shown to watchers that
are not explicitly mentioned in an ACL. There may be one User Default rule per
presentity (User), or none.
    ---presenceUserACL:These are personal rules defined by presentities
themselves on who can monitor their presence information. There may be several
entries in the list for a given presentity, each entry corresponding to one watcher.
    ---presenceUserCLDefault:This is a personal rule that is set by
presentities to define how much presence information can be shown to watchers that
belong to the user's contact list. There may be one User Contact List Default rule
per presentity (Person) or none.
    ---commProfileSet:A user will have a default commprofile set.A
commprofile set can exist without any handles or commprofiles referencing it. I.e.
you can create a commprofile set without needing to also create either a handle or
a commprofile.A commprofile set can contain multiple commprofiles, but only one of
each specific type. This is enforced by having the CommProfile uniqueness constraint
include type, commprofile_set_id.
    </xs:documentation>
</xs:annotation>
<xs:sequence>
  <xs:element name="authenticationType" type="xs:string"/>
  <xs:element name="description" type="xs:string" minOccurs="0"/>
  <xs:element name="displayName" type="xs:string" minOccurs="0"/>
  <xs:element name="displayNameAscii" type="xs:string" minOccurs="0"/>
  <xs:element name="dn" type="xs:string" minOccurs="0"/>
  <xs:element name="isDuplicatedLoginAllowed" type="xs:boolean"
minOccurs="0"/>
  <xs:element name="isEnabled" type="xs:boolean" minOccurs="0"/>
  <xs:element name="isVirtualUser" type="xs:boolean" minOccurs="0"/>
  <xs:element name="givenName" type="xs:string"/>
  <xs:element name="honorific" type="xs:string" minOccurs="0"/>

```

```

<xs:element name="loginName">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:maxLength value="128"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<xs:element name="middleName" type="xs:string" minOccurs="0"/>
<xs:element name="managerName" type="xs:string" minOccurs="0"/>
<xs:element name="preferredGivenName" type="xs:string" minOccurs="0"/>
<xs:element name="preferredLanguage" type="xs:string" minOccurs="0"/>
<xs:element name="source" type="xs:string" minOccurs="0"
  maxOccurs="1"/>
<xs:element name="sourceUserKey" type="xs:string" minOccurs="0"
  maxOccurs="1"/>
<xs:element name="status" type="xs:string" minOccurs="0"/>
<xs:element name="suffix" type="xs:string" minOccurs="0"/>
<xs:element name="surname" type="xs:string"/>
<xs:element name="timeZone" type="xs:string" minOccurs="0"/>
<xs:element name="title" type="xs:string" minOccurs="0"/>
<xs:element name="userName" type="xs:string" minOccurs="0"
  maxOccurs="1"/>
<xs:element name="userPassword" type="xs:string" minOccurs="0"/>
<xs:element name="commPassword" type="xs:string" minOccurs="0"/>
<xs:element name="userType" type="xs:string" minOccurs="0"
maxOccurs="unbounded"/>
  <xs:element name="roles" minOccurs="0">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="role" type="xs:string" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="address" type="tns:xmlAddress" minOccurs="0"
maxOccurs="unbounded"/>
  <xs:element name="securityIdentity" type="tns:xmlSecurityIdentity"
minOccurs="0" maxOccurs="unbounded"/>
  <!-- Contact list Entries -->
  <xs:element name="ownedContactLists" minOccurs="0">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="contactList" type="tns:xmlContactList"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="ownedContacts" minOccurs="0">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="contact" type="tns:xmlContact"
maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <!-- Presence ACL User Entries -->
  <xs:element name="presenceUserDefault" type="tns:xmlPresUserDefaultType"
minOccurs="0"/>
  <xs:element name="presenceUserACL" type="tns:xmlPresUserACLEntryType"
minOccurs="0" maxOccurs="unbounded"/>
  <xs:element name="presenceUserCLDefault"
type="tns:xmlPresUserCLDefaultType" minOccurs="0"/>
  <xs:element name="commProfileSet" type="tns:xmlCommProfileSetType"
minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

```

```

<xs:complexType name="xmlSecurityIdentity">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      ---SecurityIdentity:Represents the possible external identities
that a user may have for the purpose of authentication. The type and format of an
identity depends on the external Identity Provider and can include X.509
certificates or Kerberos user accounts
      ---identity:The unique external identity of the user. This is a free
text field and no format is enforced. The format will depend on the identity type.
Kerberos user account can take the form of: username@domainName
e.g. jsmith@acme.org
      ---realm:The name of the security domain that this identity is valid
in.
      ---type:The text representation of the type of identity. Possible
values are: "principalname", "X509" and "Kerberos"
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="identity" type="xs:string"/>
    <xs:element name="realm" type="xs:string" minOccurs="0"/>
    <xs:element name="type" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlPresInfoTypeAccessType">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      ---PresInfoTypeAccess: For the purpose of access control, presence
information is partitioned into several areas called Presence Info Types. Examples
of Presence Info Types would be "Telephony Presence", "Instant Messaging Presence",
"Calendar Presence", or "Full Presence".
      ---infoType:This defines the different classes of presence information.
      ---access:Presence access type possible values: ALLOW, BLOCK,
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="infoType" type="tns:xmlPresInfoTypeType"/>
    <xs:element name="access" type="xs:string" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlPresACRuleType">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      ---ACRuleType:This contains rules that are similar to a User ACL
in the sense that its entries define access between individual presentities and
watchers. However this rule is managed by the administrator as opposed to
presentities themselves. Entries of Enforced User ACL can also be defined with
different priorities. Entries with higher priority will have more weight than
entries with lower priority.
      ---infotypeaccess:This is a link between acl entries, presence info
types, and access actions.
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="infoTypeAccess" type="tns:xmlPresInfoTypeAccessType"
minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlPresUserDefaultType">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      ---PresUserDefault:These are personal rules that are set by
presentities to define how much presence information can be shown to watchers that
are not explicitly mentioned in an ACL. There may be one User Default rule per
presentity (User), or none.
    </xs:documentation>
  </xs:annotation>

```

```

        </xs:annotation>
        <xs:complexContent>
          <xs:extension base="tns:xmlPresACRuleType"/>
        </xs:complexContent>
      </xs:complexType>
      <xs:complexType name="xmlPresUserCLDefaultType">
        <xs:annotation>
          <xs:documentation xml:lang="en">
            ---PresUserCLDefault:This is a personal rule that is set by
            presentities to define how much presence information can be shown to watchers that
            belong to the user's contact list. There may be one User Contact List Default rule
            per presentity (Person) or none.
          </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
          <xs:extension base="tns:xmlPresACRuleType"/>
        </xs:complexContent>
      </xs:complexType>
      <xs:complexType name="xmlPresUserACLEntryType">
        <xs:annotation>
          <xs:documentation xml:lang="en">
            ---UserACLEntry:These are personal rules defined by presentities
            themselves on who can monitor their presence information. There may be several
            entries in the list for a given presentity, each entry corresponding to one watcher.
            ---watcherLoginName: LoginName,if the watcher is a user.
            ---watcherDisplayName:DisplayName,if the watcher is a contact.
          </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
          <xs:extension base="tns:xmlPresACRuleType">
            <xs:sequence>
              <xs:choice>
                <xs:element name="watcherLoginName" type="xs:string"
minOccurs="0"/>
                <xs:element name="watcherDisplayName" type="xs:string"
minOccurs="0"/>
              </xs:choice>
            </xs:sequence>
          </xs:extension>
        </xs:complexContent>
      </xs:complexType>
      <xs:complexType name="xmlPresInfoTypeType">
        <xs:annotation>
          <xs:documentation xml:lang="en">
            ---PresInfoType:Entries that define the difference classes of presence
            information.
            ---label:A unique string that names this info type (e.g. "Telephony
            Presence").
            ---filter:Internal definition of which part of presence information is
            covered by this info type. The value of this field should be treated as opaque
            string; it is maintained and used only by Presence services.
            ---specFlags:This field is empty for regular info types, but for
            special info types it contains a comma-separated list of keywords that identify
            these types. In this version only "FULL" that represents full presence information
            is supported.
          </xs:documentation>
        </xs:annotation>
        <xs:sequence>
          <xs:element name="label" type="xs:string"/>
          <xs:element name="filter" type="xs:string"/>
          <xs:element name="specFlags" type="xs:string" minOccurs="0"/>
        </xs:sequence>
      </xs:complexType>
      <!-- Contact List entries -->
      <xs:complexType name="xmlContactList">

```

```

    <xs:annotation>
      <xs:documentation xml:lang="en">
        ---ContactList:The ContactList is a collection of personal or public
        groups containing external contacts and/or Avaya users.
        ---name:The text name of the list. This in the context of the
        owner must be unique.
        ---description:A free text description of this member.
        ---isPublic:Defines if the contact is public or personal. Default =
        false.
        ---members:Represents the list of users or contacts that belong to
        contact list
        ---contactListType:Specifies the type categorizing this list.
      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element name="name" type="xs:string"/>
      <xs:element name="description" type="xs:string" minOccurs="0"/>
      <xs:element name="isPublic" type="xs:boolean"/>
      <xs:element name="members" type="tns:xmlContactListMember" minOccurs="0"
      maxOccurs="unbounded"/>
      <xs:element name="contactListType" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="xmlContactListMember">
    <xs:annotation>
      <xs:documentation xml:lang="en">
        ---ContactListMember:It supports many to many relationship between
        user, Contact and ContactList.
        ---memberContact:This represents the name of the Contact.A
        ContactListMember can either be a Contact or User
        ---speedDialContactAddress:A Contact Address added as a favorite entry
        ContactListMember can either be a Contact or User
        ---memberUser:This represents the loginname of the User.A
        ContactListMember can either be a Contact or User
        ---speedDialHandle:A handle added as a favorite entry
        ---isFavorite:A boolean indicator that reflects whether this
        contact is a favorite entry. If true, the value of entryindex would show which
        position to place this entry in any display.
        ---isSpeedDial:Each contact list member can also be flagged as a
        favorite (a.k.a. speed dial)
        ---speedDialEntry:For either a presence buddy or favorite entry, a
        specific communication address to use can be pointed to.
        ---isPresenceBuddy:Each contact list member can also be flagged as
        a presence buddy
        ---label:A free text short word or phrase for classifying this contact
        list member.
        ---altLabel:A free text short word or phrase for classifying this
        contact. This is similar to label, but it is used to store alternate language
        representations.
        ---description:A free text description of this
        member.
      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:choice>
        <xs:sequence>
          <xs:element name="memberContact" type="xs:string" minOccurs="0"/>
          <xs:element name="speedDialContactAddress"
          type="tns:xmlContactAddress" minOccurs="0"/>
        </xs:sequence>
        <xs:sequence>
          <xs:element name="memberUser" type="xs:string" minOccurs="0"/>
          <xs:element name="speedDialHandle" type="tns:xmlHandle"
          minOccurs="0"/>
        </xs:sequence>
      </xs:choice>
    </xs:sequence>
  </xs:complexType>

```

```

        <xs:element name="isFavorite" type="xs:boolean"/>
        <xs:element name="isSpeedDial" type="xs:boolean"/>
        <xs:element name="speedDialEntry" type="xs:int" minOccurs="0"/>
        <xs:element name="isPresenceBuddy" type="xs:boolean"/>
        <xs:element name="label" type="xs:string" minOccurs="0"/>
        <xs:element name="altLabel" type="xs:string" minOccurs="0"/>
        <xs:element name="description" type="xs:string" minOccurs="0"/>
        <xs:element name="priorityLevel" type="xs:int" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlContactAddress">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            ---address:A fully qualified URI for interacting with this
            contact. Any addresses added to this table should contain a qualifier e.g. sip,
            sips, tel, mailto. The address should be syntactically valid based on the qualifier.
            It must be possible to add via the GUI and Interface. The application must do
            validation.
            ---altLabel:A free text description for classifying this contact.
            This is similar to ContactLabel, but it is used to store alternate language
            representations.
            ---contactCategory:It represents the category of this entry e.g.
            Home, Office, Mobile.
            ---contactType:It represents the type of contact this entry e.g.
            phone, SIP, IM, Email.
            ---label:A free text description for classifying this contact.
        </xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="address" type="xs:string"/>
        <xs:element name="altLabel" type="xs:string" minOccurs="0"/>
        <xs:element name="contactCategory" type="xs:string"/>
        <xs:element name="contactType" type="xs:string"/>
        <xs:element name="label" type="xs:string" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlAddress">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            ---addressType:Specifies the role of the address. Examples: Home,
            business.
            ---name:The Name property defines the unique label by which the
            address is known. Default format for user specific address should include user name
            place address type.
            ---building:The name or other designation of a structure
            ---localityName:The name of a locality, such as a city, county or
            other geographic region.
            ---postalCode:A code used by postal services to route mail to a
            destination. In the United States this is the zip code.
            ---room:Name or designation of a room.
            ---stateOrProvince:The full name of a state or province.
            ---country:A country.
            ---street:The physical address of the object such as an address for
            package delivery
            ---postalAddress:A free formed text area for the complete physical
            delivery address. It may be used in place of the specific fields in this table.
            ---isPrivate:A boolean indicator to specify if this address
            could be shared across multiple users.True is private, false is sharable. Default
            is false.
        </xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="addressType" type="xs:string"/>
        <xs:element name="name" type="xs:string"/>
        <xs:element name="building" type="xs:string" minOccurs="0"/>

```

```

<xs:element name="localityName" type="xs:string" minOccurs="0"/>
<xs:element name="postalCode" type="xs:string" minOccurs="0"/>
<xs:element name="room" type="xs:string" minOccurs="0"/>
<xs:element name="stateOrProvince" type="xs:string" minOccurs="0"/>
<xs:element name="country" type="xs:string" minOccurs="0"/>
<xs:element name="street" type="xs:string" minOccurs="0"/>
<xs:element name="postalAddress" minOccurs="0">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:maxLength value="1024"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<xs:element name="isPrivate" type="xs:boolean" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="xmlContact">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      ---Contact:An entity that represents a non Avaya application user
      (external) contact. Contacts can be collected together along with User entities into
      a contact list. Contacts can be created by an administrator or an end user. Contacts
      have name attributes, and owner, and can be public or personal.A contact also
      includes one or more contact addresses that can be used for establishing an
      interaction with the contact. Contacts can be designated as being a user's presence
      buddy or added as a favorite entry (i.e. speed dial).
      ---company:The organization that the contact belongs to.
      ---description:A free text field containing human readable text
      providing information on this entry.
      ---displayName:The localized name of a contact to be used when
      displaying. It will typically be the localized full name. This value may be
      provisioned from the user's enterprise directory entry. If it does not exist,
      synchronization rules can be used to populate it for other fields e.g. Surname,
      GivenName, or LoginName.
      ---displayNameAscii:The full text name of the contact represented
      in ASCII. It is used to support display (e.g. endpoints) that cannot handle
      localized text.
      ---dn:The distinguished name of the user. The DN is a sequence of
      relative distinguished names (RDN) connected by commas. An RDN is an attribute with
      an associated value in the form of attribute=value, normally expressed in a UTF-8
      string format.The dn can be used to uniquely identify this record. Note the dn is
      changeable.
      ---givenName:The first name of the contact.
      ---initials:Initials of the contact
      ---middleName:The middle name of the contact.
      ---preferredGivenName:The nick name of the contact.
      ---preferredLanguage:The individual's preferred written or spoken
      language. Values will conform to rfc4646 and the reader should refer to rfc4646 for
      syntax. This format uses the ISO standard Language (ISO-639) and region (ISO-3166)
      codes In the absence of a value the client's locale should be used, if no value is
      set, en-US should be defaulted.
      ---isPublic:Defines if the contact is public or personal. Default =
      false.
      ---source:Free format text field that identifies the entity that
      created this user record. The format of this field will be either a IP Address/
      Port or a name representing an enterprise LDAP or Avaya.
      ---sourceUserKey:The key of the user from the source system. If the
      source is an Enterprise Active Directory server, this value will be the objectGUID.
      ---suffix:The text appended to a name e.g. Jr., III.
      ---surname:The user's last name, also called the family name.
      ---title:The job function of a person in their organizational
      context.Examples: supervisor, manager
      ---ContactAddress:Represents a contact's address.
      ---addresses:A fully qualified URI for interacting with this contact.
      Any addresses added to this table should contain a qualifier e.g. sip, sips, tel,

```

mailto. The address should be syntactically valid based on the qualifier. It must be possible to add via the GUI and Interface. The application must do validation.

```

</xs:documentation>
</xs:annotation>
<xs:sequence>
  <xs:element name="company" type="xs:string" minOccurs="0"/>
  <xs:element name="description" type="xs:string" minOccurs="0"/>
  <xs:element name="displayName" type="xs:string"/>
  <xs:element name="displayNameAscii" type="xs:string"/>
  <xs:element name="dn" type="xs:string" minOccurs="0"/>
  <xs:element name="givenName" type="xs:string"/>
  <xs:element name="initials" type="xs:string" minOccurs="0"/>
  <xs:element name="middleName" type="xs:string" minOccurs="0"/>
  <xs:element name="preferredGivenName" type="xs:string" minOccurs="0"/>
  <xs:element name="preferredLanguage" type="xs:string" minOccurs="0"/>
  <xs:element name="isPublic" type="xs:boolean"/>
  <xs:element name="source" type="xs:string"/>
  <xs:element name="sourceUserKey" type="xs:string"/>
  <xs:element name="suffix" type="xs:string" minOccurs="0"/>
  <xs:element name="surname" type="xs:string"/>
  <xs:element name="title" type="xs:string" minOccurs="0"/>
  <xs:element name="ContactAddress" type="tns:xmlContactAddress"
minOccurs="0" maxOccurs="unbounded"/>
  <xs:element name="addresses" type="tns:xmlAddress" minOccurs="0"
maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="xmlHandle">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      ---HandleName:This is the name given to the user to allow
communication to be established with the user. It is an alphanumeric value that must
comply with the userinfo related portion of a URI as described in rfc2396. However,
it is further restricted as ASCII characters with only the "+" prefix to signify
this is an E.164 handle and "_" and "." special characters supported.Note, the
handle plus domain can be used to construct a user's Address of Record.
      ---handleType:The value reflecting the type of handle this is.
Possible values are "username", "e164", and "privatesubsystem".
      ---handleSubType:This is an additional qualify on the handle type
to help specify which private subsystem this handle belongs to.
      ---domainName:The text name of the domain.
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="handleName" type="xs:string"/>
    <xs:element name="handleType" type="xs:string"/>
    <xs:element name="handleSubType" type="xs:string"/>
    <xs:element name="domainName" type="xs:string" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlCommProfileType">
  <xs:sequence>
    <xs:element name="commProfileType" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlCommProfileSetType">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      ---commProfileSetName:The unique name of this CommProfile.
This is used to aid in the lookup of the CommProfile
      ---isPrimary:A boolean value indicating whether Communication
profile is primary or not.
    </xs:documentation>
  </xs:annotation>
</xs:sequence>

```

```

<xs:element name="commProfileSetName" type="xs:string"/>
<xs:element name="isPrimary" type="xs:boolean"/>
<xs:element name="handleList" minOccurs="0">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      ---handleList:List of handles
      ---handle:A user's address of record (AOR) is represented by
a combination of a handle (userpart) and domain (domainpart).The entity that
contains the userinfo part of an address that can be used to establish an
interaction with a user. A user can have multiple handles.
    </xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:element name="handle" type="tns:xmlHandle"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="commProfileList" minOccurs="0">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      ---commProfileList:List of communication profile
      ---commProfile:A communication profile is an entity that
supports communication interactions established through Avaya Communication
Services. A communication profile is used to represent a user's subscription to a
product specific communication subsystem and contains its specific configuration
needs for the user.
    </xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:element name="commProfile" type="tns:xmlCommProfileType"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
<xs:complexType name="ForgeinCommProfileType">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      ---ForeignCommProfileType:A ForeignCommProfile is used to represent a
user's address information when routing to that address is controlled by a non Avaya
system or Avaya applications not using this User CIM to populate their handles and
aliases.
      ---csEncryptionKeyId:The service will be responsible for using
this key and the secure store library API when encrypting and decrypting the
password field when respectively set or accessed by an authorized client.
      ---servicePassword:Password is an optional field if an Avaya
application needs to authenticate with the foreign service. This field will be
stored using a reversible encryption algorithm. The key will be specified through a
reference to EncryptionKey.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="ext:xmlCommProfileType">
      <xs:sequence>
        <xs:element name="csEncryptionKeyId" type="xs:long" minOccurs="0"/>
        <xs:element name="servicePassword" type="xs:string" minOccurs="0"/>
        <xs:element name="serviceData" type="xs:string" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

```

<xs:complexType name="xmlSecureStore">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      ---SecureStore:The Entity is used to persist the secure store. Each
application can have a single secure store and the application name used to
represent the secure store must be unique.
      ---passwordEncrypted :This section gets generated by the encryption
util which encrypts the userPassword and CommPassword.
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="secureStoreData" type="xs:base64Binary"/>
    <xs:element name="passwordEncrypted" type="xs:boolean"/>
  </xs:sequence>
</xs:complexType>
</xs:schema>

```

### Sample XML for bulk importing users with minimal attributes

```

<?xml version="1.0" encoding="UTF-8"?>
  <!-- Root Element 'Users' represent collection of user (containing 1 or more
users)-->
<tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/
schema/import userimport.xsd" >

  <tns:user>
    <authenticationType>Basic</authenticationType>
    <givenName>John</givenName>
    <loginName>jmiller@avaya.com</loginName>
    <surname>Miller</surname>
    <userPassword>mypassword</userPassword>
  </tns:user>

</tns:users>

```

### Sample XML for bulk importing users with all attributes

```

<?xml version="1.0" encoding="UTF-8"?>
  <!-- Root Element 'Users' represent collection of user (containing 1 or more
users)-->
<tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/
schema/import userimport.xsd" >
  <!-- authenticationType: This defines the type of authentication that this user
will undergo at runtime to obtain access to the system.Possible Values:
BASIC,ENTERPRISE
  description:A text description of the user. Human readable description of this
user instance.
  displayName:The localized name of a user to be used when displaying. It will
typically be the localized full name. This value may be provisioned from the users
enterprise directory entry. If it does not exist, synchronization rules can be used
to populate it for other fields e.g. Surname, GivenName, or LoginName.
  displayNameAscii:The full text name of the user represented in ASCII. It is used
to support display (e.g. endpoints) that cannot handle localized text.
  dn:The distinguished name of the user. The DN is a sequence of relative
distinguished names (RDN) connected by commas. An RDN is an attribute with an
associated value in the form of attribute=value, normally expressed in a UTF-8
string format.The dn can be used to identify the user and may be used for
authentication subject mapping. Note the dn is changeable.
  isDuplicatedLoginAllowed:A boolean indicator showing whether this user is
allowed a duplicate concurrent logins.A true stipulates that the user is allow to
have duplicate logins. Default value is true.
  isEnabled:A boolean indicator showing whether or not the user is active. Users
with AuthenticationType equals Basic will fail if this value is false.This attribute

```

can be used to disable access between login attempts. A running sessions login will not be revocable. Alternatively the administrator can always modify the password to disable the user from logging in. A true stipulates this is an active user, a false used for a disabled user. Default value is false.

**isVirtualUser:**A boolean indicator showing whether or not the record is being used for a non-human entity such as an application, service, software agent, etc. This is to be used where the entity will behave as a user and needs to have subset of the user profile populated. If the entity does not behave as a user and has a different trust relationship e.g. a trust certificate it should not be treated as a virtual user. A virtual user can represent an Avaya or external non-human entity. This attribute is provided as a convenience to track such accounts. A true stipulates this is a virtual users, a false is used for human users. Default value is false.

**givenName:**The first name of the user.

**honorific:**The personal title used to address a user. This is typically a social title and not the work title which is contained in the title attribute. This attribute can map to PersonalTitle.

**loginName:**This is the unique system login name given to the user. It can take the form of username@domain or just username. This may vary across customers. It can be used to help provision default user handles in the CSHandle table. The username is an alphanumeric value that must comply with the userinfo related portion of a URI as described in rfc2396. However, it is further restricted as ASCII characters with only the \_ and . special characters supported. This is the rfc2798 uid attribute.

**middleName:**The middle name of the user

**managerName:**Text name of the users manager. This is a free formed field and does not require the users manager to also be a user of the solution. This attribute was requested to support reporting needs.

**preferredGivenName:**The preferred first name of the user.

**preferredLanguage:**The individuals preferred written or spoken language. Values will conform to rfc4646 and the reader should refer to rfc4646 for syntax. This format uses the ISO standard Language ISO639 and region ISO3166 codes In the absence of a value the clients locale should be used, if no value is set, en-US should be defaulted.

**source:**Free format text field that identifies the entity that created this user record. The format of this field will be either a IP Address/Port or a name representing an enterprise LDAP or Avaya.

**sourceUserKey:**The key of the user from the source system. If the source is an Enterprise Active Directory server, this value will be the objectGUID.

**status:**This information is to help manage provisioning activities such as correcting or completing the provisioning of a user instance. It can also signify that approval is needed (PENDINGAUTHZ) before a user account is sufficiently configured to be a valid user (PROVISIONED). Possible Values: AUTHPENDING;PENDINGAUTHZ;PROVISIONED

**suffix:**The text appended to a name e.g. Jr., III.

**surname:**The users last name, also called the family name.

**timeZone:**The preferred time zone of the user. For example: (-12:00) International Date Line West.

**title:**The job function of a person in their organizational context.

**userName:**This is the username portion of the loginName field. It is an alphanumeric value that must comply with the userinfo related portion of a URI as described in rfc2396. However, it is further restricted as ASCII characters with only the \_ and . special characters supported. This is the rfc2798 uid attribute.

**userPassword:**The encrypted password for this users account. A null password is used when the user is authenticated by the enterprise such as with a separate source such as the enterprise LDAP.

**commPassword:**The encrypted subscriber or communication password with which the user logs can use to authentication with on to any CommProfile SIP and non SIP. This attribute is meant to be a shared across different communication profiles and thus different communication services.

**userType:**This enumerates the possible primary user application types. A User can be associated with multiple user types. Possible values are ADMINISTRATOR;COMMUNICATION USER;AGENT;SUPERVISOR;RESIDENT EXPERT;SERVICE TECHNICIAN;LOBBY PHONE

**roles:**Text name of a role. This value needs to pre-exist in SMGR DB

**address:**The address of the user.

**securityIdentity:**The SecurityIdentity is used to hold any additional identities

for a user that can be used for authentication such as their loginName, Kerberos account name, or their X509 certificate name.

**ownedContactLists:**It is a collection of internal or external contacts. ContactList is owned by a specific user and has a name that a unique name within the context of its owner.

**ownedContacts:**It represents a non Avaya application user (external) contact. Contacts can be collected together along with User entities into a contact list. Contacts can be created by an administrator or an end user.

**presenceUserDefault:**These are personal rules that are set by presentities to define how much presence information can be shown to watchers that are not explicitly mentioned in an ACL. There may be one User Default rule per presentity (User), or none.

**presenceUserACL:**These are personal rules defined by presentities themselves on who can monitor their presence information. There may be several entries in the list for a given presentity, each entry corresponding to one watcher.

**presenceUserCLDefault:**This is a personal rule that is set by presentities to define how much presence information can be shown to watchers that belong to the users contact list. There may be one User Contact List Default rule per presentity (Person) or none.

**commProfileSet:**A user will have a default commprofile set.A commprofile set can exist without any handles or commprofiles referencing it. I.e. you can create a commprofile set without needing to also create either a handle or a commprofile.A commprofile set can contain multiple commprofiles, but only one of each specific type. This is enforced by having the CSCommProfile uniqueness constraint include type, cs\_commprofile\_set\_id.

```
-->
<tns:user>
  <authenticationType>BASIC</authenticationType>
  <description>this is description</description>
  <displayName> John Miller</displayName>
  <displayNameAscii></displayNameAscii>
  <dn>dc=acme,dc=org</dn>
  <isDuplicatedLoginAllowed>>true</isDuplicatedLoginAllowed>
  <isEnabled>true</isEnabled>
  <isVirtualUser>>false</isVirtualUser>
  <givenName>John</givenName>
  <honorific>Mr</honorific>
  <loginName>jmiller@avaya.com</loginName>
  <middleName></middleName>
  <managerName>Jay Smith</managerName>
  <preferredGivenName>John</preferredGivenName>
  <preferredLanguage>English</preferredLanguage>
  <source>LDAP</source>
  <sourceUserKey>18966</sourceUserKey>
  <status>AUTHPENDING</status>
  <suffix>Mr</suffix>
  <surname>Miller</surname>
  <timeZone>(-12:00) International Date Line West</timeZone>
  <title>Mr</title>
  <userName>jmiller</userName>
  <userPassword>password</userPassword>
  <commPassword>mycommPassword</commPassword>
  <userType>ADMINISTRATOR</userType>
  <roles>
    <role>End-User</role>
  </roles>
  <!--addressType:Specifies the role of the address. Examples: Home, business.
  name:The Name property defines the unique label by which the address is known.
  Default format for user specific address should include user name place address type.
  building:The name or other designation of a structure
  localityName:The name of a locality, such as a city, county or other
  geographic region.
  postalCode:A code used by postal services to route mail to a destination. In the
  United States this is the zip code.
  room:Name or designation of a room.
-->
```

```

stateOrProvince:The full name of a state or province.
country:A country.
street:The physical address of the object such as an address for package delivery
postalAddress:A free formed text area for the complete physical delivery
address. It may be used in place of the specific fields in this table.
isPrivate:A boolean indicator to specify if this address could be shared across
multiple users.True is private, false is sharable. Default is false.
-->
<address>
  <addressType>OFFICE</addressType>
  <name>Avaya Office</name>
  <building>building 11</building>
  <localityName>Magarpatta</localityName>
  <postalCode>411028</postalCode>
  <room>room 502</room>
  <stateOrProvince>Maharashtra</stateOrProvince>
  <country>India</country>
  <street>street</street>
  <postalAddress></postalAddress>
  <isPrivate>>true</isPrivate>
</address>
<!-- SecurityIdentity:Represents the possible external identities that a user
may have for the purpose of authentication. The type and format of an identity
depends on the external Identity Provider and can include X.509 certificates or
Kerberos user accounts
identity:The unique external identity of the user. This is a free text field and
no format is enforced. The format will depend on the identity type. Kerberos user
account can take the form of: username@domainName
e.g. jsmith@acme.org
realm:The name of the security domain that this identity is valid in.
type:The text representation of the type of identity. Possible values are:
principalname,X509 and Kerberos
-->
<securityIdentity>
  <identity>jmiller@acme.org </identity>
  <realm>acme</realm>
  <type>principalname</type>
</securityIdentity>
<!--ContactList:The ContactList is a collection of personal or public groups
containing external contacts and/or Avaya users.
name:The text name of the list. This in the context of the owner must be unique.
description:A free text description of this member.
isPublic:Defines if the contact is public or personal. Default = false.
members:Represents the list of users or contacts that belong to contact list
contactListType:Specifies the type categorizing this list.
-->
<ownedContactLists>
  <contactList>
    <name>MycontactList</name>
    <description>This is my contactList</description>
    <isPublic>>false</isPublic>
    <!--
      memberContact:This represents the name of the Contact.A
ContactListMember can either be a Contact o User
      speedDialContactAddress:A Contact Address added as a favorite entry
      memberUser:This represents the loginname of the User.A
ContactListMember can either be a Contact or User
      speedDialHandle:A handle added as a favorite entry
      isFavorite:A boolean indicator that reflects whether this contact
is a favorite entry. If true, the value of entryindex would show which position to
place this entry in any display.
      isSpeedDial:Each contact list member can also be flagged as a favorite
(a.k.a. speed dial)
      speedDialEntry:For either a presence buddy or favorite entry, a
specific communication address to use can be pointed to.
    -->
  </contactList>
</ownedContactLists>

```

```

        isPresenceBuddy:Each contact list member can also be flagged as a
presence buddy
        label:A free text short word or phrase for classifying this contact
list member.
        altLabel:A free text short word or phrase for classifying this
contact. This is similar to label, but it is used to store alternate language
representations.
        description:A free text description of this member.
-->
<members>
  <memberContact>Phil Bath</memberContact>
  <speedDialContactAddress>
    <address>+44-1234568</address>
    <altLabel>Phone</altLabel>
    <contactCategory>OFFICE</contactCategory>
    <contactType>PHONE</contactType>
    <label>Phone</label>
  </speedDialContactAddress>
  <isFavorite>true</isFavorite>
  <isSpeedDial>true</isSpeedDial>
  <speedDialEntry>1234</speedDialEntry>
  <isPresenceBuddy>true</isPresenceBuddy>
  <label>My Contact in Dublin office</label>
  <altLabel>Phone Number for contacting Denver office</altLabel>
  <description>Contact Details</description>
  <priorityLevel>0</priorityLevel>
</members>
<contactListType>CONTACTCENTER</contactListType>
</contactList>
</ownedContactLists>
<!-- Contact:An entity that represents a non Avaya application user (external)
contact. Contacts can be collected together along with User entities into a contact
list. Contacts can be created by an administrator or an end user. Contacts have name
attributes, and owner, and can be public or personal.A contact also includes one or
more contact addresses that can be used for establishing an interaction with the
contact. Contacts can be designated as being a users presence buddy or added as a
favorite entry (i.e. speed dial).
  company:The organization that the contact belongs to.
  description:A free text field containing human readable text providing
information on this entry.
  displayName:The localized name of a contact to be used when displaying. It will
typically be the localized full name. This value may be provisioned from the users
enterprise directory entry. If it does not exist, synchronization rules can be used
to populate it for other fields e.g. Surname, GivenName, or LoginName.
  displayNameAscii:The full text name of the contact represented in ASCII. It is
used to support display (e.g. endpoints) that cannot handle localized text.
  dn:The distinguished name of the user. The DN is a sequence of relative
distinguished names (RDN) connected by commas. An RDN is an attribute with an
associated value in the form of attribute=value, normally expressed in a UTF-8
string format.The dn can be used to uniquely identify this record. Note the dn is
changeable.
  givenName:The first name of the contact.
  initials:Initials of the contact
  middleName:The middle name of the contact.
  preferredGivenName:The nick name of the contact.
  preferredLanguage:The individuals preferred written or spoken language. Values
will conform to rfc4646 and the reader should refer to rfc4646 for syntax. This
format uses the ISO standard Language ISO639 and region ISO3166 codes In the absence
of a value the clients locale should be used, if no value is set, en-US should be
defaulted.
  isPublic:Defines if the contact is public or personal. Default = false.
  source:Free format text field that identifies the entity that created this user
record. The format o this field will be either a IP Address/Port or a name
representing an enterprise LDAP or Avaya.
  sourceUserKey:The key of the user from the source system. If the source is an

```

Enterprise Active Directory server, this value will be the objectGUID.

suffix:The text appended to a name e.g. Jr., III.

surname:The users last name, also called the family name.

title:The job function of a person in their organizational context.Examples:  
supervisor, manager

ContactAddress:Represents a contacts address.

addresses:A fully qualified URI for interacting with this contact. Any addresses added to this table should contain a qualifier e.g. sip, sips, tel, mailto. The address should be syntactically valid based on the qualifier. It must be possible to add via the GUI and Interface. The application must do validation.

```
-->
<ownedContacts>
  <contact>
    <company>ABC</company>
    <description>Company ABC description</description>
    <displayName>Phil Bath</displayName>
    <displayNameAscii></displayNameAscii>
    <dn>dc=acme,dc=org</dn>
    <givenName>John</givenName>
    <initials>Mr</initials>
    <middleName>M</middleName>
    <preferredGivenName>Phil</preferredGivenName>
    <preferredLanguage>English</preferredLanguage>
    <isPublic>>false</isPublic>
    <source>ldap</source>
    <sourceUserKey>123546</sourceUserKey>
    <suffix>Jr.</suffix>
    <surname>Bath</surname>
    <title>Manager</title>
  <!--
    type:The value reflecting the type of handle this is. Possible values are
    username, e164, and privatesubsystem
    category:The value representing a further qualification to the contact
    address. Possible values include Office, Home, Mobile.
    handle:This is the name given to the user to allow communication to be
    established with the user. It is an alphanumeric value that must comply with the
    userinfo related portion of a URI as described in rfc2396. However, it is further
    restricted as ASCII characters with only the + prefix to signify this is an E.164
    handle and _ and . special characters supported.The handle and type together are
    unique within a specific domain. Note, the handle plus domain can be used to
    construct a users Address of Record.
    label:A free text description for classifying this contact.
    altLabel:A free text description for classifying this contact. This is
    similar to ContactLabel, but it is used to store alternate language representations.
  -->
  <ContactAddress>
    <address>+44-1234568</address>
    <altLabel>Phone</altLabel>
    <contactCategory>OFFICE</contactCategory>
    <contactType>PHONE</contactType>
    <label>Phone</label>
  </ContactAddress>
  <addresses>
  <!--
    addressType:The unique text name of the address type. Possible values are:
    Home, business.
    name: The Name property defines the unique label by which the address is
    known. Default format for user specific address should include user name place
    address type.
    building:The name or other designation of a structure.
    localityName:The name of a locality, such as a city, county or other
    geographic region.
    postalCode:A code used by postal services to route mail to a destination.
    In the United States this is the zip code.
```

```

    room:Name or designation of a room.
    stateOrProvince:The full name of a state or province.
    country:A country.
    street:The physical address of the object such as an address for package
delivery
    postalAddress:A free formed text area for the complete physical delivery
address. It may be used in place of the specific fields in this table.
-->

    <addressType>office</addressType>
    <name>Phil Bath</name>
    <building>building A</building>
    <localityName>Magarpatta</localityName>
    <postalCode>411048</postalCode>
    <room>room 123</room>
    <stateOrProvince>MH</stateOrProvince>
    <country>India</country>
    <street>Hadapsar</street>
    <isPrivate>true</isPrivate>

    </addresses>
    </contact>
    </ownedContacts>
    <!-- PresUserDefault:These are personal rules that are set by presentities
to define how much presence information can be shown to watchers that are not
explicitly mentioned in an ACL. There may be one User Default rule per presentity
(User), or none.presentity (User), or none.
presentity (User), or none.
    label:A unique string that names this info type (e.g. Telephony Presence).
    filter:Internal definition of which part of presence information is
covered by this info type. The value of this field should be treated as opaque
string; it is maintained and used only by Presence services.
    specFlags:This field is empty for regular info types, but for special info
types it contains a comma separated list of keywords that identify these types. In
this version only FULL that represents full presence information is supported.
-->
    <presenceUserDefault>
    <infoTypeAccess>
    <infoType>
    <label>Telephony Presence</label>
    <filter>filter</filter>
    <specFlags>FULL</specFlags>
    </infoType>
    <access>BLOCK</access>
    </infoTypeAccess>
    </presenceUserDefault>
    <!--UserACLEntry:These are personal rules defined by presentities themselves on
who can monitor their presence information. There may be several entries in the list
for a given presentity, each entry corresponding to one watcher.
    label:A unique string that names this info type (e.g. Telephony Presence).
    filter:Internal definition of which part of presence information is
covered by this info type. The value of this field should be treated as opaque
string; it is maintained and used only by Presence services.
    specFlags:This field is empty for regular info types, but for special info
types it contains a comma separated list of keywords that identify these types. In
this version only FULL that represents full presence information is supported.
-->
    <presenceUserACL>
    <infoTypeAccess>
    <infoType>
    <label>ALL</label>
    <filter>filter</filter>
    <specFlags>FULL</specFlags>
    </infoType>
    <access>BLOCK</access>

```

```

    </infoTypeAccess>
    <watcherLoginName>admin</watcherLoginName>
  </presenceUserACL>
  <!--PresUserCLDefault:This is a personal rule that is set by presentities to
define how much presence information can be shown to watchers that belong to the
users contact list. There may be one User Contact List Default rule per presentity
(Person) or none.
-->
  <presenceUserCLDefault>
    <infoTypeAccess>
      <infoType>
        <label>Telephony</label>
        <filter>filter</filter>
        <specFlags>FULL</specFlags>
      </infoType>
      <access>BLOCK</access>
    </infoTypeAccess>
  </presenceUserCLDefault>
  <!--commProfileSet:A user will have a default commprofile set.A commprofile set can
exist without any handles or commprofiles referencing it. I.e. you can create a
commprofile set without needing to also create either a handle or a commprofile.A
commprofile set can contain multiple commprofiles, but only one of each specific
type. This is enforced by having the CommProfile uniqueness constraint include type,
commprofile_set_id.
  HandleName:This is the name given to the user to allow communication to be
established with the user. It is an alphanumeric value that must comply with the
userinfo related portion of a URI as described in rfc2396. However, it is further
restricted as ASCII characters with only the + prefix to signify this is an E.164
handle and _ and . special characters supported.Note, the handle plus domain can be
used to construct a users Address of Record.
  handleType:The value reflecting the type of handle this is. Possible values are
username, e164, and privatesubsystem.
  handleSubType:This is an additional qualify on the handle type to help specify
which private subsystem this handle belongs to.
  domainName:The text name of the domain.
-->
  <commProfileSet>
    <commProfileSetName>Primary</commProfileSetName>
    <isPrimary>>true</isPrimary>
    <handleList>
      <handle>
        <handleName>sip:abc@yahoo.com</handleName>
        <handleType>sip</handleType>
        <handleSubType>msrtc</handleSubType>
      </handle>
    </handleList>
    <!--The below is extended communication profile-->
  <!--
  <commProfileList>
    <commProfile xsi:type="ext:ASCommProfile" xmlns:ext="http://xml.avaya.com/
schema/import1">
      <commProfileType>ASM</commProfileType>
      <ext:forkingPolicy>Sequential</ext:forkingPolicy>
      <ext:origApplicationSet>Default Denever Origination</
ext:origApplicationSet>
      <ext:termApplicationSet>Default Denever Termination</
ext:termApplicationSet>
      <ext:userCommunity>Denever</ext:userCommunity>
      <ext:subscriptionSet>subscriptionSet</ext:subscriptionSet>
    </commProfile>
  </commProfileList>
-->
</commProfileSet>

```

```
</tns:user>
</tns:users>
```

## XML Schema Definition for partially importing users

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<xs:schema xmlns:delta="http://xml.avaya.com/schema/deltaImport"
xmlns:base="http://xml.avaya.com/schema/import" xmlns:xs="http://www.w3.org/2001/
XMLSchema" targetNamespace="http://xml.avaya.com/schema/deltaImport" version="1.0">

  <xs:import namespace="http://xml.avaya.com/schema/import"
schemaLocation="userimport.xsd"/>

  <xs:element name="userDelta" type="delta:xmlUserDelta"/>
  <xs:element name="deltaUserList" type="delta:xmlDeltaUserList"/>

  <xs:complexType name="xmlDeltaUserList">
    <xs:sequence>
      <xs:element name="secureStore" type="base:xmlSecureStore"/></xs:element>
      <xs:element name="userDelta" type="delta:xmlUserDelta" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="xmlUserDelta">
    <xs:sequence>
      <xs:element name="authenticationType"
type="xs:string" minOccurs="0" maxOccurs="1" />
      <xs:element name="description" type="xs:string"
minOccurs="0" />
      <xs:element name="displayName" type="xs:string"
minOccurs="0" />
      <xs:element name="displayNameAscii" type="xs:string"
minOccurs="0" />
      <xs:element name="dn" type="xs:string" minOccurs="0" />
      <xs:element name="isDuplicatedLoginAllowed"
type="xs:boolean" minOccurs="0" />
      <xs:element name="isEnabled" type="xs:boolean" minOccurs="0"
maxOccurs="1" />
      <xs:element name="isVirtualUser" type="xs:boolean"
minOccurs="0" />
      <xs:element name="givenName" type="xs:string" maxOccurs="1"
minOccurs="0" />
      <xs:element name="honorific" type="xs:string" minOccurs="0" />
      <xs:element name="loginName" type="xs:string" maxOccurs="1"
minOccurs="1" />
      <xs:element name="middleName" type="xs:string"
minOccurs="0" />
      <xs:element name="managerName" type="xs:string"
minOccurs="0" />
      <xs:element name="preferredGivenName" type="xs:string"
minOccurs="0" />
      <xs:element name="preferredLanguage" type="xs:string"
minOccurs="0" />
      <xs:element name="source" type="xs:string" minOccurs="0"
maxOccurs="1" />
      <xs:element name="sourceUserKey" type="xs:string"
minOccurs="0" maxOccurs="1" />
      <xs:element name="status" type="xs:string"
minOccurs="0" />
      <xs:element name="suffix" type="xs:string" minOccurs="0" />
      <xs:element name="surname" type="xs:string" minOccurs="0"
maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>

```

```

<xs:element name="timeZone" type="xs:string" minOccurs="0" />
<xs:element name="title" type="xs:string" minOccurs="0" />
<xs:element name="userName" type="xs:string" maxOccurs="1"
minOccurs="0" />
<xs:element name="userPassword" type="xs:string"
minOccurs="0" />
<xs:element name="commPassword" type="xs:string"
minOccurs="0" />
<xs:element name="userType" type="xs:string"
minOccurs="0" maxOccurs="unbounded" />
<xs:element name="roles" minOccurs="0">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="role" type="xs:string"
minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="address" type="base:xmlAddress"
minOccurs="0" maxOccurs="unbounded" />
<xs:element name="securityIdentity"
type="base:xmlSecurityIdentity" minOccurs="0" maxOccurs="unbounded" />
<!-- Contact list Entries -->
<xs:element name="ownedContactLists" minOccurs="0"
maxOccurs="1">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="contactList"
type="base:xmlContactList" maxOccurs="1" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="ownedContacts" minOccurs="0">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="contact" type="base:xmlContact"
maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<!-- Presence ACL User Entries -->
<xs:element name="presenceUserDefault"
type="base:xmlPresUserDefaultType" minOccurs="0" />
<xs:element name="presenceUserACL"
type="base:xmlPresUserACLEntryType" minOccurs="0"
maxOccurs="unbounded" />
<xs:element name="presenceUserCLDefault"
type="base:xmlPresUserCLDefaultType" minOccurs="0" maxOccurs="1" />
<xs:element name="commProfileSet"
type="base:xmlCommProfileSetType" maxOccurs="unbounded" minOccurs="0">
  </xs:element>
</xs:sequence>
</xs:complexType>
</xs:schema>

```

### Sample XML for partially importing users

```

<?xml version="1.0" encoding="UTF-8"?>
<delta:deltaUserList xmlns:delta="http://xml.avaya.com/schema/deltaImport"
xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd ">
  <delta:userDelta>
    <authenticationType>ENTERPRISE</authenticationType>
    <description>this is description</description>
  </delta:userDelta>
</delta:deltaUserList>

```

```

<displayName>John Miller</displayName>
<displayNameAscii></displayNameAscii>
<dn>dc=acme,dc=org</dn>
<isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
<isEnabled>true</isEnabled>
<isVirtualUser>true</isVirtualUser>
<givenName>John</givenName>
<honorific>Mr</honorific>
<loginName>jmiller@avaya.com</loginName>
<middleName></middleName>
<managerName>Jay Smith</managerName>
<preferredGivenName>John</preferredGivenName>
<preferredLanguage>English</preferredLanguage>
<source>LDAP</source>
<sourceUserKey>18966</sourceUserKey>
<status>AUTHPENDING</status>
<suffix>Mr</suffix>
<surname>Miller</surname>
<timeZone>(-12:00) International Date Line West</timeZone>
<title>Mr</title>
<userName>jmiller</userName>
<commPassword>mycommPassword</commPassword>
<userType>ADMINISTRATOR</userType>
<roles>
  <role>End-User</role>
</roles>
<address>
  <addressType>OFFICE</addressType>
  <name>Avaya Office</name>
  <building>building 11</building>
  <localityName>Magarpatta</localityName>
  <postalCode>411028</postalCode>
  <room>room 502</room>
  <stateOrProvince>Maharashtra</stateOrProvince>
  <country>India</country>
  <street>street</street>
  <postalAddress></postalAddress>
  <isPrivate>true</isPrivate>
</address>
<securityIdentity>
  <identity>jmiller@acme.org </identity>
  <realm>acme</realm>
  <type>principalname</type>
</securityIdentity>
<ownedContactLists>
  <contactList>
    <name>MycontactList</name>
    <description>This is my contactList</description>
    <isPublic>false</isPublic>
    <members>
      <memberContact>Phil Bath</memberContact>
      <speedDialContactAddress>
        <address>+44-1234568</address>
        <altLabel>Phone</altLabel>
        <contactCategory>OFFICE</contactCategory>
        <contactType>PHONE</contactType>
        <label>Phone</label>
      </speedDialContactAddress>
      <isFavorite>true</isFavorite>
      <isSpeedDial>true</isSpeedDial>
      <speedDialEntry>1234</speedDialEntry>
      <isPresenceBuddy>true</isPresenceBuddy>
      <label>My Contact in Dublin office</label>
      <altLabel>Phone Number for contacting Denver office</altLabel>
      <description>Contact Details</description>
    
```

```

    <priorityLevel>0</priorityLevel>
  </members>
  <contactListType>CONTACTCENTER</contactListType>
</contactList>
</ownedContactLists>
<ownedContacts>
  <contact>
    <company>ABC</company>
    <description>Company ABC description</description>
    <displayName>Phil Bath</displayName>
    <displayNameAscii></displayNameAscii>
    <dn>dc=acme,dc=org</dn>
    <givenName>John</givenName>
    <initials>Mr</initials>
    <middleName>M</middleName>
    <preferredGivenName>Phil</preferredGivenName>
    <preferredLanguage>English</preferredLanguage>
    <isPublic>>false</isPublic>
    <source>ldap</source>
    <sourceUserKey>123546</sourceUserKey>
    <suffix>Jr.</suffix>
    <surname>Bath</surname>
    <title>Manager</title>
    <ContactAddress>
      <address>+44-1234568</address>
      <altLabel>Phone</altLabel>
      <contactCategory>OFFICE</contactCategory>
      <contactType>PHONE</contactType>
      <label>Phone</label>
    </ContactAddress>
    <addresses>
      <addressType>office</addressType>
      <name>Phil Bath</name>
      <building>building A</building>
      <localityName>Magarpatta</localityName>
      <postalCode>411048</postalCode>
      <room>room 123</room>
      <stateOrProvince>MH</stateOrProvince>
      <country>India</country>
      <street>Hadapsar</street>
      <isPrivate>>true</isPrivate>
    </addresses>
  </contact>
</ownedContacts>
<presenceUserDefault>
  <infoTypeAccess>
    <infoType>
      <label>Telephony Presence</label>
      <filter>filter</filter>
      <specFlags>FULL</specFlags>
    </infoType>
    <access>BLOCK</access>
  </infoTypeAccess>
</presenceUserDefault>
<presenceUserACL>
  <infoTypeAccess>
    <infoType>
      <label>ALL</label>
      <filter>filter</filter>
      <specFlags>FULL</specFlags>
    </infoType>
    <access>BLOCK</access>
  </infoTypeAccess>
  <watcherLoginName>admin</watcherLoginName>
</presenceUserACL>

```

```

    <presenceUserCLDefault>
      <infoTypeAccess>
        <infoType>
          <label>Telephony</label>
          <filter>filter</filter>
          <specFlags>FULL</specFlags>
        </infoType>
        <access>BLOCK</access>
      </infoTypeAccess>
    </presenceUserCLDefault>

  </delta:userDelta>
</delta:deltaUserList>

```

## XML Schema Definition for bulk deleting users

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/bulkdelete"
targetNamespace="http://xml.avaya.com/schema/bulkdelete"
  elementFormDefault="qualified" version="1.0" xmlns:xs="http://www.w3.org/
2001/XMLSchema" >

  <xs:element name="user" type="tns:xmlUserDelete" />
  <xs:element name="deleteType" type="tns:xmlDeleteType" />

  <xs:element name="deleteUsers">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="deleteType" type="tns:xmlDeleteType" maxOccurs="1"
minOccurs="1"/>
        <xs:element minOccurs="1" maxOccurs="unbounded" name="user"
type="tns:xmlUserDelete" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="xmlUserDelete">
    <xs:sequence>
      <xs:element name="loginName" minOccurs="1" maxOccurs="1">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:maxLength value="128"></xs:maxLength>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element name="id" type="xs:string" maxOccurs="1" minOccurs="0"></
xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="xmlDeleteType">
    <xs:restriction base="xs:string"></xs:restriction>
  </xs:simpleType>
</xs:schema>

```

## Sample XML for bulk deleting users

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:deleteUsers xmlns:tns="http://xml.avaya.com/schema/bulkdelete"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
xml.avaya.com/schema/bulkdelete UserProfileSchemaDefinitionForBulkDelete.xsd ">
  <tns:deleteType>soft</tns:deleteType>
  <tns:user>
    <tns:loginName>jmiller@avaya.com</tns:loginName>

```

```

</tns:user>
</tns:deleteUsers>

```

## XML Schema Definition for bulk importing elements

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://www.avaya.com/rts"
  xmlns="http://www.avaya.com/rts"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">

  <!-- <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"> -->
  <xs:element name="RTSElements">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="ApplicationSystems" minOccurs="0"
          maxOccurs="unbounded">
          <xs:annotation>
            <xs:documentation>
              Application System Types
            </xs:documentation>
          </xs:annotation>
          <xs:complexType>
            <xs:sequence>
              <xs:element name="ApplicationSystem"
                type="ApplicationSystem" maxOccurs="unbounded">
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="ApplicationSystemAssigns"
          minOccurs="0" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Source" type="Source"
                minOccurs="1" maxOccurs="unbounded" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="ApplicationSystem">
    <xs:annotation>
      <xs:documentation></xs:documentation>
    </xs:annotation>

    <xs:sequence>
      <xs:element name="Host" type="Host" minOccurs="1"
        maxOccurs="1">
      </xs:element>
      <xs:element name="ApplicationSystemType"
        type="ApplicationSystemType" minOccurs="1" maxOccurs="1">
      </xs:element>

      <xs:element name="SecureStoreData" type="SecureStoreData" minOccurs="0"
        maxOccurs="1"/>

      <xs:element name="AccessPoints" minOccurs="0"
        maxOccurs="unbounded">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="AccessPoint"

```

```

        type="AccessPoint" minOccurs="1" maxOccurs="unbounded" />
    </xs:sequence>
</xs:complexType>
</xs:element>

<xs:element name="Ports" minOccurs="0"
maxOccurs="unbounded">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="Port" type="Port"
                minOccurs="1" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

<xs:element name="SNMPAttributes" type="SNMPAttributes" minOccurs="0"
maxOccurs="1">
</xs:element>

<xs:element name="Attributes" minOccurs="0"
maxOccurs="unbounded">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="Attribute" type="Attribute"
                minOccurs="1" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>
</xs:element>

</xs:sequence>

<xs:attribute name="name" type="xs:string" use="required">
</xs:attribute>

<xs:attribute name="description" type="xs:string">
</xs:attribute>

<xs:attribute name="displaykey" type="xs:string"></xs:attribute>

<xs:attribute name="isTrusted" type="xs:boolean"></xs:attribute>

</xs:complexType>
<xs:complexType name="SNMPAttributes">
    <xs:annotation>
        <xs:documentation></xs:documentation>
    </xs:annotation>
    <xs:attribute name="snmpVersion" type="snmpVersionType" use="required">
</xs:attribute>

    <xs:attribute name="readCommunity" type="xs:string">
</xs:attribute>

    <xs:attribute name="writeCommunity" type="xs:string">
</xs:attribute>

    <xs:attribute name="userName" type="xs:string">
</xs:attribute>

    <xs:attribute name="authenticationProtocol"
type="authenticationProtocolType">
</xs:attribute>

    <xs:attribute name="authenticationPassword" type="xs:string">
</xs:attribute>

```

```

<xs:attribute name="privacyProtocol" type="privacyProtocolType">
</xs:attribute>

<xs:attribute name="privacyPassword" type="xs:string">
</xs:attribute>

<xs:attribute name="snmpRetries" type="xs:int" use="required">
</xs:attribute>

<xs:attribute name="snmpTimeout" type="xs:long" use="required">
</xs:attribute>

<xs:attribute name="deviceTypeName" type="xs:string"> </xs:attribute>

<xs:attribute name="sysOid" type="xs:string">
</xs:attribute>
</xs:complexType>

<xs:complexType name="Host">
<xs:annotation>
  <xs:documentation></xs:documentation>
</xs:annotation>

<xs:attribute name="ipaddress" type="xs:string"
  use="required">
</xs:attribute>

<xs:attribute name="description" type="xs:string">
</xs:attribute>

<xs:attribute name="ostype" type="xs:string"></xs:attribute>
</xs:complexType>

<xs:complexType name="ApplicationSystemType">
<xs:annotation>
  <xs:documentation></xs:documentation>
</xs:annotation>

<xs:attribute name="name" type="xs:string" use="required">
</xs:attribute>

<xs:attribute name="version" type="xs:string" use="required">
</xs:attribute>
</xs:complexType>

<xs:complexType name="AccessPoint">
<xs:annotation>
  <xs:documentation></xs:documentation>
</xs:annotation>

<xs:attribute name="name" type="xs:string" use="required">
</xs:attribute>

<xs:attribute name="description" type="xs:string">
</xs:attribute>

<xs:attribute name="displaykey" type="xs:string"></xs:attribute>

<xs:attribute name="type" type="AccessPointType"
  use="required">
</xs:attribute>

<xs:attribute name="uri" type="xs:string"></xs:attribute>

```

```

<xs:attribute name="host" type="xs:string" use="required">
</xs:attribute>

<xs:attribute name="port" type="xs:string"></xs:attribute>

<xs:attribute name="protocol" type="xs:string"></xs:attribute>

<xs:attribute name="loginid" type="xs:string"></xs:attribute>

<xs:attribute name="password" type="xs:string"></xs:attribute>

<xs:attribute name="containerType" type="ContainerType"></xs:attribute>

<xs:attribute name="order" type="xs:int" use="required">
</xs:attribute>

</xs:complexType>

<xs:complexType name="Port">
  <xs:annotation>
    <xs:documentation></xs:documentation>
  </xs:annotation>

  <xs:attribute name="name" type="xs:string" use="required">
</xs:attribute>

  <xs:attribute name="description" type="xs:string">
</xs:attribute>

  <xs:attribute name="protocol" type="xs:string" use="required"></xs:attribute>

  <xs:attribute name="port" type="xs:int" use="required"></xs:attribute>
</xs:complexType>

<xs:complexType name="Source">
  <xs:sequence>
    <xs:element name="Assignment" minOccurs="1"
      maxOccurs="unbounded">
      <xs:complexType>
        <xs:attribute name="name" type="xs:string">
</xs:attribute>

        <xs:attribute name="targetAppSystemName"
          type="xs:string" use="required">
</xs:attribute>

        <xs:attribute name="targetAppSystemTypeName"
          type="xs:string" use="required">
</xs:attribute>

        <xs:attribute name="targetAppSystemTypeVersion"
          type="xs:string" use="required">
</xs:attribute>

        <xs:attribute name="targetAppSystemHost"
          type="xs:string" use="required">
</xs:attribute>

        <xs:attribute name="priority" type="xs:int"></xs:attribute>
      </xs:complexType>
    </xs:element>
  </xs:sequence>

  <xs:attribute name="sourceApplicationSystemName"
    type="xs:string" use="required">

```

```

</xs:attribute>

<xs:attribute name="sourceAppSystemTypeName" type="xs:string"
  use="required">
</xs:attribute>

<xs:attribute name="sourceAppSystemTypeVersion" type="xs:string"
  use="required">
</xs:attribute>

<xs:attribute name="sourceAppSystemHost" type="xs:string"
  use="required">
</xs:attribute>
</xs:complexType>

<xs:complexType name="Attribute">
  <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
  <xs:attribute name="value" type="xs:string" use="required"></xs:attribute>
  <!-- added for secure store integration. -->
  <xs:attribute name="isencrypted" type="xs:boolean" use="optional"
default="false"></xs:attribute>
</xs:complexType>

<xs:complexType name="SecureStoreData">
  <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
  <xs:attribute name="value" type="xs:string" use="required"></
xs:attribute>
</xs:complexType>

<xs:simpleType name="AccessPointType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="TrustManagement" />
    <xs:enumeration value="EMURL" />
    <xs:enumeration value="WS" />
    <xs:enumeration value="GUI" />
    <xs:enumeration value="Other" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ContainerType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="JBOSS" />
    <xs:enumeration value="SIPAS" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="authenticationProtocolType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="MD5" />
    <xs:enumeration value="SHA" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="privacyProtocolType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="DES"/>
    <xs:enumeration value="3DES"/>
    <xs:enumeration value="AES128"/>
    <xs:enumeration value="AES192"/>
    <xs:enumeration value="AES256"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="snmpVersionType">
  <xs:restriction base="xs:int">
    <xs:enumeration value="1"/>

```

```

        <xs:enumeration value="3"/>
    </xs:restriction>
</xs:simpleType>

</xs:schema>

```

### Sample XML for bulk importing elements

```

<?xml version="1.0" encoding="UTF-8"?>
<RTSElements xsi:schemaLocation="http://www.avaya.com/rts ApplicationSystems.xsd "
xmlns="http://www.avaya.com/rts" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
  <ApplicationSystems>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test1">
      <Host description="Host" ipaddress="localhost" ostype="Host"/>
      <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test2">
      <Host description="Host" ipaddress="localhost" ostype="Host"/>
      <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test3">
      <Host description="Host" ipaddress="localhost" ostype="Host"/>
      <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test4">
      <Host description="Host" ipaddress="localhost" ostype="Host"/>
      <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test5">
      <Host description="Host" ipaddress="localhost" ostype="Host"/>
      <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test6">
      <Host description="Host" ipaddress="localhost" ostype="Host"/>
      <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test7">
      <Host description="Host" ipaddress="localhost" ostype="Host"/>
      <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test8">
      <Host description="Host" ipaddress="localhost" ostype="Host"/>
      <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test9">
      <Host description="Host" ipaddress="localhost" ostype="Host"/>
      <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test10">
      <Host description="Host" ipaddress="localhost" ostype="Host"/>
      <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Tes11t">

```

```

        <Host description="Host" ipaddress="localhost" ostype="Host"/>
        <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test12">
        <Host description="Host" ipaddress="localhost" ostype="Host"/>
        <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test13">
        <Host description="Host" ipaddress="localhost" ostype="Host"/>
        <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
    <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test14">
        <Host description="Host" ipaddress="localhost" ostype="Host"/>
        <ApplicationSystemType name="Other Applications" version="0"/>
    </ApplicationSystem>
</ApplicationSystems>
</RTSElements>

```

## XML Schema Definition for bulk importing Session Manager profiles

```

<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:smgr="http://xml.avaya.com/schema/import"
    targetNamespace="http://xml.avaya.com/schema/import_sessionmanager"
    elementFormDefault="qualified">
<xsd:import namespace="http://xml.avaya.com/schema/import"
    schemaLocation="userimport.xsd"/>

<xsd:complexType name="SessionManagerCommProfXML">
<xsd:complexContent>
<xsd:extension base="smgr:xmlCommProfileType" >
<xsd:sequence>
<xsd:element name="primarySM" type="xsd:string"/>
    <xsd:element name="secondarySM" type="xsd:string" minOccurs="0" />
    <xsd:element name="terminationAppSequence"
type="xsd:string" minOccurs="0" />
    <xsd:element name="originationAppSequence"
type="xsd:string" minOccurs="0" />
    <xsd:element name="survivabilityServer"
type="xsd:string" minOccurs="0" />
    <xsd:element name="homeLocation"
type="xsd:string" minOccurs="0" />
</xsd:sequence>
</xsd:extension>
</xsd:complexContent>
</xsd:complexType>
</xsd:schema>

```

## Sample XML for bulk importing Session Manager profiles

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd ">

    <!-- User Record for: 5555555@domain.com -->
    <tns:user>

(Other user elements are required here - consult the main user record XML schema
reference)

    <!-- This is the password for any SIP endpoints (phones)

```

## Managing Users

```
        associated with the user's Session Manager Profile -->
        <commPassword>123456</commPassword>

(Other user elements may be required here - consult the main user record XML schema
reference)

        <!-- Here, a Communication Profile is defined for the user -->
        <commProfileSet>
            <commProfileSetName>Primary</commProfileSetName>
            <isPrimary>true</isPrimary>

<!-- The user must be given one or more handles of type "SIP"
to associate SIP devices with the Session Manager
Profile. In this case, a SIP phone will be registered
with a Session Manager as 5555555@domain.com -->
        <handleList>
            <handle>
                <handleName>5555555</handleName>
                <handleType>sip</handleType>
                <handleSubType>username</handleSubType>
                <domainName>domain.com</domainName>
            </handle>
        </handleList>

        <!-- Here, one or more product-specific profiles may be
        Defined -->
<commProfileList>

<!-- A Session Manager Profile is defined to associate
the SIP phone, 5555555@domain.com, with a primary
and secondary Session Manager instance
("Primary SM" and "Secondary SM"),
origination and termination application
sequences (both are "Sequence to My CM"),
a Survivability Server ("BSM"), and the user
is given the Home Location, "My Home" -->
        <commProfile xsi:type="sm:SessionManagerCommProfXML"
xmlns:sm="http://xml.avaya.com/schema/import_sessionmanager">
            <commProfileType>SessionManager</commProfileType>
            <sm:primarySM>Primary SM</sm:primarySM>
            <sm:secondarySM>Secondary SM</sm:secondarySM>
            <sm:terminationAppSequence>Sequence to My CM
        </sm:terminationAppSequence>
            <sm:originationAppSequence>Sequence to My CM
        </sm:originationAppSequence>
            <sm:survivabilityServer>BSM
        </sm:survivabilityServer>
            <sm:homeLocation>My Home</sm:homeLocation>
        </commProfile>

<!-- A CM Station Profile is associated with this
Communication Profile. The application
sequence, "Sequence to My CM", invoked by
Session Manager for calls to and from
5555555@domain.com, sequences calls to the
CM, "My CM". SIP devices associated
with this Communication Profile are associated
with the CM Station that has number 555-5555. The
CM Station, 555-5555, already exists on the CM, so the
"useExistingExtension" element has value "true". -->
<commProfile xsi:type="ipt:xmlStationProfile"
xmlns:ipt="http://xml.avaya.com/schema/import_csm_cm">
            <commProfileType>CM</commProfileType>
            <ipt:cmName>My CM</ipt:cmName>
```

```

        <ipt:useExistingExtension>true</ipt:useExistingExtension>
        <ipt:extension>5555555</ipt:extension>
    </commProfile>

</commProfileList>
</commProfileSet>
</tns:user>
</tns:users>

```

## XML Schema Definition for bulk importing endpoint profiles

```

<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:one="http://
xml.avaya.com/schema/import" elementFormDefault="qualified"
targetNamespace="http://xml.avaya.com/schema/import_csm_cm" xmlns:csm="http://
xml.avaya.com/schema/import_csm_cm">
<xs:import namespace="http://xml.avaya.com/schema/import"
schemaLocation="userimport.xsd"/>

<!--Changes in xsd file need to generate jaxb src using this xsd-->
<xs:complexType name="xmlStationProfile">
    <xs:complexContent>
        <xs:extension base="one:xmlCommProfileType" >
            <xs:sequence>
                <!-- CM Name as it appears under 'Applications/Application Management/
Entities -->
                <xs:element name="cmName" type="xs:string" maxOccurs="1"
minOccurs="1"/>

                <!-- 'true' if already created extension is to be used. 'false' if
available extension is to be used. -->
                <xs:element name="useExistingExtension" type="xs:boolean"
maxOccurs="1" minOccurs="0"/>

                <!-- Station extension number that need to be assigned to the user. -->
                <xs:element name="extension" maxOccurs="1" minOccurs="1">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]+([.-][0-9]+)*/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Template name to be used to create station. Values defined in
Template will be used if not provided. -->
                <xs:element name="template" type="xs:string" maxOccurs="1"
minOccurs="0"/>

                <!-- Specifies the set type of the station -->
                <xs:element name="setType" type="xs:string" maxOccurs="1"
minOccurs="0"/>

                <!-- Security code for station. Value can be digit only. -->
                <xs:element name="securityCode" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]*/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Valid values for port -->
                <!--01 to 64 First and second numbers are the cabinet number -->
                <!--A to E Third character is the carrier -->
                <!--01 to 20 Fourth and fifth characters are the slot number -->

```

```

        <!--01 to 32 Sixth and seventh characters are the circuit number -->
        <!--x or X Indicates that there is no hardware associated with
the port assignment since the switch was set up, and the administrator expects that
the extension would have a non-IP set. Or, the extension had a non-IP set, and it
dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony
(CTI) stations, as well as for SBS Extensions. -->
        <!--IP Indicates that there is no hardware associated with the port
assignment since the switch was set up, and the administrator expects that the
extension would have an IP set. This is automatically entered for certain IP station
set types, but you can enter for a DCP set with softphone permissions. This changes
to the s00000 type when the set registers. -->
        <xs:element name="port" type="xs:string" maxOccurs="1"
minOccurs="0" />

        <!-- Whether the station should be deleted if it unassigned from the
user. -->
        <xs:element name="deleteOnUnassign" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

        <!-- true/false to enable/disable lock messages feature. -->
        <xs:element name="lockMessages" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

        <!-- A coverage path is a prioritized sequence of extensions to which
your voice system will route an unanswered call. -->
        <!-- Valid values: Path Number between 1-2000, time of day table,
t1-t999, or blank. -->
        <xs:element name="coveragePath1" maxOccurs="1" minOccurs="0">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:pattern value="(t[1-9][0-9]{0,2})|([1-9][0-9]{0,2}|
1[0-9]{3}|2000)"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- A coverage path is a prioritized sequence of extensions to which
your voice system will route an unanswered call. -->
        <!-- Valid values: Path Number between 1-2000, time of day table,
t1-t999, or blank. -->
        <xs:element name="coveragePath2" maxOccurs="1" minOccurs="0">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:pattern value="(t[1-9][0-9]{0,2})|([1-9][0-9]{0,2}|
1[0-9]{3}|2000)"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- The extension the system should hunt to for this telephone when
the telephone is busy. A station hunting chain can be created by assigning a hunt-
to station to a series of telephones. -->
        <xs:element name="huntToStation" type="xs:string" maxOccurs="1"
minOccurs="0" />

        <!-- Provides for partitioning of attendant groups and/or stations
and trunk groups. -->
        <!-- Typically this is used for multiple tenants in a building or
multiple departments within a company or organization. -->
        <!-- Valid values: 1 to 100 -->
        <xs:element name="tn" maxOccurs="1" minOccurs="0">
            <xs:simpleType>
                <xs:restriction base="xs:int">
                    <xs:minInclusive value="0" />
                    <xs:maxInclusive value="100" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

```

```

        </xs:restriction>
    </xs:simpleType>
</xs:element>

    <!-- Typically this is used for multiple tenants in a building or
multiple departments within a company or organization. -->
    <!-- Typically this is used for multiple tenants in a building or
multiple departments within a company or organization. -->
    <!-- Valid values: 0 to 995 -->
    <xs:element name="cor" maxOccurs="1" minOccurs="0">
        <xs:simpleType>
            <xs:restriction base="xs:int">
                <xs:minInclusive value="0"/>
                <xs:maxInclusive value="995"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <!-- Class of Service lets you define groups of users and control
those groups' access to features -->
    <!-- Valid values: 1 to 15 -->
    <xs:element name="cos" maxOccurs="1" minOccurs="0">
        <xs:simpleType>
            <xs:restriction base="xs:int">
                <xs:minInclusive value="0" />
                <xs:maxInclusive value="15" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="tests" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

    <xs:element name="dataModule" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

    <!-- Controls the behavior of speakerphones. -->
    <xs:element name="speakerphone" maxOccurs="1" minOccurs="0">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="none"/>
                <xs:enumeration value="1-way"/>
                <xs:enumeration value="2-way"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <!-- The language that displays on stations -->
    <!-- Time of day is displayed in 24-hour format (00:00 - 23:59)
for all languages except English, which is displayed in 12-hour format (12:00 a.m.
to 11:59 p.m.). -->
    <!-- unicode: Displays English messages in a 24-hour format . If no
Unicode file is installed, displays messages in English by default. -->
    <xs:element name="displayLanguage" maxOccurs="1" minOccurs="0">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="english"/>
                <xs:enumeration value="french"/>
                <xs:enumeration value="italian"/>
                <xs:enumeration value="spanish"/>
                <xs:enumeration value="unicode"/>
                <xs:enumeration value="user-defined"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

```

```

        </xs:element>

        <!-- Defines the personalized ringing pattern for the station.
        Personalized Ringing allows users of some telephones to have
one of 8 ringing patterns for incoming calls.
        For virtual stations, this field dictates the ringing pattern
on its mapped-to physical telephone.
        -->
        <!-- L = 530 Hz, M = 750 Hz, and H = 1060 Hz -->
        <!-- Valid Entries Usage
            1 MMM (standard ringing)
            2 HHH
            3 LLL
            4 LHH
            5 HHL
            6 HLL
            7 HLH
            8 LHL
        -->
        <xs:element name="personalizedRingingPattern" maxOccurs="1"
minOccurs="0">
            <xs:simpleType>
                <xs:restriction base="xs:int">
                    <xs:minInclusive value="0" />
                    <xs:maxInclusive value="8" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- The Message Lamp Extension associated with the current extension
-->
        <xs:element name="messageLampExt" maxOccurs="1" minOccurs="0">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:pattern value="[0-9]+([.-][0-9]+)*/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Enables or disables the mute button on the station. -->
        <xs:element name="muteButtonEnabled" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

        <!--
is
        When used with Multi-media Call Handling, indicates which extension
dial
        assigned to the data module of the multimedia complex. Users can
        this extension to place either a voice or a data call, and voice
made to
        conversion, coverage, and forwarding apply as if the call were
        the 1-number.
        -->
        <!--
        Valid Entry Usage A valid BRI data extension For MMCH, enter the
        extension of the data module that is part of this multimedia
complex.
        H.323 station extension For 4600 series IP Telephones, enter the
        corresponding
        H.323 station. For IP Softphone, enter the
        Agent
        H.323 station. If you enter a value in this field, you can register
        this station for either a road-warrior or telecommuter/Avaya IP
        application. blank Leave this field blank for single-connect IP
    
```

```

        applications.
-->
<xs:element name="mediaComplexExt" maxOccurs="1" minOccurs="0" >
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:pattern value="[0-9]+([.-][0-9]+)*/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<!-- Whether this is IP soft phone. -->
<xs:element name="ipSoftphone" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!--
  Survivable GK Node Name Identifies the existence of other H.323
  gatekeepers located within gateway products that offer survivable
call
  features. For example, the MultiTech MVPxxx-AV H.323 gateway family
  and the SLS function within the H.248 gateways. When a valid IP node
  name is entered into this field, Communication Manager adds the IP
  address of this gateway to the bottom of the Alternate Gatekeeper
List
  for this IP network region. As H.323 IP stations register with
  Communication Manager, this list is sent down in the registration
  confirm message. This allows the IP station to use the IP address of
  this Survivable Gatekeeper as the call controller of last resort to
  register with. Available only if the station type is an H.323
station
  (46xxor 96xx models).
  Valid Entry      Usage
  Valid IP node name      Any valid previously-administered
IP node name.
  blank      There are no external gatekeeper
nodes within a customer's network. This is the default value.
-->
<xs:element name="survivableGkNodeName" type="xs:string"
maxOccurs="1" minOccurs="0" />

<!--
  Sets a level of restriction for stations to be used with the
  survivable dial plan to limit certain users to only to certain types
  of calls. You can list the restriction levels in order from the most
  restrictive to least restrictive. Each level assumes the calling
  ability of the ones above it. This field is used by PIM module
of the
  Integrated Management to communicate with the Communication Manager
  administration tables and obtain the class of service information.
PIM
  module builds a managed database to send for Standard Local
  Survivability (SLS) on the H.248 gateways. Available for all analog
  and IP station types.
  Valid Entries      Usage
  emergency      This station can only be used to place
emergency calls.
  internal      This station can only make intra-switch
calls. This is the default.
  local      This station can only make calls that are
defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's
routing tables.
  toll      This station can place any national toll
calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's
routing tables.
  unrestricted      This station can place a call to any number

```

## Managing Users

defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users.

```
-->
<xs:element name="survivableCOR" maxOccurs="1" minOccurs="0">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="emergency"/>
      <xs:enumeration value="internal"/>
      <xs:enumeration value="local"/>
      <xs:enumeration value="toll"/>
      <xs:enumeration value="unrestricted"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<!--
incoming
successfully
obtain
database
IP
Valid Entry      Usage
      true      Allows this station to be an incoming trunk
destination while the Media Gateway is running in survivability mode. This is the
default.
      false      Prevents this station from receiving
incoming trunk calls when in survivable mode.
-->
<xs:element name="survivableTrunkDest" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

<!-- Enter the complete Voice Mail Dial Up number. -->
<xs:element name="voiceMailNumber" maxOccurs="1" minOccurs="0" >
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:pattern value="[0-9]{0,23}[0-9]||[*]||[#]||~p|~w|~W|~m|
~s"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<!-- Analog telephones only. -->
<!--
Valid entries      Usage
      true      Enter true if this telephone is not located
in the same building with the system. If you enter true, you must complete R Balance
Network.
      false      Enter false if the telephone is located in
the same building with the system.
-->
<xs:element name="offPremisesStation" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!-- If a second line on the telephone is administered on the I-2
channel, enter analog. Otherwise, enter data module if applicable or none. -->
```

```

    <xs:element name="dataOption" maxOccurs="1" minOccurs="0">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="analog"/>
          <xs:enumeration value="data-module"/>
          <xs:enumeration value="none"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>

    <xs:element name="displayModule" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

    <!-- if led or neon then messageLampExt should be enable otherwise
its blank -->
    <xs:element name="messageWaitingIndicator" maxOccurs="1"
minOccurs="0" >
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="led"/>
          <xs:enumeration value="neon"/>
          <xs:enumeration value="none"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>

    <!-- Enter true to use this station as an endpoint in a remote office
configuration. -->
    <xs:element name="remoteOfficePhone" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

    <!-- Defines the source for Leave Word Calling (LWC) messages. -->
    <!--
Valid entries          Usage
    audix                If LWC is attempted, the messages are
stored in AUDIX.
    spe                  If LWC is attempted, the messages are stored in
the system processing element (spe).
    none                 If LWC is attempted, the messages are not stored.

-->
    <xs:element name="lwcReception" maxOccurs="1" minOccurs="0">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="audix"/>
          <xs:enumeration value="msa"/>
          <xs:enumeration value="spe"/>
          <xs:enumeration value="none"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>

    <!--
messages
    Enter true to allow internal telephone users to leave short LWC

    for this extension. If the system has hospitality, enter true for
    guest-room telephones if the extension designated to receive failed
    wakeup messages should receive LWC messages that indicate the wakeup
    calls failed. Enter true if LWC Reception is audix.
-->
    <xs:element name="lwcActivation" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

    <xs:element name="lwcLogExternalCalls" type="xs:boolean"

```

## Managing Users

```
maxOccurs="1" minOccurs="0" />
  <xs:element name="cdrPrivacy" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
  <xs:element name="redirectNotification" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
  <xs:element name="perButtonRingControl" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
  <xs:element name="bridgedCallAlerting" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
  <xs:element name="bridgedIdleLinePreference" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
  <xs:element name="confTransOnPrimaryAppearance" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
  <xs:element name="customizableLabels" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
  <xs:element name="expansionModule" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
  <xs:element name="ipVideoSoftphone" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

  <xs:element name="activeStationRinging" maxOccurs="1" minOccurs="0">
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:enumeration value="single"/>
        <xs:enumeration value="continuous"/>
        <xs:enumeration value="if-busy-single"/>
        <xs:enumeration value="silent"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>

  <!-- Defines how call rings to the telephone when it is on-hook. -->
  <!--
    Valid entries          Usage
    continuous            Enter continuous to cause all calls
to this telephone to ring continuously.
    if-busy-single        Enter if-busy-single to cause calls
to this telephone to ring continuously when the telephone is off-hook and idle and
calls to this telephone to
                                receive one ring cycle and then ring
silently when the telephone is off-hook and active.
    silent-if-busy        Enter silent-if-busy to cause calls
to ring silently when this station is busy.
    single                Enter single to cause calls to this
telephone to receive one ring cycle and then ring silently.
  -->
  <xs:element name="idleActiveRinging" type="xs:string" maxOccurs="1"
minOccurs="0" /> <!-- not found in xhtml -->

  <!-- Must be set to true when the Type field is set to H.323. -->
  <xs:element name="switchhookFlash" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

  <!-- If this field is true, the short switch-hook flash (50 to
150) from a 2500-type set is ignored. -->
  <xs:element name="ignoreRotaryDigits" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

  <!--
    H.320 Conversion "â€" Valid entries are true and false (default).
This field is
                                optional for non-multimedia complex voice stations and for Basic
multimedia complex voice stations. It is mandatory for Enhanced
multimedia complex voice stations. Because the system can only
handle
```

```

        a limited number of conversion calls, you might need to limit the
        number of telephones with H.320 conversion. Enhanced multimedia
        complexes must have this flag set to true.
-->
        <xs:element name="h320Conversion" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
<!--
    The service link is the combined hardware and software multimedia
    connection between an Enhanced mode complex's H.320 DVC
system and the
    Avaya DEFINITY Server which terminates the H.320 protocol. A service
    link is never used by a Basic mode complex H.320 DVC system.
service
    Connecting a service link will take several seconds. When the
link is connected, it uses MMI, VC and system timeslot resources.
When
    the service link is disconnected it does not tie up any resources.
    The
    Service Link Mode can be administered as either "as-needed" or
    "permanent" as described below: - As-Needed - Most non-
call center
    multimedia users will be administered with this service link
mode. The
    as-needed mode provides the Enhanced multimedia complex with a
    connected service link whenever a multimedia call is answered by the
call
    station and for a period of 10 seconds after the last multimedia
call
    on the station has been disconnected. Having the service link stay
    connected for 10 seconds allows a user to disconnect a multimedia
Multimedia
    and then make another multimedia call without having to wait for the
    service link to disconnect and re-establish. - Permanent -
    call center agents and other users who are constantly making or
    receiving multimedia calls might want to be administered with this
    service link mode. The permanent mode service link will be connected
    during the station's first multimedia call and will remain in a
    connected state until the user disconnects from their PC's
multimedia
    application or the Avaya DEFINITY Server restarts. This provides a
    multimedia user with a much quicker video cut-through when
answering a
    multimedia call from another permanent mode station or a multimedia
    call that has been early answered. - Multimedia Mode - There
are two
    multimedia modes, Basic and Enhanced, as
-->
<xs:element name="serviceLinkMode" maxOccurs="1" minOccurs="0" >
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="as-needed"/>
      <xs:enumeration value="permanent"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<!--
    There are two multimedia modes, Basic and Enhanced, as described
    below:
    Basic - A Basic multimedia complex consists of a
    BRI-connected multimedia-equipped PC and a non-BRI-connected
    multifunction telephone set. When in Basic mode, users place voice
    calls at the multifunction telephone and multimedia calls from the
    multimedia equipped PC. Voice calls will be answered at the

```

```

multifunction telephone and multimedia calls will alert first at the
PC and if unanswered will next alert at the voice station if it is
administered with H.320 enabled. A Basic mode complex has limited
multimedia feature capability.
Enhanced - An Enhanced multimedia complex consists of a
BRI-connected multimedia-equipped PC and a non-BRI-connected
multifunction telephone. The Enhanced mode station acts as though
the
PC were directly connected to the multifunction telephone; the
service
link provides the actual connection between the Avaya DEFINITY
Server
and the PC. Thus, voice and multimedia calls are originated and
received at the telephone set. Voice and multimedia call status are
also displayed at the telephone set. An Enhanced mode station allows
multimedia calls to take full advantage of most call control
features
-->
<xs:element name="multimediaMode" maxOccurs="1" minOccurs="0" >
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="basic"/>
      <xs:enumeration value="enhanced"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<!-- Controls the auditing or interrogation of a served user's
message waiting indicator (MWI).
Valid entries          Usage
fp-mwi                 Use if the station is a served user of
an fp-mwi message center.
qsig-mwi               Use if the station is a served user of a
qsig-mwi message center.
blank                  Leave blank if you do not want to audit
the served user's MWI or
an fp-mwi or qsig-mwi message center.
if the user is not a served user of either
-->
<xs:element name="mwiServedUserType" maxOccurs="1" minOccurs="0" >
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="fp-mwi"/>
      <xs:enumeration value="qsig-mwi"/>
      <xs:enumeration value="sip-adjunct"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<!-- The AUDIX associated with the station.
Must contain a user-defined adjunct name that was previously
administered.
-->
  <xs:element name="audixName" type="xs:string" maxOccurs="1"
minOccurs="0" />

<!--
Automatic Moves allows a DCP telephone to be unplugged from one
location and moved to a new location without additional
Communication
Manager administration. Communication Manager automatically
associates
the extension to the new port.

*****CAUTION*****

```



## Managing Users

| for                                | service when dialing from remote locations that do not have local trunks. Do not use an Avaya IP endpoint to dial emergency numbers  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
|------------------------------------|--|---------------|-------|-------------|---------------------------------|--|---------------------------------------|------------------------|--------------------------------------|-------------------------------|--------------------------------------|-----------------------|------------------------------------|--------------------|---------------------------------------|----------------------|-------------------------|-----------------------------|---------------------------------------|-----------------------------|-------------------------------------|-----------------------------|---------------------------------------|------------------------|---------------------------------------|--------------------|--|---------|--|-----------------------------|---------------------------------------|------------------------|--|--------------------|--|-----------------------------|-------------------------------------|--|-------------------------|--|---------------------------------------|-------|--------------------------------------|------------------------------------|---------------------------------------|-----------------------------------|--------------------------------------|----------------------------------|--|-----------------------------|--|--------------------------|--|--------------------------------|--------------------|--|------------------------------------|-------|--|
| product                            | emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| only if                            | indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations. Please contact your Avaya representative if you have questions about emergency calls from IP telephones. Available   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
|                                    | the station is an IP Softphone or a remote office station.   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| following results:                 | <table><thead><tr><th>Valid entries</th><th>Usage</th></tr></thead><tbody><tr><td>as-on-local</td><td>Type as-on-local to achieve the</td></tr><tr><td></td><td>If the administrator chooses to leave</td></tr><tr><td>the Emergency Location</td><td>Extension fields (that correspond to</td></tr><tr><td>this station's IP address) on</td><td>the IP Address Mapping screen blank,</td></tr><tr><td>the value as-on-local</td><td>sends the extension entered in the</td></tr><tr><td>Emergency Location</td><td>Extension field in the Station screen</td></tr><tr><td>to the Public Safety</td><td>Answering Point (PSAP).</td></tr><tr><td>Address Mapping screen with</td><td>If the administrator populates the IP</td></tr><tr><td>local functions as follows:</td><td>emergency numbers, the value as-on-</td></tr><tr><td>field in the Station screen</td><td>- If the Emergency Location Extension</td></tr><tr><td>Extension field in the</td><td>is the same as the Emergency Location</td></tr><tr><td>on-local sends the</td><td>IP Address Mapping screen, the value as-</td></tr><tr><td>(PSAP).</td><td>extension to the Public Safety Answering Point</td></tr><tr><td>field in the Station screen</td><td>- If the Emergency Location Extension</td></tr><tr><td>Extension field in the</td><td>is different from the Emergency Location</td></tr><tr><td>on-local sends the</td><td>IP Address Mapping screen, the value as-</td></tr><tr><td>screen to the Public Safety</td><td>extension in the IP Address Mapping</td></tr><tr><td></td><td>Answering Point (PSAP).</td></tr><tr><td></td><td>Enter block to prevent the completion</td></tr><tr><td>block</td><td>for users who move around but always</td></tr><tr><td>of emergency calls. Use this entry</td><td>nearby, and for users who are farther</td></tr><tr><td>have a circuit-switched telephone</td><td>than an adjacent area code served by</td></tr><tr><td>away from the Avaya S8XXX Server</td><td></td></tr><tr><td>the same 911 Tandem office.</td><td>When users attempt to dial an emergency call</td></tr><tr><td>from an IP Telephone and</td><td>the call is blocked, they can dial 911</td></tr><tr><td>from a nearby circuit-switched</td><td>telephone instead.</td></tr><tr><td></td><td>Enter cesid to allow Communication</td></tr><tr><td>cesid</td><td></td></tr></tbody></table> | Valid entries | Usage | as-on-local | Type as-on-local to achieve the |  | If the administrator chooses to leave | the Emergency Location | Extension fields (that correspond to | this station's IP address) on | the IP Address Mapping screen blank, | the value as-on-local | sends the extension entered in the | Emergency Location | Extension field in the Station screen | to the Public Safety | Answering Point (PSAP). | Address Mapping screen with | If the administrator populates the IP | local functions as follows: | emergency numbers, the value as-on- | field in the Station screen | - If the Emergency Location Extension | Extension field in the | is the same as the Emergency Location | on-local sends the | IP Address Mapping screen, the value as- | (PSAP). | extension to the Public Safety Answering Point | field in the Station screen | - If the Emergency Location Extension | Extension field in the | is different from the Emergency Location | on-local sends the | IP Address Mapping screen, the value as- | screen to the Public Safety | extension in the IP Address Mapping |  | Answering Point (PSAP). |  | Enter block to prevent the completion | block | for users who move around but always | of emergency calls. Use this entry | nearby, and for users who are farther | have a circuit-switched telephone | than an adjacent area code served by | away from the Avaya S8XXX Server |  | the same 911 Tandem office. | When users attempt to dial an emergency call | from an IP Telephone and | the call is blocked, they can dial 911 | from a nearby circuit-switched | telephone instead. |  | Enter cesid to allow Communication | cesid |  |
| Valid entries                      | Usage  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| as-on-local                        | Type as-on-local to achieve the  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
|                                    | If the administrator chooses to leave  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| the Emergency Location             | Extension fields (that correspond to   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| this station's IP address) on      | the IP Address Mapping screen blank,   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| the value as-on-local              | sends the extension entered in the   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| Emergency Location                 | Extension field in the Station screen  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| to the Public Safety               | Answering Point (PSAP).  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| Address Mapping screen with        | If the administrator populates the IP  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| local functions as follows:        | emergency numbers, the value as-on-  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| field in the Station screen        | - If the Emergency Location Extension  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| Extension field in the             | is the same as the Emergency Location  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| on-local sends the                 | IP Address Mapping screen, the value as-   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| (PSAP).                            | extension to the Public Safety Answering Point   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| field in the Station screen        | - If the Emergency Location Extension  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| Extension field in the             | is different from the Emergency Location   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| on-local sends the                 | IP Address Mapping screen, the value as-   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| screen to the Public Safety        | extension in the IP Address Mapping  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
|                                    | Answering Point (PSAP).  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
|                                    | Enter block to prevent the completion  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| block                              | for users who move around but always   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| of emergency calls. Use this entry | nearby, and for users who are farther  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| have a circuit-switched telephone  | than an adjacent area code served by   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| away from the Avaya S8XXX Server   |  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| the same 911 Tandem office.        | When users attempt to dial an emergency call   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| from an IP Telephone and           | the call is blocked, they can dial 911   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| from a nearby circuit-switched     | telephone instead.   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
|                                    | Enter cesid to allow Communication   |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |
| cesid                              |  |               |       |             |                                 |  |                                       |                        |                                      |                               |                                      |                       |                                    |                    |                                       |                      |                         |                             |                                       |                             |                                     |                             |                                       |                        |                                       |                    |  |         |  |                             |                                       |                        |  |                    |  |                             |                                     |  |                         |  |                                       |       |                                      |                                    |                                       |                                   |                                      |                                  |  |                             |  |                          |  |                                |                    |  |                                    |       |  |

Manager to send the CESID information supplied by the IP Softphone to the PSAP. The end user enters the emergency information into the IP Softphone. Use this entry for IP Softphones with road warrior service that are near enough to the Avaya S8XXX Server that an emergency call routed over the itâ€™s trunk reaches the PSAP that covers the server or switch. If the server uses ISDN trunks for emergency calls, the digit string is the telephone number, provided that the number is a local direct-dial number with the local area code, at the physical location of the IP Softphone. If the server uses CAMA trunks for emergency calls, the end user enters a specific digit string for each IP Softphone location, based on advice from the local emergency response personnel.

option Enter option to allow the user to select the option (extension, block, or cesid) that the user selected during registration and the IP Softphone reported. Use this entry for extensions that can be swapped back and forth between IP Softphones and a telephone with a fixed location. The user chooses between block and cesid on the softphone. A DCP or IP telephone in the office automatically selects extension.

```

-->
<xs:element name="remoteSoftphoneEmergencyCalls" maxOccurs="1"
minOccurs="0" >
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="as-on-local"/>
      <xs:enumeration value="block"/>
      <xs:enumeration value="cesid"/>
      <xs:enumeration value="option"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<!--
  This field allows the system to properly identify the location of a
  caller who dials a 911 emergency call from this station. An entry in
  this field must be of an extension type included in the dial
  plan, but
  does not have to be an extension on the local system. It can be a UDP
  extension. The entry defaults to blank. A blank entry typically
  would
  be used for an IP softphone dialing in through PPP from somewhere
  outside your network. If you populate the IP Address Mapping screen
  with emergency numbers, the feature functions as follows: If the
  Emergency Location Extension field in the Station screen is the same
  as the Emergency Location Extension field in the IP Address Mapping
  screen, the feature sends the extension to the Public Safety
  Answering
  Point (PSAP). If the Emergency Location Extension field in the

```

## Managing Users

```
Station
the
    screen is different from the Emergency Location Extension field in
    IP Address Mapping screen, the feature sends the extension in the IP
    Address Mapping screen to the Public Safety Answering Point (PSAP).
-->
<xs:element name="emergencyLocationExt" maxOccurs="1" minOccurs="0" >
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:pattern value="[0-9]+([\.-][0-9]+)*/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<!--
  A softphone can register no matter what emergency call handling
settings
  the user has entered into the softphone. If a softphone dials
911, the
  administered Emergency Location Extension is used. The softphone's
  user-entered settings are ignored. If an IP telephone dials 911, the
  administered Emergency Location Extension is used. If a call center
  agent dials 911, the physical station extension is displayed,
  overriding the administered LoginID for ISDN Display . Does not
apply
  to SCCAN wireless telephones, or to extensions administered as type
  h.323.
-->
<xs:element name="alwaysUse" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!-- Activates or deactivates Precedence Call Waiting for this station
-->
  <xs:element name="precedenceCallWaiting" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

  <!--
  Enables or disables automatic selection of any idle appearance for
  transferred or conferenced calls. Communication Manager first
attempts
  to find an idle appearance that has the same extension number as the
  call being transferred or conferenced has. If that attempt fails,
  Communication Manager selects the first idle appearance.
-->
  <xs:element name="autoSelectAnyIdleAppearance"
type="xs:boolean" maxOccurs="1" minOccurs="0" />

  <!--
  Allows or denies users in the telephone's Coverage Path to
retrieve
  Leave Word Calling (LWC) messages for this telephone. Applies
only if
  the telephone is enabled for LWC Reception.
-->
  <xs:element name="coverageMsgRetrieval" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

  <!--
  In EAS environments, the auto answer setting for the Agent LoginID
can
  override a station's setting when an agent logs in.
  Valid Entry Usage
  all All ACD and non-ACD calls terminated to an
idle station cut through immediately.
  Does not allow automatic hands-free answer
```

```

for intercom calls. With non-ACD calls,
the set is also rung while the call is cut
through. The ring can be prevented by activating
the ringer-off feature button when the Allow
Ringer-off with Auto-Answer is enabled for the system.
acd Only ACD split /skill calls and direct
agent calls to auto answer. Non-ACD calls terminated to a station ring audibly.
hook and idle, only the ACD split/skill calls and direct agent calls
For analog stations, the station is off-
auto answer; non-ACD calls receive busy
treatment. If the station is active on an ACD call and
a non-ACD call arrives, the Agent receives
call-waiting tone.
none All calls terminated to this station
receive an audible ringing treatment.
icom Allows a telephone user to answer an intercom
call from the same intercom group without pressing the intercom
button.
-->
<xs:element name="autoAnswer" maxOccurs="1" minOccurs="0" >
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="acd"/>
      <xs:enumeration value="all"/>
      <xs:enumeration value="icom"/>
      <xs:enumeration value="none"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<!--
  Enables or disables data restriction that is used to prevent
tones, such as call-waiting tones, from interrupting data calls.
  Data restriction provides permanent protection and cannot be
changed by the telephone user. Cannot be assigned if Auto Answer
is administered as all or acd. If enabled, whisper page to this
station is denied.
-->
<xs:element name="dataRestriction" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!--
  Indicates which call appearance is selected when the user lifts the
handset and there is an incoming call.
  Valid Entry Usage
  true The user connects to an idle call
appearance instead of the ringing call.
  false The Alerting Appearance Preference is set
and the user connects to the ringing call appearance.
-->
<xs:element name="idleAppearancePreference" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

<!--
  enable/disable call waiting for this station
-->
<xs:element name="callWaitingIndication" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

<!--
  Attendant call waiting allows attendant-originated or attendant-
extended calls to a busy
  single-line telephone to wait and sends distinctive call-
waiting tone to the single-line user.
  Enable/disable attendant call waiting

```

## Managing Users

```

-->
  <xs:element name="attCallWaitingIndication" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
  <!--
    Enter true so the telephone can receive the 3 different types
of ringing patterns which identify the type of incoming calls.
    Distinctive ringing might not work properly for off-premises
telephones. -->
  <xs:element name="distinctiveAudibleAlert" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
  <!--
    Valid Entries          Usage
    true                  Restricts the last idle call appearance used
for incoming priority calls and outgoing call originations only.
    false                 Last idle call appearance is used for
incoming priority calls and outgoing call originations.
-->
  <xs:element name="restrictLastAppearance" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
  <!--
    Valid entries          Usage
    true                  Analog disconnect signal is sent
automatically to the port after a call terminates. Analog devices
(such as answering machines and
speakerphones) use this signal to turn the devices off after a call terminates.
    false                 Hunt group agents are alerted to incoming
calls. In a hunt group environment, the disconnect
signal blocks the reception of zip
tone and incoming call notification by an auto-answer station when a call
is queued for the station.
-->
  <xs:element name="adjunctSupervision" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
  <!--
    Send Calling Number.
    Valid Entries          Usage
    y                      All outgoing calls from the station
will deliver the Calling Party Number
(CPN) information as "Presentation Allowed."
    n                      No CPN information is sent for the call
    r                      Outgoing non-DCS network calls from the
station will deliver the Calling
Party Number information as "Presentation
Restricted."
-->
  <xs:element name="perStationCpnSendCallingNumber" maxOccurs="1"
minOccurs="0" >
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:enumeration value="r"/>
        <xs:enumeration value="n"/>
        <xs:enumeration value="y"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <!--
    Appears on the Station screen for analog telephones, only if the
Without Flash field in the
    ANALOG BUSY AUTO CALLBACK section of the Feature-Related System
Parameters

```

```

        screen is set to true. The Busy Auto Callback without Flash field
then defaults to true for all analog
        telephones that allow Analog Automatic Callback.
        Set true to provide automatic callback for a calling analog
station without flashing the hook.
-->
        <xs:element name="busyAutoCallbackWithoutFlash" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

        <!-- Provides audible message waiting. -->
        <xs:element name="audibleMessageWaiting" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

        <!--
        Only administrable if Hospitality is enabled on the System
Parameters
        Customer-Options (Optional Features) screen. This field affects the
Client
        telephone display on calls that originated from a station with
        Room Class of Service. Note: For stations with an audix station
        type, AUDIX Voice Power ports, or ports for any other type of
        messaging that needs display information, Display Client
Redirection
        must be enabled.
        Set true to redirect information for a call originating from a
Client Room and terminating to this station displays.
-->
        <xs:element name="displayClientRedirection" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

        <!--
        Valid Entries          Usage
        true                   Indicates that a station's line
selection is not to be moved from the currently selected line button
        to a different, non-alerting line button.
If you enter true, the line selection on an on-hook station only moves from the last
used line button to a line button with an
audibly alerting call. If there are no alerting calls, the line selection
remains on the button last used for a call.
        false                  The line selection on an on-hook station
with no alerting calls can be moved to a different line button, which might be
serving a different
        extension.
-->
        <xs:element name="selectLastUsedAppearance" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

        <!-- Whether an unanswered forwarded call is provided coverage
treatment. -->
        <xs:element name="coverageAfterForwarding" type="xs:string"
maxOccurs="1" minOccurs="0" />

        <!-- Allow/disallow direct audio connections between IP endpoints. -->
        <xs:element name="directIpIpAudioConnections" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

        <!-- Allows IP endpoints to be connected through the server's IP
circuit pack. -->
        <xs:element name="ipAudioHairpinning" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

        <xs:element name="primeAppearancePreference" type="xs:string"
maxOccurs="1" minOccurs="0" />

```

```

        <!-- Elements with complex data type. Please refer the appropriate
elements for more details. -->
        <xs:element name="stationSiteData" type="csm:xmlStationSiteData"
maxOccurs="1" minOccurs="0" />
        <xs:element name="abbrList"
type="csm:xmlStationAbbreviatedDialingData" maxOccurs="unbounded" minOccurs="0" />
        <xs:element name="buttons" type="csm:xmlButtonData" maxOccurs="24"
minOccurs="0" />
        <xs:element name="featureButtons" type="csm:xmlButtonData"
maxOccurs="24" minOccurs="0" />
        <xs:element name="expansionModuleButtons" type="csm:xmlButtonData"
maxOccurs="72" minOccurs="0" />
        <xs:element name="softKeys" type="csm:xmlButtonData" maxOccurs="15"
minOccurs="0" />
        <xs:element name="displayButtons" type="csm:xmlButtonData"
maxOccurs="unbounded" minOccurs="0" />
        <xs:element name="stationDataModule" type="csm:xmlStationDataModule"
maxOccurs="1" minOccurs="0" />
        <xs:element name="hotLineData" type="csm:xmlStationHotLineData"
maxOccurs="1" minOccurs="0" />
        <xs:element name="nativeName" type="csm:xmlNativeNameData"
maxOccurs="1" minOccurs="0"/>

        <!-- Number of button modules -->
        <xs:element name="buttonModules" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:int">
                <xs:minInclusive value="0" />
                <xs:maxInclusive value="3" />
            </xs:restriction>
        </xs:simpleType>
        </xs:element>

        <xs:element name="unconditionalInternalDest" maxOccurs="1"
minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}
[#]|[*][0-9]{1,17}|[0-9]{1,18}|[*][#]||"/>
            </xs:restriction>
        </xs:simpleType>
        </xs:element>

        <xs:element name="unconditionalInternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

        <xs:element name="unconditionalExternalDest" maxOccurs="1"
minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}
[#]|[*][0-9]{1,17}|[0-9]{1,18}|[*][#]||"/>
            </xs:restriction>
        </xs:simpleType>
        </xs:element>

        <xs:element name="unconditionalExternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

        <xs:element name="busyInternalDest" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">

```

```

        <xs:pattern value="[*][0-9]{1,16}{#}|[0123456789]{1,17}
[#]|[*][0-9]{1,17}|[0-9]{1,18}|[*][#]||"/>
        </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="busyInternalActive" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

        <xs:element name="busyExternalDest" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[*][0-9]{1,16}{#}|[0123456789]{1,17}
[#]|[*][0-9]{1,17}|[0-9]{1,18}|[*][#]||"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="busyExternalActive" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

        <xs:element name="noReplyInternalDest" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[*][0-9]{1,16}{#}|[0123456789]{1,17}
[#]|[*][0-9]{1,17}|[0-9]{1,18}|[*][#]||"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="noReplyInternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

        <xs:element name="noReplyExternalDest" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[*][0-9]{1,16}{#}|[0123456789]{1,17}
[#]|[*][0-9]{1,17}|[0-9]{1,18}|[*][#]||"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="noReplyExternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

        <xs:element name="sacCfOverride" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="a"/>
                <xs:enumeration value="n"/>
                <xs:enumeration value="y"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="lossGroup" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:int">
                <xs:minInclusive value="1" />
                <xs:maxInclusive value="19" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="timeOfDayLockTable" maxOccurs="1" minOccurs="0" >

```

```

        <xs:simpleType>
            <xs:restriction base="xs:int">
                <xs:minInclusive value="1" />
                <xs:maxInclusive value="5" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="emuLoginAllowed" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

    <xs:element name="ec500State" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="enabled"/>
                <xs:enumeration value="disabled"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="type3pccEnabled" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="None"/>
                <xs:enumeration value="Avaya"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="sipTrunk" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="aar|ars|[1-9]|[1-9][0-9]|[1-9]([0-9]
{2}|[1]([0-9]){3}|2000)/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="multimediaEarlyAnswer" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
    <xs:element name="bridgedApprOrigRestr" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

    <xs:element name="callApprDispFormat" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="inter-location"/>
                <xs:enumeration value="intra-location"/>
                <xs:enumeration value="disp-param-default"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="ipPhoneGroupId" maxOccurs="1" minOccurs="0">
        <xs:simpleType>
            <xs:restriction base="xs:int">
                <xs:minInclusive value="0" />
                <xs:maxInclusive value="999" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="xoipEndPointType" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">

```

```

        <xs:enumeration value="auto"/>
        <xs:enumeration value="fax"/>
        <xs:enumeration value="modem"/>
        <xs:enumeration value="tty"/>
    </xs:restriction>
</xs:simpleType>
</xs:element>

    <xs:element name="xid" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
    <xs:element name="stepClearing" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
    <xs:element name="fixedTei" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

    <xs:element name="tei" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[0-6][0-3]"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="countryProtocol" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="1"/>
                <xs:enumeration value="2"/>
                <xs:enumeration value="3"/>
                <xs:enumeration value="6"/>
                <xs:enumeration value="etsi"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="endptInit" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

    <xs:element name="spid" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[0-9]{1,10}"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

to 62 -->
    <xs:element name="endptId" maxOccurs="1" minOccurs="0" > <!-- 00
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[0-6][0-2]"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="isMCTSignalling" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
    <xs:element name="isShortCallingPartyDisplay" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
    <xs:element name="passageWay" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
    <xs:element name="dtmfOverIp" maxOccurs="1" minOccurs="0" >
        <xs:simpleType>
            <xs:restriction base="xs:string">

```

```

                <xs:enumeration value="in-band"/>
                <xs:enumeration value="in-band-g711"/>
                <xs:enumeration value="out-of-band"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="location" type="xs:string" maxOccurs="1"
minOccurs="0" />
    </xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>

<xs:complexType name="xmlStationSiteData">
    <xs:sequence>
        <xs:element name="room" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:maxLength value="10"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="jack" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:maxLength value="5"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="cable" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:maxLength value="5"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="floor" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="building" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="headset" type="xs:boolean" maxOccurs="1" minOccurs="0" />
        <xs:element name="speaker" type="xs:boolean" maxOccurs="1" minOccurs="0" />

        <xs:element name="mounting" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="d"/>
                    <xs:enumeration value="w"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="cordLength" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:int">
                    <xs:minInclusive value="0" />
                    <xs:maxInclusive value="99" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="setColor" type="xs:string" maxOccurs="1" minOccurs="0" />
    </xs:sequence>
</xs:complexType>

```

```

<xs:complexType name="xmlStationAbbreviatedDialingData">
  <xs:sequence>
    <xs:element name="listType" maxOccurs="1" minOccurs="1" >
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="enhanced"/>
          <xs:enumeration value="group"/>
          <xs:enumeration value="personal"/>
          <xs:enumeration value="system"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>

    <xs:element name="number" type="xs:int" maxOccurs="1" minOccurs="1" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlButtonData">
  <xs:sequence>
    <xs:element name="number" type="xs:int" maxOccurs="1" minOccurs="1" /
><!-- *****Must present***** -->
    <xs:element name="type" type="xs:string" maxOccurs="1" minOccurs="1" /
><!-- *****Must present***** -->
    <xs:element name="data1" type="xs:string" maxOccurs="1" minOccurs="0" />
    <xs:element name="data2" type="xs:string" maxOccurs="1" minOccurs="0" />
    <xs:element name="data3" type="xs:string" maxOccurs="1" minOccurs="0" />
    <xs:element name="data4" type="xs:string" maxOccurs="1" minOccurs="0" />
    <xs:element name="data5" type="xs:string" maxOccurs="1" minOccurs="0" />
    <xs:element name="data6" type="xs:string" maxOccurs="1" minOccurs="0" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlStationDataModule">
  <xs:sequence>
    <xs:element name="dataExtension" maxOccurs="1" minOccurs="1" ><!--
*****Must present***** -->
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:pattern value="[0-9]+([.-][0-9]+)*/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>

    <xs:element name="name" maxOccurs="1" minOccurs="0" >
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="29"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="cor" maxOccurs="1" minOccurs="1" ><!-- *****Must
present***** -->
      <xs:simpleType>
        <xs:restriction base="xs:int">
          <xs:minInclusive value="0" />
          <xs:maxInclusive value="995" />
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="cos" maxOccurs="1" minOccurs="1" ><!-- *****Must
present***** -->
      <xs:simpleType>
        <xs:restriction base="xs:int">
          <xs:minInclusive value="0" />

```

```

        <xs:maxInclusive value="15" />
    </xs:restriction>
</xs:simpleType>
</xs:element>

    <xs:element name="itc" maxOccurs="1" minOccurs="1" ><!-- *****Must
present***** -->
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="restricted"/>
                <xs:enumeration value="unrestricted"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="tn" maxOccurs="1" minOccurs="1" ><!-- *****Must
present***** -->
        <xs:simpleType>
            <xs:restriction base="xs:int">
                <xs:minInclusive value="0" />
                <xs:maxInclusive value="100" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
<xs:element name="listType" maxOccurs="1" minOccurs="0" >
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="enhanced"/>
            <xs:enumeration value="group"/>
            <xs:enumeration value="personal"/>
            <xs:enumeration value="system"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<xs:element name="listId" type="xs:int" maxOccurs="1" minOccurs="0" />

<xs:element name="specialDialingOption" maxOccurs="1" minOccurs="0" >
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="default"/>
            <xs:enumeration value="hot-line"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>
<xs:element name="specialDialingAbbrDialCode" maxOccurs="1" minOccurs="0" >
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:maxLength value="4"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>
</xs:sequence>
</xs:complexType>
<xs:complexType name="xmlStationHotLineData">
    <xs:sequence>
        <xs:element name="hotLineDestAbbrevList" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:int">
                    <xs:minInclusive value="1" />
                    <xs:maxInclusive value="3" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="hotLineAbbrevDialCode" maxOccurs="1" minOccurs="0" >

```

```

        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[0-9]*"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
</xs:sequence>
</xs:complexType>

<xs:complexType name="xmlNativeNameData">
    <xs:sequence>
        <xs:element name="locale" type="xs:string" maxOccurs="1" minOccurs="1" />
        <xs:element name="name" maxOccurs="1" minOccurs="1" >
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:maxLength value="27"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:sequence>
</xs:complexType>

</xs:schema>

```

### Sample XML for bulk importing endpoint profiles

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
  <tns:user>
    <authenticationType>BASIC</authenticationType>
    <description>description</description>
    <displayName>displayname</displayName>
    <displayNameAscii>displayNameAscii</displayNameAscii>
    <dn>dn</dn>
    <isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
    <isEnabled>true</isEnabled>
    <isVirtualUser>false</isVirtualUser>
    <givenName>givenName00</givenName>
    <honorific>honorific</honorific>
    <loginName>user00_00xyz@avaya.com</loginName>
    <middleName>middleName</middleName>
    <managerName>managerName</managerName>
    <preferredGivenName>preferredGivenName</preferredGivenName>
    <preferredLanguage>preferredLanguage</preferredLanguage>
    <source>local</source>
    <sourceUserKey>sourceUserKey</sourceUserKey>
    <status>AUTHPENDING</status>
    <suffix>suffix</suffix>
    <surname>surname</surname>
    <timeZone>timeZone</timeZone>
    <title>title</title>
    <userName>userName00</userName>
    <userPassword>userPassword</userPassword>
    <commPassword>commPassword</commPassword>
    <userType>ADMINISTRATOR</userType>
    <commProfileSet>
      <commProfileSetName>
        commProfileSetName00
      </commProfileSetName>
      <isPrimary>true</isPrimary>
    </commProfileSet>
    <commProfileList>
      <commProfile xsi:type="ipt:xmlStationProfile"
        xmlns:ipt="http://xml.avaya.com/schema/import_csm_cm">

```

```

<commProfileType>CM</commProfileType>
<ipt:cmName>PUIM81</ipt:cmName>
<ipt:useExistingExtension>
  false
</ipt:useExistingExtension>
<ipt:extension>7100000</ipt:extension>
<ipt:template>DEFAULT_4620_CM_6_0</ipt:template>
<ipt:setType>4620</ipt:setType>
<ipt:securityCode>78974231</ipt:securityCode>
<ipt:port>IP</ipt:port>
<ipt:coveragePath1>1</ipt:coveragePath1>
<ipt:tn>1</ipt:tn>
<ipt:cor>10</ipt:cor>
<ipt:cos>4</ipt:cos>
<ipt:dataModule>>false</ipt:dataModule>
<ipt:speakerphone>1-way</ipt:speakerphone>
<ipt:displayLanguage>english</ipt:displayLanguage>
<ipt:ipSoftphone>>false</ipt:ipSoftphone>
<ipt:survivableCOR>internal</ipt:survivableCOR>
<ipt:survivableTrunkDest>
  true
</ipt:survivableTrunkDest>
<ipt:offPremisesStation>
  false
</ipt:offPremisesStation>
<ipt:dataOption>none</ipt:dataOption>
<ipt:displayModule>>false</ipt:displayModule>
<ipt:lwcReception>spe</ipt:lwcReception>
<ipt:lwcActivation>>true</ipt:lwcActivation>
<ipt:lwcLogExternalCalls>
  false
</ipt:lwcLogExternalCalls>
<ipt:cdrPrivacy>>false</ipt:cdrPrivacy>
<ipt:redirectNotification>
  true
</ipt:redirectNotification>
<ipt:perButtonRingControl>
  false
</ipt:perButtonRingControl>
<ipt:bridgedCallAlerting>
  false
</ipt:bridgedCallAlerting>
<ipt:bridgedIdleLinePreference>
  false
</ipt:bridgedIdleLinePreference>
<!-- <ipt:confTransOnPrimaryAppearance></
ipt:confTransOnPrimaryAppearance>
  <ipt:customizableLabels></ipt:customizableLabels> -->
<ipt:expansionModule>>true</ipt:expansionModule>
<ipt:ipVideoSoftphone>>false</ipt:ipVideoSoftphone>
<ipt:activeStationRinging>
  single
</ipt:activeStationRinging>
<!-- <ipt:idleActiveRinging></ipt:idleActiveRinging>
  <ipt:switchhookFlash></ipt:switchhookFlash>
  <ipt:ignoreRotaryDigits></ipt:ignoreRotaryDigits>-->
<ipt:h320Conversion>>false</ipt:h320Conversion>
<ipt:serviceLinkMode>as-needed</ipt:serviceLinkMode>
<ipt:multimediaMode>enhanced</ipt:multimediaMode>
<!-- <ipt:mwiServedUserType></ipt:mwiServedUserType> -->
<!-- <ipt:audixName></ipt:audixName> -->
<!-- <ipt:automaticMoves></ipt:automaticMoves> -->
<ipt:remoteSoftphoneEmergencyCalls>
  as-on-local
</ipt:remoteSoftphoneEmergencyCalls>

```

```

        <!-- <ipt:alwaysUse></ipt:alwaysUse> -->
        <ipt:precedenceCallWaiting>
            false
        </ipt:precedenceCallWaiting>
        <ipt:autoSelectAnyIdleAppearance>
            false
        </ipt:autoSelectAnyIdleAppearance>
        <ipt:coverageMsgRetrieval>
            true
        </ipt:coverageMsgRetrieval>
        <ipt:autoAnswer>none</ipt:autoAnswer>
        <ipt:dataRestriction>>false</ipt:dataRestriction>
        <ipt:idleAppearancePreference>
            false
        </ipt:idleAppearancePreference>
        <!-- <ipt:attCallWaitingIndication></
ipt:attCallWaitingIndication> -->
        <!-- <ipt:distinctiveAudibleAlert></
ipt:distinctiveAudibleAlert> -->
        <ipt:restrictLastAppearance>
            true
        </ipt:restrictLastAppearance>
        <!-- <ipt:adjunctSupervision></ipt:adjunctSupervision> -->
        <!-- <ipt:perStationCpnSendCallingNumber></
ipt:perStationCpnSendCallingNumber> -->
        <!-- <ipt:busyAutoCallbackWithoutFlash></
ipt:busyAutoCallbackWithoutFlash> -->
        <ipt:audibleMessageWaiting>
            false
        </ipt:audibleMessageWaiting>
        <ipt:displayClientRedirection>
            false
        </ipt:displayClientRedirection>
        <ipt:selectLastUsedAppearance>
            false
        </ipt:selectLastUsedAppearance>
        <ipt:coverageAfterForwarding>
            system
        </ipt:coverageAfterForwarding>
        <ipt:directIpIpAudioConnections>
            true
        </ipt:directIpIpAudioConnections>
        <ipt:ipAudioHairpinning>
            false
        </ipt:ipAudioHairpinning>
        <!-- <ipt:primeAppearancePreference></
ipt:primeAppearancePreference> -->
        </commProfile>
    </commProfileList>
</commProfileSet>
</tns:user>
</tns:users>

```

## XML Schema Definition for bulk importing messaging profiles

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:one="http://
xml.avaya.com/schema/import" elementFormDefault="qualified"
targetNamespace="http://xml.avaya.com/schema/import_csm_mm" xmlns:csm="http://
xml.avaya.com/schema/import_csm_mm">

    <xs:import namespace="http://xml.avaya.com/schema/import"
schemaLocation="userimport.xsd"/>
    <!--Changes in xsd file need to generate jaxb src using this xsd-->
    <xs:complexType name="xmlMessagingProfile">

```

```

    <xs:complexContent>
      <xs:extension base="one:xmlCommProfileType" >
        <xs:sequence>
          <!--
            Specifies the messaging system of the subscriber you want
to add.
            You can choose this option from the drop-down box.
          -->
          <xs:element name="messagingName" type="xs:string" maxOccurs="1"
minOccurs="1" />
          <xs:element name="useExisting" type="xs:boolean" maxOccurs="1"
minOccurs="0"/><!-- use existing -->

          <!-- Specifies the messaging template of a subscriber. -->
          <xs:element name="messagingTemplate" type="xs:string"
maxOccurs="1" minOccurs="0" />

          <xs:element name="mailboxNumber" maxOccurs="1" minOccurs="1" >
            <xs:simpleType>
              <xs:restriction base="xs:string">
                <xs:pattern value="[0-9]{1,10}"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:element>

          <!--
            Specifies the default password the subscriber must use to
log in to his or her mailbox.
            The password can be from one digit in length to a maximum
of 15 digits.
          -->
          <xs:element name="password" maxOccurs="1" minOccurs="1">
            <xs:simpleType>
              <xs:restriction base="xs:string">
                <xs:pattern value="[0-9]{1,15}"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:element>
          <xs:element name="deleteOnUnassign" type="xs:boolean"
maxOccurs="1" minOccurs="0"/>

          <!-- follows overriding subscriber data -->

          <!--
            The class of service for this subscriber.
            The COS controls subscriber access to many features and
provides general settings,
            such as mailbox size.
          -->
          <xs:element name="cos" maxOccurs="1" minOccurs="0" > <!-- MM/
CMM field -->
            <xs:simpleType>
              <xs:restriction base="xs:string">
                <xs:pattern value="[0-9]|[0-9]{2}|[0-4][0-9]{2}|[5]
[0-4][0-9]|[5][5][0-1]"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:element>

          <!--
            Specifies the default community ID for the subscriber.
            Community IDs are used to control message sending and receiving
among groups of subscribers.
            The default value is 1.
          -->

```

```

-->
<!-- MM/CMM field -->
  <xs:element name="communityID" maxOccurs="1" minOccurs="0" >
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:pattern value="[0-9]|[0-1][0-5]"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>

  <!--
    Specifies the name that appears before the machine name and
    domain in the subscriber's e-mail address.
    The machine name and domain are automatically added to the
    handle you enter when the subscriber sends or
    receives an e-mail.
  -->
  <xs:element name="emailHandle" maxOccurs="1" minOccurs="0" >
<!-- MM/CMM field -->
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:pattern value="^[a-zA-Z0-9\w\.-]*"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

  <!--
    Specifies the display name of the subscriber in address book
    listings,
    such as those for e-mail client applications.
    The name you enter can be 1 to 64 characters in length.
  -->
  <xs:element name="commonName" type="xs:string" maxOccurs="1"
minOccurs="0" /> <!-- MM/CMM field -->

  <!--
    Specifies one or more alternate number to reach a subscriber.
    You can use secondary extensions to specify a telephone
    number for direct reception of faxes,
    to allow callers to use an existing Caller Application, or to
    identify each line appearance on the subscriber's telephone set
    if they have different telephone numbers.
  -->
  <xs:element name="secondaryExtension" maxOccurs="1"
minOccurs="0" > <!-- MM/CMM field -->
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:pattern value="[0-9]{10}"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>

  <xs:element name="mmSpecific" type="csm:xmlMMSpecific"
maxOccurs="1" minOccurs="0" />
  <xs:element name="cmmSpecific" type="csm:xmlCMMSpecific"
maxOccurs="1" minOccurs="0" />
  </xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>

  <xs:complexType name="xmlMMSpecific">
    <xs:sequence>
  <!--

```

## Managing Users

```

        Specifies a unique address in the voice mail network.
        The numeric address can be from 1 to 50 digits and can contain the
Mailbox Number.
-->
<xs:element name="numericAddress" maxOccurs="1" minOccurs="0"> <!-- MM
field -->
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:pattern value="[0-9]*/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<!-- The primary telephone extension of the subscriber. -->
<xs:element name="pbxExtension" maxOccurs="1" minOccurs="0" > <!-- MM
field -->
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:pattern value="[+0-9]*/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<!--
    The telephone number of the subscriber as displayed in address book
listings and client applications.
    The entry can be a maximum of 50 characters in length and can contain
any combination of
    digits (0-9), period (.), hyphen (-), plus sign (+), and left and
right parentheses ([) and (]).
-->
<xs:element name="telephoneNumber" maxOccurs="1" minOccurs="0" > <!--
MM field -->
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:pattern value="[+.\()0-9]*/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

<!--
    If the subscriber name is entered in multi-byte character format,
then this field specifies the ASCII translation of the subscriber name.
-->
<xs:element name="asciiVersionOfName" type="xs:string" maxOccurs="1"
minOccurs="0" /> <!-- MM field -->

<!--
    Specifies whether your password expires or not. You can choose one
of the following:
        - yes: for password to expire
        - no: if you do not want your password to expire
-->
<xs:element name="expirePassword" type="csm:xmlYesNoType" maxOccurs="1"
minOccurs="0"/> <!-- MM field -->

<!--
    Specifies whether you want your mailbox to be locked.
    A subscriber mailbox can become locked after two unsuccessful login
attempts.
    You can choose one of the following:
        - no: to unlock your mailbox
        - yes: to lock your mailbox and prevent access to it
-->
<xs:element name="mailBoxLocked" type="csm:xmlYesNoType" maxOccurs="1"

```

```

minOccurs="0" /> <!-- MM field -->

    <!--
        Specifies the mailbox number or transfer dial string of the
        subscriber's personal operator or assistant.
        This field also indicates the transfer target when a caller to this
        subscriber presses 0 while listening to the subscriber's greeting.
    -->
    <xs:element name="personalOperatorMailbox" maxOccurs="1" minOccurs="0">
<!-- MM field -->
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[0-9]+([*#,][0-9]+)*/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <!--
        Specifies when to route calls to the backup operator mailbox.
        The default value for this field is Always Active.
    -->
    <xs:element name="personalOperatorSchedule" type="xs:string"
maxOccurs="1" minOccurs="0" /> <!-- MM field -->

    <!--
        Specifies the order in which the subscriber hears the voice messages.
        You can choose one of the following:
        - urgent first then newest: to direct the system to play any
        messages marked as urgent prior to playing non-urgent messages. Both the urgent and
        non-urgent messages are played in the reverse order of how they were received.
        - oldest messages first: to direct the system to play messages
        in the order they were received.
        - urgent first then oldest: to direct the system to play any
        messages marked as urgent prior to playing non-urgent messages. Both the urgent and
        non-urgent messages are played in the order of how they were received.
        - newest messages first: to direct the system to play messages
        in the reverse order of how they were received.
    -->
    <xs:element name="tuiMessageOrder" maxOccurs="1" minOccurs="0" > <!--
MM field -->
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="urgent first then newest"/>
                <xs:enumeration value="oldest messages first"/>
                <xs:enumeration value="newest messages first"/>
                <xs:enumeration value="urgent first then oldest"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <!--
        Specifies the intercom paging settings for a subscriber. You can
        choose one of the following:
        - paging is off: to disable intercom paging for this subscriber.
        - paging is manual: if the subscriber can modify, with Subscriber
        Options or the TUI,
        the setting that allows callers to page the
        subscriber.
        - paging is automatic: if the TUI automatically allows callers
        to page the subscriber.
    -->
    <xs:element name="intercomPaging" maxOccurs="1" minOccurs="0" > <!-- MM
field -->
        <xs:simpleType>
            <xs:restriction base="xs:string">

```

```

        <xs:enumeration value="paging is off"/>
        <xs:enumeration value="paging is manual"/>
        <xs:enumeration value="paging is automatic"/>
    </xs:restriction>
</xs:simpleType>
</xs:element>

<!--
    Specifies whether a subscriber can receive messages, e-mail messages
    and call-answer messages from other subscribers.
    You can choose one of the following:
        - yes: to allow the subscriber to create, forward, and receive
    messages.
        - no: to prevent the subscriber from receiving call-answer
    messages and to hide the subscriber from
        the telephone user interface (TUI). The subscriber
    cannot use the TUI to access the mailbox, and other TUI users cannot address
    messages to the subscriber.
-->
<xs:element name="voiceMailEnabled" type="csm:xmlTrueFalseType"
maxOccurs="1" minOccurs="0" />

<!--
    Specifies additional, useful information about a subscriber.
    Entries in this field are for convenience and are not used by the
    messaging system.
-->
<xs:element name="miscellaneous1" type="csm:xmlLength51Type"
maxOccurs="1" minOccurs="0" />

<!--
    Specifies additional, useful information about a subscriber.
    Entries in this field are for convenience and are not used by the
    messaging system.
-->
<xs:element name="miscellaneous2" type="csm:xmlLength51Type"
maxOccurs="1" minOccurs="0" />

<!--
    Specifies additional, useful information about a subscriber.
    Entries in this field are for convenience and are not used by the
    messaging system.
-->
<xs:element name="miscellaneous3" type="csm:xmlLength51Type"
maxOccurs="1" minOccurs="0" />

<!--
    Specifies additional, useful information about a subscriber.
    Entries in this field are for convenience and are not used by the
    messaging system.
-->
<xs:element name="miscellaneous4" type="csm:xmlLength51Type"
maxOccurs="1" minOccurs="0" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="xmlCMMSpecific">
    <xs:sequence>

<!--
    Specifies the number of the switch on which this subscriber's
    extension is administered.
    You can enter "0" through "99", or leave this field blank.
    - Leave this field blank if the host switch number should be used.
    - Enter a "0" if no message waiting indicators should be sent

```

for this subscriber.

You should enter 0 when the subscriber does not have a phone on any switch in the network.

```

-->
<xs:element name="switchNumber" maxOccurs="1" minOccurs="0" > <!-- CMM
field -->
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:pattern value="[0-9]|[0-9][0-9]"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<!--
  Specifies the Subscriber Account Code.
  The Subscriber Account Code is used to create Call Detail Records
on the switch for calls placed by the voice ports.
  The value you enter in this field can contain any combination of
digits from 0 to 9.
  If an account code is not specified, the system will use the
subscriber's mailbox extension as the account code.
-->
<xs:element name="accountCode" maxOccurs="1" minOccurs="0" > <!-- CMM
field -->
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:pattern value="([0-9])*"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<!--
  Specifies the number to be used as the default destination for the
Transfer Out of Messaging feature.
  You can enter 3 to 10 digits in this field depending on the length
of the system's extension, or leave this field blank.
-->
<xs:element name="coveringExtension" maxOccurs="1" minOccurs="0"> <!--
CMM field -->
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:pattern value="[0-9]{10}"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<!--
  Specifies additional, useful information about a subscriber.
  Entries in this field are for convenience and are not used by the
messaging system.
-->
<xs:element name="miscellaneous1" type="csm:xmlLength11Type"
maxOccurs="1" minOccurs="0" />

<!--
  Specifies additional, useful information about a subscriber.
  Entries in this field are for convenience and are not used by the
messaging system.
-->
<xs:element name="miscellaneous2" type="csm:xmlLength11Type"
maxOccurs="1" minOccurs="0" />

<!--
  Specifies additional, useful information about a subscriber.
  Entries in this field are for convenience and are not used by the

```

```

messaging system.
-->
  <xs:element name="miscellaneous3" type="csm:xmlLength11Type"
maxOccurs="1" minOccurs="0" />

  <!--
    Specifies additional, useful information about a subscriber.
    Entries in this field are for convenience and are not used by the
messaging system.
-->
  <xs:element name="miscellaneous4" type="csm:xmlLength11Type"
maxOccurs="1" minOccurs="0" />
</xs:sequence>
</xs:complexType>

<xs:simpleType name="xmlYesNoType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Yes" />
    <xs:enumeration value="No" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="xmlTrueFalseType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="TRUE" />
    <xs:enumeration value="FALSE" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="xmlLength11Type">
  <xs:restriction base="xs:string">
    <xs:maxLength value="11"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="xmlLength51Type">
  <xs:restriction base="xs:string">
    <xs:maxLength value="51"/>
  </xs:restriction>
</xs:simpleType>
</xs:schema>

```

### Sample XML for bulk importing messaging profiles

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
  <tns:user>
    <authenticationType>BASIC</authenticationType>
    <description>description</description>
    <displayName>displayname</displayName>
    <displayNameAscii>displayNameAscii</displayNameAscii>
    <dn>dn</dn>
    <isDuplicatedLoginAllowed>>true</isDuplicatedLoginAllowed>
    <isEnabled>true</isEnabled>
    <isVirtualUser>>false</isVirtualUser>
    <givenName>givenName00</givenName>
    <honorific>honorific</honorific>
    <loginName>user00_00xyz@avaya.com</loginName>
    <middleName>middleName</middleName>
    <managerName>managerName</managerName>
    <preferredGivenName>preferredGivenName</preferredGivenName>
    <preferredLanguage>preferredLanguage</preferredLanguage>
    <source>local</source>
  </tns:user>
</tns:users>

```

```

<sourceUserKey>sourceUserKey</sourceUserKey>
<status>AUTHPENDING</status>
<suffix>suffix</suffix>
<surname>surname</surname>
<timeZone>timeZone</timeZone>
<title>title</title>
<userName>userName00</userName>
<userPassword>userPassword</userPassword>
<commPassword>commPassword</commPassword>
<userType>ADMINISTRATOR</userType>
<commProfileSet>
  <commProfileSetName>
    commProfileSetName00
  </commProfileSetName>
  <isPrimary>true</isPrimary>
  <commProfileList>
    <commProfile xsi:type="ipt:xmlMessagingProfile"
      xmlns:ipt="http://xml.avaya.com/schema/import_csm_mm">
      <commProfileType>Messaging</commProfileType>
      <ipt:messagingName>MM-155-187</ipt:messagingName>
      <ipt:useExisting>false</ipt:useExisting>
      <ipt:messagingTemplate>
        DEFAULT_MM_5_2
      </ipt:messagingTemplate>
      <ipt:mailboxNumber>3201</ipt:mailboxNumber>
      <ipt:password>534456346</ipt:password>
      <ipt:cos>0</ipt:cos>
      <ipt:communityID>1</ipt:communityID>
      <ipt:mmSpecific>
        <ipt:numericAddress>3201</ipt:numericAddress>
        <ipt:pbxExtension>32134</ipt:pbxExtension>
        <ipt:telephoneNumber>42342</ipt:telephoneNumber>
        <!--<ipt:expirePassword></ipt:expirePassword>-->
        <ipt:tuiMessageOrder>1</ipt:tuiMessageOrder>
        <ipt:intercomPaging>1</ipt:intercomPaging>
        <ipt:voiceMailEnabled>
          FALSE
        </ipt:voiceMailEnabled>
        <ipt:miscellaneous1>
          Miscellaneous
        </ipt:miscellaneous1>
      </ipt:mmSpecific>
    </commProfile>
  </commProfileList>
</commProfileSet>
</tns:user>
</tns:users>

```

## XML Schema Definition for bulk importing global setting records

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ext="http://
xml.avaya.com/schema/import" xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://xml.avaya.com/schema/import" version="1.0">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      This Schema defines schema for bulk import and export of System ACL, Public
      Contacts and Shared Address.
    </xs:documentation>
  </xs:annotation>
  <xs:element name="presenceSystemDefault" type="tns:xmlPresSystemDefaultType"/>
  <xs:element name="presenceEnforcedUserACL"
type="tns:xmlPresEnforcedUserACLEntryType"/>
  <xs:element name="presenceSystemRule" type="tns:xmlPresSystemRuleType"/>
  <xs:element name="presenceSystemACL" type="tns:xmlPresSystemACLEntryType"/>

```

```

<xs:element name="publicContact" type="tns:xmlPublicContact"/>
<xs:element name="globalSettings" type="tns:globalSettingsType"/>
<xs:element name="sharedAddress" type="tns:xmlSharedAddress"/>
<xs:complexType name="globalSettingsType">
<xs:annotation>
  <xs:documentation xml:lang="en">
    ---Root Element 'presenceSystemDefault' represent a global default that
    defines access to presence if none of the more specific rules apply. There must be
    at least one System Default rule defined.
    ---Root Element 'presenceEnforcedUserACL' represent collection of
    Enforced User ACL (containing 1 or more Enforced User ACL).This rule is similar to
    a User ACL in the sense that its entries define access between individual
    presentities and watchers. However this rule is managed by the administrator as
    opposed to presentities themselves. Entries of Enforced User ACL can also be defined
    with different priorities. Entries with higher priority will have more weight than
    entries with lower priority.
    ---Root Element 'presenceSystemRule' represent collection of System Rules
    (containing 1 or more System Rules).Global rules that enforce certain level of
    presence access for everyone in the solution. There may be several rules that apply
    to all presentities and all watchers. System Rules are used to enforce global
    policies. For example, a system rule can declare that telephony presence should be
    available to everybody in the company. System Rules can be defined with different
    priorities. Rules with higher priority will have more weight than rules with lower
    priority
    ---Root Element 'presenceSystemACL' represent collection of System ACL
    (containing 1 or more System ACL).System ACL (Access Control List) - are enterprise-
    wide rules that can allow a watcher to see presence of all users or deny a watcher
    from accessing anyone's presence. There may be several entries in the list, each
    entry corresponding to one watcher. System ACL is normally used to provide critical
    system services with a privileged access to presence of all users.
    ---Root Element 'publicContact' represent collection of public contacts
    (containing 1 or more public contacts).A personal contact is owned by an individual
    user and is not accessible to all users. A public contact can be shared by all users
    and is owned by the default system user.
    ---Root Element 'sharedAddress' represent collection of shared Address
    (containing 1 or more shared Addresses).A shared Address can be shared by all users.
  </xs:documentation>
</xs:annotation>
<xs:sequence>
  <xs:element name="presenceSystemDefault"
type="tns:xmlPresSystemDefaultType" minOccurs="0" maxOccurs="unbounded"/>
  <xs:element name="presenceEnforcedUserACL"
type="tns:xmlPresEnforcedUserACLEntryType" minOccurs="0" maxOccurs="unbounded"/>
  <xs:element name="presenceSystemRule" type="tns:xmlPresSystemRuleType"
minOccurs="0" maxOccurs="unbounded"/>
  <xs:element name="presenceSystemACL"
type="tns:xmlPresSystemACLEntryType" minOccurs="0" maxOccurs="unbounded"/>
  <xs:element name="sharedAddress" type="tns:xmlSharedAddress"
minOccurs="0" maxOccurs="unbounded"/>
  <xs:element name="publicContact" type="tns:xmlPublicContact"
minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="xmlSharedAddress">
  <xs:sequence>
    <xs:annotation>
      <xs:documentation xml:lang="en">
        ---addressType:The unique text name of the address type. Possible
        values are: Home, business.
        ---name: The Name property defines the unique label by which the
        address is known. Default format for user specific address should include user name
        place address type.
        ---building:The name or other designation of a structure.
        ---localityName:The name of a locality, such as a city, county
        or other geographic region.
      </xs:documentation>
    </xs:annotation>
  </xs:sequence>
</xs:complexType>

```

```

        ---postalCode:A code used by postal services to route mail to a
destination. In the United States this is the zip code.
        ---room:Name or designation of a room.
        ---stateOrProvince:The full name of a state or province.
        ---country:A country.
        ---street:The physical address of the object such as an address for
package delivery
        ---postalAddress:A free formed text area for the complete physical
delivery address. It may be used in place of the specific fields in this table.
        ---readOnly:A boolean indicator showing whether or not the address
can be changed from its default value.
    </xs:documentation>
</xs:annotation>
<xs:element name="addressType" type="xs:string"/>
<xs:element name="name" type="xs:string"/>
<xs:element name="building" type="xs:string" minOccurs="0"/>
<xs:element name="localityName" type="xs:string" minOccurs="0"/>
<xs:element name="postalCode" type="xs:string" minOccurs="0"/>
<xs:element name="room" type="xs:string" minOccurs="0"/>
<xs:element name="stateOrProvince" type="xs:string" minOccurs="0"/>
<xs:element name="country" type="xs:string" minOccurs="0"/>
<xs:element name="street" type="xs:string" minOccurs="0"/>
<xs:element name="postalAddress" minOccurs="0">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:maxLength value="1024"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>
<xs:element name="readOnly" type="xs:boolean" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="xmlPublicContact">
    <xs:sequence>
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---company:The organization that the contact belongs to.
                ---description: A free text field containing human readable text
providing information on this entry.
                ---displayName:The localized name of a contact to be used when
displaying. It will typically be the localized full name. This value may be
provisioned from the user's enterprise directory entry. If it does not exist,
synchronization rules can be used to populate it for other fields e.g. Surname,
GivenName, or LoginName.
                ---displayNameAscii:The full text name of the contact represented
in ASCII. It is used to support display (e.g. endpoints) that cannot handle
localized text.
                ---dn:The distinguished name of the user. The DN is a sequence
of relative distinguished names (RDN) connected by commas. An RDN is an attribute
with an associated value in the form of attribute=value, normally expressed in a
UTF-8 string format. The dn can be used to uniquely identify this record. Note the
dn is changeable.
                ---givenName:The first name of the contact.
                ---initials:Initials of the contact.
                ---middleName:The middle name of the contact.
                ---preferredGivenName:The nick name of the contact.
                ---preferredLanguage:The individual's preferred written or spoken
language. Values will conform to rfc4646 and the reader should refer to rfc4646 for
syntax. This format uses the ISO standard Language (ISO-639) and region (ISO-3166)
codes In the absence of a value the client's locale should be used, if no value is
set, en-US should be defaulted.
                ---source:Free format text field that identifies the entity that
created this user record. The format of this field will be either a IP Address/
Port or a name representing an enterprise LDAP or Avaya.
                ---sourceUserKey:The key of the user from the source system.
            
```

## Managing Users

If the source is an Enterprise Active Directory server, this value will be the objectGUID.

---suffix:The text appended to a name e.g. Jr., III.  
---surname:The user's last name, also called the family name.  
---title:The job function of a person in their organizational context.Examples: supervisor, manager.  
---contactAddresses:A Entity used to store a contact's address.  
---addresses:A fully qualified URI for interacting with this contact. Any addresses added to this entity should contain a qualifier e.g. sip, sips, tel, mailto. The address should be syntactically valid based on the qualifier. It must be possible to add via the GUI and Interface. The application must do validation.

```
</xs:documentation>
</xs:annotation>
<xs:element name="company" type="xs:string" minOccurs="0"/>
<xs:element name="description" type="xs:string" minOccurs="0"/>
<xs:element name="displayName" type="xs:string"/>
<xs:element name="displayNameAscii" type="xs:string"/>
<xs:element name="dn" type="xs:string" minOccurs="0"/>
<xs:element name="givenName" type="xs:string"/>
<xs:element name="initials" type="xs:string" minOccurs="0"/>
<xs:element name="middleName" type="xs:string" minOccurs="0"/>
<xs:element name="preferredGivenName" type="xs:string" minOccurs="0"/>
<xs:element name="preferredLanguage" type="xs:string" minOccurs="0"/>
<xs:element name="source" type="xs:string"/>
<xs:element name="sourceUserKey" type="xs:string"/>
<xs:element name="suffix" type="xs:string" minOccurs="0"/>
<xs:element name="surname" type="xs:string"/>
<xs:element name="title" type="xs:string" minOccurs="0"/>
<xs:element name="contactAddresses" type="tns:xmlContactAddressList"
minOccurs="0"/>
  <xs:element name="addresses" type="tns:xmlAddressList" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="xmlContactAddressList">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      ContactAddressList: A list containing Contact Addresses
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="contact" type="tns:xmlContactAddress" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlContactAddress">
  <xs:sequence>
    <xs:annotation>
      <xs:documentation xml:lang="en">
        ---type:The value reflecting the type of handle this is. Possible
values are "username", "e164", and "privatesubsystem
        ---category:The value representing a further qualification to
the contact address. Possible values include Office, Home, Mobile.
        ---handle:This is the name given to the user to allow communication
to be established with the user. It is an alphanumeric value that must comply with
the userinfo related portion of a URI as described in rfc2396. However, it is
further restricted as ASCII characters with only the "+" prefix to signify this is
an E.164 handle and "_" and "." special characters supported.The handle and type
together are unique within a specific domain. Note, the handle plus domain can be
used to construct a user's Address of Record.
        ---label:A free text description for classifying this contact.
        ---altLabel:A free text description for classifying this contact.
This is similar to ContactLabel, but it is used to store alternate language
representations.
      </xs:documentation>
```

```

        </xs:annotation>
        <xs:element name="type" type="xs:string"/>
        <xs:element name="category" type="xs:string" minOccurs="0"/>
        <xs:element name="handle" type="xs:string"/>
        <xs:element name="label" type="xs:string" minOccurs="0"/>
        <xs:element name="altLabel" type="xs:string" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlAddressList">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            AddressList: A list containing Addresses
        </xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="address" type="tns:xmlAddress" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlAddress">
    <xs:complexContent>
        <xs:extension base="tns:xmlSharedAddress">
            <xs:sequence>
                <xs:annotation>
                    <xs:documentation xml:lang="en">
                        private:A boolean indicator to specify if this attribute
set could be shared across multiple users. Private attributes sets can only be owned
by a single user. Default=false.
                    </xs:documentation>
                </xs:annotation>
                <xs:element name="private" type="xs:boolean"/>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="xmlPresInfoTypeAccessType">
    <xs:sequence>
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---accessLevel:possible values:IM,Telephony
                ---action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING,
UNDEFINED
            </xs:documentation>
        </xs:annotation>
        <xs:element name="accessLevel" type="xs:string"/>
        <xs:element name="action" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlPresACRuleType">
    <xs:sequence>
        <xs:element name="infoTypeAccess" type="tns:xmlPresInfoTypeAccessType"
minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlPresSystemDefaultType">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            'presenceSystemDefault' represent a global default that defines
access to presence if none of the more specific rules apply. There must be at least
one System Default rule defined.
        </xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="tns:xmlPresACRuleType"/>
    </xs:complexContent>

```

```

</xs:complexType>
<xs:complexType name="xmlPresSystemRuleType">
  <xs:complexContent>
    <xs:extension base="tns:xmlPresACRuleType">
      <xs:sequence>
        <xs:annotation>
          <xs:documentation xml:lang="en">
            --- 'presenceSystemRule' represent collection of System
            Rules (containing 1 or more System Rules).Global rules that enforce certain level
            of presence access for everyone in the solution. There may be several rules that
            apply to all presentities and all watchers. System Rules
            are used to enforce global policies. For example, a system rule can declare that
            telephony presence should be available to everybody in the company. System
            Rules can be defined with different priorities. Rules with
            higher priority will have more weight than rules with lower priority apply to all
            presentities and all watchers.
            ---priority:Entries of Enforced User ACL can also be defined
            with different priorities. Entries with higher priority will have more weight than
            entries with lower priority.
          </xs:documentation>
        </xs:annotation>
        <xs:element name="priority" type="xs:string"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
<xs:complexType name="xmlPresSystemACLEntryType">
  <xs:complexContent>
    <xs:extension base="tns:xmlPresACRuleType">
      <xs:sequence>
        <xs:annotation>
          <xs:documentation xml:lang="en">
            ---'presenceSystemACL' represent collection of System ACL
            (containing 1 or more System ACL).System ACL (Access Control List) - are enterprise-
            wide rules that can allow a watcher to see presence of all users or deny a watcher
            from accessing anyone's presence. There may be several entries in the list, each
            entry corresponding to one watcher. System ACL is normally used to provide critical
            system services with a privileged access to presence of all users.
            ---watcherLoginName:LoginName of the watcher. This value
            needs to be specified if watcher is a user.
            ---watcherDisplayName:DisplayName of the watcher. This
            value needs to be specified if watcher is a Contact
          </xs:documentation>
        </xs:annotation>
        <xs:choice>
          <xs:element name="watcherLoginName" type="xs:string"
minOccurs="0"/>
          <xs:element name="watcherDisplayName" type="xs:string"
minOccurs="0"/>
        </xs:choice>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
<xs:complexType name="xmlPresEnforcedUserACLEntryType">
  <xs:complexContent>
    <xs:extension base="tns:xmlPresACRuleType">
      <xs:sequence>
        <xs:annotation>
          <xs:documentation xml:lang="en">
            ---'presenceEnforcedUserACL' represent collection of
            Enforced User ACL (containing 1 or more Enforced User ACL).This rule is similar to
            a User ACL in the sense that its entries define access between individual
            presentities and watchers. However this rule is managed by the administrator as
            opposed to presentities themselves. Entries of Enforced User ACL can also be defined
          </xs:documentation>
        </xs:annotation>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

```

```

with different priorities. Entries with higher priority will have more weight than
entries with lower priority.
    ---watcherLoginName:LoginName of the watcher. This value
needs to be specified if watcher is a user.
    ---watcherDisplayName:DisplayName of the watcher. This
value needs to be specified if watcher is a Contact
    ---priority:Entries of Enforced User ACL can also be
defined with different priorities. Entries with higher priority will have more
weight than entries with lower priority.
    ---userName:LoginName of the presentity.
    </xs:documentation>
  </xs:annotation>
  <xs:element name="userName" type="xs:string"/>
  <xs:choice>
    <xs:element name="watcherLoginName" type="xs:string"
minOccurs="0"/>
    <xs:element name="watcherDisplayName" type="xs:string"
minOccurs="0"/>
  </xs:choice>
  <xs:element name="priority" type="xs:string"/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:schema>

```

## Sample XML for bulk importing global setting records

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:globalSettings xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
xml.avaya.com/schema/import systemPresence.xsd ">
  <!-- Root Element 'presenceSystemDefault' represent a global default that defines
access to presence if none of the more specific rules apply. There must be at least
one System Default rule defined.
    accessLevel:possible values:ALL,Telephony
    action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
-->
  <tns:presenceSystemDefault>
    <infoTypeAccess>
      <accessLevel>ALL</accessLevel>
      <action>ALLOW</action>
    </infoTypeAccess>
  </tns:presenceSystemDefault>
  <!--Root Element 'presenceEnforcedUserACL' represent collection of Enforced User
ACL (containing 1 or more Enforced User ACL).This rule is similar to a User ACL in
the sense that its entries define access between individual presentities
and watchers. However this rule is managed by the administrator as opposed to
presentities themselves. Entries of Enforced User ACL can also be defined with
different priorities. Entries with higher priority will have more weight than
entries with lower priority.
    accessLevel:possible values:ALL,Telephony
    action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
    watcherLoginName:LoginName of the watcher. This value needs to be specified if
watcher is a user.
    watcherDisplayName:DisplayName of the watcher. This value needs to be specified
if watcher is a Contact
    priority:Entries of Enforced User ACL can also be defined with different
priorities. Entries with higher priority will have more weight than entries with
lower priority.
    userName:LoginName of the presentity.
-->
  <tns:presenceEnforcedUserACL>
    <infoTypeAccess>

```

```

    <accessLevel>Telephony</accessLevel>
    <action>BLOCK</action>
  </infoTypeAccess>
  <userName>jmiller@avaya.com</userName>
  <watcherLoginName>userlogin2@avaya.com</watcherLoginName>
  <priority>HIGH</priority>
</tns:presenceEnforcedUserACL>
<!-- Root Element 'presenceSystemRule' represent collection of System Rules
(containing 1 or more System Rules).Global rules that enforce certain level of
presence access for everyone in the solution. There may be several rules that apply
to all presentities and all watchers. System Rules are used to enforce global
policies. For example, a system rule can declare that telephony presence should be
available to everybody in the company. System Rules can be defined with different
priorities. Rules with higher priority will have more weight than rules with lower
priority
  accessLevel:possible values:IM,Telephony
  action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
  watcherLoginName:LoginName of the watcher. This value needs to be specified if
watcher is a user.
  watcherDisplayName:DisplayName of the watcher. This value needs to be specified
if watcher is a Contact
  priority:Entries of Enforced User ACL can also be defined with different
priorities. Entries with higher priority will have more weight than entries with
lower priority.
-->
<tns:presenceSystemRule>
  <infoTypeAccess>
    <accessLevel>Telephony</accessLevel>
    <action>ALLOW</action>
  </infoTypeAccess>
  <priority>HIGH</priority>
</tns:presenceSystemRule>
<!--Root Element 'presenceSystemACL' represent collection of System ACL
(containing 1 or more System ACL).System ACL (Access Control List) - are enterprise-
wide rules that can allow a watcher to see presence of all users or deny a
watcher from accessing anyone's presence. There may be several entries in the list,
each entry corresponding to one watcher. System ACL is normally used to provide
critical system services with a privileged access to presence of all users.
  accessLevel:possible values:IM,Telephony
  action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
  watcherLoginName:LoginName of the watcher. This value needs to be specified if
watcher is a user.
-->
<tns:presenceSystemACL>
  <infoTypeAccess>
    <accessLevel>Telephony</accessLevel>
    <action>BLOCK</action>
  </infoTypeAccess>
  <watcherLoginName>jmiller@avaya.com</watcherLoginName>
</tns:presenceSystemACL>
<!--Root Element 'publicContact' represent collection of public contacts
(containing 1 or more public contacts).A personal contact is owned by an individual
user and is not accessible to all users. A public contact can be shared by all users
and is owned by the default system user.
  company:The organization that the contact belongs to.
  description: A free text field containing human readable text providing
information on this entry.
  displayName:The localized name of a contact to be used when displaying. It will
typically be the localized full name. This value may be provisioned from the user's
enterprise directory entry. If it does not exist, synchronization rules can be used
to populate it for other fields e.g. Surname, GivenName, or LoginName.
  displayNameAscii:The full text name of the contact represented in ASCII. It is
used to support display (e.g. endpoints) that cannot handle localized text.
  dn:The distinguished name of the user. The DN is a sequence of relative
distinguished names (RDN) connected by commas. An RDN is an attribute with an

```

associated value in the form of attribute=value, normally expressed in a UTF-8 string format. The dn can be used to uniquely identify this record. Note the dn is changeable.

givenName:The first name of the contact.  
 initials:Initials of the contact.  
 middleName:The middle name of the contact.  
 preferredGivenName:The nick name of the contact.  
 preferredLanguage:The individual's preferred written or spoken language. Values will conform to rfc4646 and the reader should refer to rfc4646 for syntax. This format uses the ISO standard Language (ISO-639) and region (ISO-3166) codes In the absence of a value the client's locale should be used, if no value is set, en-US should be defaulted.

source:Free format text field that identifies the entity that created this user record. The format of this field will be either a IP Address/Port or a name representing an enterprise LDAP or Avaya.

sourceUserKey:The key of the user from the source system. If the source is an Enterprise Active Directory server, this value with be the objectGUID.

suffix:The text appended to a name e.g. Jr., III.

surname:The user's last name, also called the family name.

title:The job function of a person in their organizational context.Examples: supervisor, manager.

contactAddresses:A table used to store a contact's address.

addresses:A fully qualified URI for interacting with this contact. Any addresses added to this table should contain a qualifier e.g. sip, sips, tel, mailto. The address should be syntactically valid based on the qualifier. It must be possible to add via the GUI and Interface. The application must do validation.

-->

```
<tns:publicContact>
  <company>ABC</company>
  <description>Company ABC description</description>
  <displayName>John Miller</displayName>
  <displayNameAscii></displayNameAscii>
  <dn>dc=acme,dc=org</dn>
  <givenName>John</givenName>
  <initials>Mr</initials>
  <middleName>M</middleName>
  <preferredGivenName>John</preferredGivenName>
  <preferredLanguage>English</preferredLanguage>
  <source>ldap</source>
  <sourceUserKey>18966</sourceUserKey>
  <suffix>Jr.</suffix>
  <surname>Miller</surname>
  <title>Manager</title>
```

<!--type:The value reflecting the type of handle this is. Possible values are "username", "e164", and "privatesubsystem

category:The value representing a further qualification to the contact address. Possible values include Office, Home, Mobile.

handle:This is the name given to the user to allow communication to be established with the user. It is an alphanumeric value that must comply with the userinfo related portion of a URI as described in rfc2396. However, it is further restricted as ASCII characters with only the "+" prefix to signify this is an E. 164 handle and "\_" and "." special characters supported.The handle and type together are unique within a specific domain. Note, the handle plus domain can be used to construct a user's Address of Record.

label:A free text description for classifying this contact.

altLabel:A free text description for classifying this contact. This is similar to ContactLabel, but it is used to store alternate language representations.

-->

```
<contactAddresses>
  <contact>
    <type>sip</type>
    <category>office</category>
    <handle>sip:jmiller@abc.com</handle>
    <label>Miller</label>
    <altLabel>John</altLabel>
```

```

    </contact>
  </contactAddresses>
  <addresses>
    <!-- addressType:The unique text name of the address type. Possible values
are: Home, business.
    name: The Name property defines the unique label by which the address is
known. Default format for user specific address should include user name place
address type.
    building:The name or other designation of a structure.
    localityName:The name of a locality, such as a city, county or other
geographic region.
    postalCode:A code used by postal services to route mail to a destination.
In the United States this is the zip code.
    room:Name or designation of a room.
    stateOrProvince:The full name of a state or province.
    country:A country.
    street:The physical address of the object such as an address for package
delivery
    postalAddress:A free formed text area for the complete physical delivery
address. It may be used in place of the specific fields in this table.
-->
    <address>
      <addressType>office</addressType>
      <name>John Miller</name>
      <building>building A</building>
      <localityName>Magarpatta</localityName>
      <postalCode>411048</postalCode>
      <room>room 123</room>
      <stateOrProvince>MH</stateOrProvince>
      <country>India</country>
      <street>Hadapsar</street>
      <private>>false</private>
    </address>
  </addresses>
</tns:publicContact>
  <!--addressType:The unique text name of the address type. Possible values
are: Home, business.
  name: The Name property defines the unique label by which the address is
known. Default format for user specific address should include user name place
address type.
  building:The name or other designation of a structure.
  localityName:The name of a locality, such as a city, county or other
geographic region.
  postalCode:A code used by postal services to route mail to a destination.
In the United States this is the zip code.
  room:Name or designation of a room.
  stateOrProvince:The full name of a state or province.
  country:A country.
  street:The physical address of the object such as an address for package
delivery
  postalAddress:A free formed text area for the complete physical delivery
address. It may be used in place of the specific fields in this table.
  readOnly:A boolean indicator showing whether or not the address can be
changed from its default value.
-->
  <tns:sharedAddress>
    <addressType>office</addressType>
    <name>Avaya Pune</name>
    <building>building A</building>
    <localityName>Magarpatta</localityName>
    <postalCode>411048</postalCode>
    <room>room 123</room>
    <stateOrProvince>MH</stateOrProvince>
    <country>India</country>
    <street>Hadapsar</street>

```

```

    <readOnly>true</readOnly>
  </tns:sharedAddress>

</tns:globalSettings>

```

## XML Schema Definition for bulk deleting global setting records

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/bulkdelete"
targetNamespace="http://xml.avaya.com/schema/bulkdelete"
  elementFormDefault="qualified" version="1.0" xmlns:xs="http://www.w3.org/
2001/XMLSchema">

  <xs:element name="sharedAddress" type="tns:xmlDeleteSharedAddress"/>
  <xs:element name="publicContact" type="tns:xmlDeletePublicContact" />
  <xs:element name="presenceEnforcedUserACL"
type="tns:xmlDeletePresEnforcedUserACLEntry"/>
  <xs:element name="presenceSystemRule" type="tns:xmlDeletePresSystemRule"/>
  <xs:element name="presenceSystemACL" type="tns:xmlDeletePresSystemACLEntry"/>

  <xs:element name="deleteGlobalSettings">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="sharedAddress" type="tns:xmlDeleteSharedAddress"
minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="publicContact" type="tns:xmlDeletePublicContact"
minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="presenceEnforcedUserACL"
type="tns:xmlDeletePresEnforcedUserACLEntry" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="presenceSystemRule" type="tns:xmlDeletePresSystemRule"
minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="presenceSystemACL"
type="tns:xmlDeletePresSystemACLEntry" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="xmlDeleteSharedAddress">
    <xs:sequence>
      <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="xmlDeletePublicContact">
    <xs:sequence>
      <xs:element name="displayName" type="xs:string" maxOccurs="1"
minOccurs="1"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="xmlDeletePresEnforcedUserACLEntry">
    <xs:sequence>
      <xs:element name="userName" type="xs:string" maxOccurs="1" minOccurs="1"/>
    >
      <xs:choice>
        <xs:element name="watcherLoginName" type="xs:string" minOccurs="0"/>
        <xs:element name="watcherDisplayName" type="xs:string" minOccurs="0"/>
      </xs:choice>
      <xs:element name="priority" type="xs:string" maxOccurs="1" minOccurs="1"/>
    >
  </xs:sequence>
</xs:complexType>

```

```

    <xs:complexType name="xmlDeletePresSystemRule">
      <xs:sequence>
        <xs:element name="priority" type="xs:string" maxOccurs="1"
minOccurs="1"/>
      </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlDeletePresSystemACLEntry">
      <xs:sequence>
        <xs:choice>
          <xs:element name="watcherLoginName" type="xs:string" minOccurs="0"/>
          <xs:element name="watcherDisplayName" type="xs:string" minOccurs="0"/>
        </xs:choice>
      </xs:sequence>
    </xs:complexType>
  </xs:schema>

```

### Sample XML for bulk deleting global setting records

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:deleteGlobalSettings xmlns:tns="http://xml.avaya.com/schema/bulkdelete"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
xml.avaya.com/schema/bulkdelete systemPresence_delete.xsd ">

  <tns:presenceSystemRule>
    <tns:priority>LOW</tns:priority>
  </tns:presenceSystemRule>

  <tns:sharedAddress>
    <tns:name>Avaya Pune</tns:name>
  </tns:sharedAddress>

  <tns:publicContact>
    <tns:displayName>John Miller</tns:displayName>
  </tns:publicContact>

  <tns:presenceEnforcedUserACL>
    <tns:userName>jmiller@avaya.com</tns:userName>
    <tns:watcherDisplayName>John Miller</tns:watcherDisplayName>
    <tns:priority>HIGH</tns:priority>
  </tns:presenceEnforcedUserACL>

  <tns:presenceSystemACL>
    <tns:watcherDisplayName>John Miller</tns:watcherDisplayName>
  </tns:presenceSystemACL>
</tns:deleteGlobalSettings>

```

### XML Schema Definition for bulk importing roles

```

<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns="http://xml.avaya.com/bulkimport" xmlns:xs="http://www.w3.org/
2001/XMLSchema" targetNamespace="http://xml.avaya.com/bulkimport"
elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0">
  <xs:annotation>
    <xs:documentation xml:lang="en">
      This Schema defines schema for bulk import and export of roles.
      Root Element 'Roles' represent collection of role (containing 1 or more
roles)
    </xs:documentation>
  </xs:annotation>
  <xs:element name="Roles">
    <xs:complexType>

```

```

    <xs:sequence>
      <xs:annotation>
        <xs:documentation xml:lang="en">
          A role is a collection of access permissions on a resource. A
          user's role will determine the permissions that the user receives to access
          resources. Examples of Roles: Contact Center Manager, Agent, Administrator.
          New Roles can be added to the data model using an XML file
          conforming to this XSD.Existing Roles too can be updated.
        </xs:documentation>
      </xs:annotation>
      <xs:element name="Role" maxOccurs="unbounded">
        <xs:complexType>
          <xs:sequence>
            <xs:annotation>
              <xs:documentation xml:lang="en">
                Operation - Element Containing information
                about the Operation.The Operation requires to preexist in SMGR database.Examples of
                Operation: 'UserManagement/GlobalUserSettings/ACL' ; 'Settings/Plugin Framework' ;
                Resource - Element Containing information about the
                Resource. A Resource can be a User, Role, Operation, Group,Element.The Resource
                requires to preexist in SMGR database.Examples of Resource: 'Auditor' ;
              </xs:documentation>
            </xs:annotation>
            <xs:element name="Operation" minOccurs="0"
maxOccurs="unbounded">
              <xs:complexType>
                <xs:attribute name="ID" type="xs:string"
use="required">
                  <xs:annotation>
                    <xs:documentation xml:lang="en">
                      ID: The ID of the operation.The
                      value of this tag corresponds to the OperationID. Note that it is very important
                      that this value is unique across the system
                    </xs:documentation>
                  </xs:annotation>
                </xs:attribute>
              </xs:complexType>
            </xs:element>
            <xs:element name="Resource" minOccurs="0"
maxOccurs="unbounded">
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="ResourceAttributes"
minOccurs="0" maxOccurs="unbounded">
                    <xs:complexType>
                      <xs:attribute name="ID" type="xs:string"
use="required">
                        <xs:annotation>
                          <xs:documentation xml:lang="en">
                            ResourceAttributesID:
                            The ID of the ResourceAttributes.This specifies the attributes of a
                            resource.Examples of ResourceAttributesID: 'ALL' ; 'LoginName' ;'First Name' for
                            Resource Type 'user'
                          </xs:documentation>
                        </xs:annotation>
                      </xs:attribute>
                    </xs:complexType>
                  </xs:element>
                <xs:element name="Permissions">
                  <xs:complexType>
                    <xs:sequence>
                      <xs:annotation>
                        <xs:documentation xml:lang="en">
                          Permission: String value
                          specifying Permissions that can be assigned to the Resource Type.Examples of

```

```

Permission:view,delete
                                </xs:documentation>
                                </xs:annotation>
                                <xs:element name="Permission"
type="xs:string" maxOccurs="unbounded"/>
                                </xs:sequence>
                                </xs:complexType>
                                </xs:element>
                                </xs:sequence>
                                <xs:attribute name="ResourceType" type="xs:string"
use="required">
                                <xs:annotation>
                                <xs:documentation xml:lang="en">
specifying Type of the Resource that needs to be imported.
                                </xs:documentation>
                                </xs:annotation>
                                </xs:attribute>
                                <xs:attribute name="NativeResourceID"
type="xs:string" use="required">
                                <xs:annotation>
                                <xs:documentation xml:lang="en">
NativeResourceID: Native ID of the Resource.
                                </xs:documentation>
                                </xs:annotation>
                                </xs:attribute>
                                </xs:complexType>
                                </xs:element>
                                </xs:sequence>
                                <xs:attribute name="CanAccessAllOperations" type="xs:boolean"
use="required">
                                <xs:annotation>
                                <xs:documentation xml:lang="en">
CanAccessAllOperations - Boolean value specifying
whether this role can access all operations.
                                </xs:documentation>
                                </xs:annotation>
                                </xs:attribute>
                                <xs:attribute name="IsServices" type="xs:boolean" use=
"required" >
                                <xs:annotation>
                                <xs:documentation xml:lang="en">
IsServices - Boolean value specifying whether
this Role is a Services Role.
                                </xs:documentation>
                                </xs:annotation>
                                </xs:attribute>
                                <xs:attribute name="isDefault" type="xs:boolean"
use="required">
                                <xs:annotation>
                                <xs:documentation xml:lang="en">
isDefault - Boolean value specifying whether
this Role is a System Role.These Roles can not be deleted.
                                </xs:documentation>
                                </xs:annotation>
                                </xs:attribute>
                                <xs:attribute name="Name" type="xs:string" use="required">
                                <xs:annotation>
                                <xs:documentation xml:lang="en">
Name - String value specifying Role name.
                                </xs:documentation>
                                </xs:annotation>
                                </xs:attribute>
                                <xs:attribute name="AllResourcesPermission" type="xs:string"
use="optional">

```

```

        <xs:annotation>
            <xs:documentation xml:lang="en">
                AllResourcesPermission - String value representing
the comma separated permission strings. These permissions will be applied to all
Resources in the system. The users assigned to this role will get the specified
permissions for all resources. Examples of Resource:'view,delete'
            </xs:documentation>
        </xs:annotation>
    </xs:attribute>
    <xs:attribute name="Description" type="xs:string"
use="optional">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                Description - String value specifying Role
description.
            </xs:documentation>
        </xs:annotation>
    </xs:attribute>
    <xs:attribute name="isNHIRole" type="xs:boolean"
use="required">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                isNHIRole - Boolean value specifying whether
this Role is a non human interface (nhi) role.
            </xs:documentation>
        </xs:annotation>
    </xs:attribute>
    <xs:attribute name="shareRoles" type="xs:boolean"
use="optional">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                shareRoles - Boolean value specifying whether this
Role is a shared role across applications.
            </xs:documentation>
        </xs:annotation>
    </xs:attribute>
    <xs:attribute name="hasFullAccess" type="xs:boolean"
use="optional">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                hasFullAccess - Boolean value specifying
full access over all resources.Examples of Role with full access : 'System
Administrator' ;
            </xs:documentation>
        </xs:annotation>
    </xs:attribute>
    <xs:attribute name="ApplicationId" type="xs:string"
use="required">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ApplicationId - The value of this tag
corresponds to the ApplicationID.Examples of ApplicationId: 'SMGR' ;
            </xs:documentation>
        </xs:annotation>
    </xs:attribute>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>

```

## Sample XML for bulk importing roles

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Root Element 'Roles' represent collection of role (containing 1 or more
roles)-->
<Roles xsi:schemaLocation="http://xml.avaya.com/bulkimport BulkImport.xsd"
xmlns="http://xml.avaya.com/bulkimport" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
  <!-- A role is a collection of access permissions on a resource. A user's role
will determine the permissions that the user receives to access resources.
  CanAccessAllOperations: Boolean value specifying whether this role can access
all operations.
  IsServices: Boolean value specifying whether this Role is a Services Role.
  isDefault: Boolean value specifying whether this Role is a System Role.These
Roles can not be deleted.
  Name: String value specifying Role name.
  AllResourcesPermission:String value representing the comma separated permission
strings. These permissions will be applied to all Resources in the system. The users
assigned to this role will get the specified permissions for all resources.
  Description:String value specifying Role description.
  isNHIRole:Boolean value specifying whether this Role is a non human interface
(nhi) role.
  shareRoles: Boolean value specifying whether this Role is a shared role across
applications.
  hasFullAccess:Boolean value specifying full access over all resources.
  ApplicationId:The value of this tag corresponds to the ApplicationID.Examples
of ApplicationId: 'SMGR'
-->
  <Role CanAccessAllOperations="true" IsServices="true" isDefault="false"
Name="test-role" AllResourcesPermission="view,delete" Description="System
Administrator Role" isNHIRole="false" shareRoles="true"
hasFullAccess="false" ApplicationId="SMGR" >
    <!--Element Containing information about the Operation.The Operation requires
to preexist in SMGR database.
  ID: The ID of the operation.The value of this tag corresponds to the OperationID.
Note that it is very important that this value is unique across the system -->
    <Operation ID="GroupsAndRoles/RBAC/ViewRole"/>
    <!--Resource : Element Containing information about the Resource. A
Resource can be a User, Role, Operation, Group,Element.The Resource requires to
preexist in SMGR database.
  ResourceType: String Value for specifying Type of the Resource that
needs to be imported.
  NativeResourceID: Native ID of the Resource. -->
    <Resource ResourceType="alarmoperation"
NativeResourceID="ChangeStatusAll">
      <!-- ResourceAttributesID: The ID of the ResourceAttributes.This
specifies the attributes of a resource -->
      <ResourceAttributes ID="ALL" />
      <!--Permission: String value specifying Permissions that can be assigned
to the Resource Type.-->
      <Permissions>
        <Permission>view</Permission>
      </Permissions>
    </Resource>
  </Role>
</Roles>
```

## Attribute details defined in the Import user XSD

| Attribute          | Attribute Description   | Mandatory/Optional | Validation Constraints             |
|--------------------|---|--------------------|------------------------------------|
| authenticationType | This defines the type of authentication that this user will undergo at runtime to obtain access to the system.  | Mandatory          | Possible Values: BASIC, ENTERPRISE |
| description        | A text description of the user. Human readable description of this user instance.   | Optional           |                                    |
| displayName        | The localized name of a user to be used when displaying. It will typically be the localized full name. This value may be provisioned from the user's enterprise directory entry. If it does not exist, synchronization rules can be used to populate it for other fields e.g. Surname, GivenName, or LoginName. | Optional           |                                    |
| displayNameAscii   | The full text name of the user represented in ASCII. It is used to support display (e.g. endpoints) that cannot handle localized text.  | Optional           |                                    |
| dn                 | The distinguished name of the user. The DN is a sequence of relative distinguished names (RDN) connected by commas. An RDN is an attribute with an associated value in  | Optional           |                                    |

| Attribute                | Attribute Description   | Mandatory/Optional | Validation Constraints  |
|--------------------------|---|--------------------|-------------------------|
|                          | <p>the form of attribute=value, normally expressed in a UTF-8 string format. The dn can be used to identify the user and may be used for authentication subject mapping. Note the dn is changeable.</p>   |                    |                         |
| isDuplicatedLoginAllowed | <p>A boolean indicator showing whether this user is allowed a duplicate concurrent logins. A true stipulates that the user is allowed to have duplicate logins.</p>   | Optional           | Default value is true.  |
| isEnabled                | <p>A boolean indicator showing whether or not the user is active. Users with AuthenticationType=Basic will fail if this value is false. This attribute can be used to disable access between login attempts. A running session's login will not be revocable. Alternatively the administrator can always modify the password to disable the user from logging in. A true stipulates this is an active user, a false used for a disabled user.</p> | Optional           | Default value is false. |
| isVirtualUser            | <p>A boolean indicator showing whether or not the record is being used for a non-</p>   | Optional           | Default value is false. |

| Attribute | Attribute Description   | Mandatory/ Optional | Validation Constraints |
|-----------|---|---------------------|------------------------|
|           | <p>human entity such as an application, service, software agent, etc. This is to be used where the entity will behave as a user and needs to have subset of the user profile populated. If the entity does not behave as a user and has a different trust relationship e.g. a trust certificate it should not be treated as a virtual user. A virtual user can represent an Avaya or external non-human entity. This attribute is provided as a convenience to track such accounts. A true stipulates this is a virtual users, a false is used for human users.</p> |                     |                        |
| givenName | The first name of the user.   | Mandatory           |                        |
| honorific | The personal title used to address a user. This is typically a social title and not the work title which is contained in the title attribute. This attribute can map to "PersonalTitle".  | Optional            |                        |
| loginName | This is the unique system login name given to the user. It can take the form of username@domain or just   | Mandatory           |                        |

| Attribute          | Attribute Description   | Mandatory/Optional | Validation Constraints |
|--------------------|---|--------------------|------------------------|
|                    | <p>username. This may vary across customers. It can be used to help provision default user handles in the CSHandle table. The username is an alphanumeric value that must comply with the userinfo related portion of a URI as described in rfc2396. However, it is further restricted as ASCII characters with only the "_" and "." special characters supported. This is the rfc2798 "uid" attribute.</p> |                    |                        |
| middleName         | <p>The middle name of the user.</p>   | Optional           |                        |
| managerName        | <p>Text name of the user's manager. This is a free formed field and does not require the user's manager to also be a user of the solution. This attribute was requested to support reporting needs.</p>   | Optional           |                        |
| preferredGivenName | <p>The preferred first name of the user.</p>  | Optional           |                        |
| preferredLanguage  | <p>The individual's preferred written or spoken language. Values will conform to rfc4646. Refer to rfc4646 for syntax. This format uses the ISO standard Language (ISO-639) and region (ISO-3166) codes In</p>  | Optional           |                        |

| Attribute     | Attribute Description  | Mandatory/Optional | Validation Constraints  |
|---------------|--|--------------------|---|
|               | the absence of a value the client's locale should be used, if no value is set, en-US should be defaulted.  |                    |   |
| source        | Free format text field that identifies the entity that created this user record. The format of this field will be either a IP Address/Port or a name representing an enterprise LDAP or Avaya.   | Optional           | User Management will populate the source field with the name of the file. |
| sourceUserKey | The key of the user from the source system. If the source is an Enterprise Active Directory server, this value will be the objectGUID.   | Optional           | By default the value for will be "none"                                   |
| status        | This information is to help manage provisioning activities such as correcting or completing the provisioning of a user instance. It can also signify that approval is needed (PENDINGAUTHZ) before a user account is sufficiently configured to be a valid user (PROVISIONED). | Optional           | Possible Values:<br>AUTHPENDING;<br>PENDINGAUTHZ;<br>PROVISIONED          |
| suffix        | The text appended to a name e.g. Jr., III.   | Optional           |   |
| surname       | The user's last name, also called the family name.   | Mandatory          |   |

| Attribute | Attribute Description   | Mandatory/Optional | Validation Constraints   |
|-----------|---|--------------------|--|
| timeZone  | <p>The preferred time zone of the user. For example: America/New_York, Europe/Dublin. The application consuming this information would need to know how to translate e.g. in Java it would be <code>TimeZone.getTimeZone("Europe/Moscow");</code> In the absence of a value the local services timezone will be used.</p> | Optional           | <p>(-12:00) International Date Line West<br/>           (-11:00) Midway Island, Samoa<br/>           (-10:00) Hawaii<br/>           (-09:00) Alaska<br/>           (-08:00) Pacific Time (US &amp; Canada);<br/>           Tijuana (-07:00)<br/>           Arizona (-07:00)<br/>           Mountain Time (US &amp; Canada);<br/>           Chihuahua, La Paz (-06:00)<br/>           Central America;<br/>           Saskatchewan (-06:00)<br/>           Central Time (US &amp; Canada);<br/>           Guadalajara, Mexico City (-05:00)<br/>           Indiana (East); Bogota, Lima, Quito (-05:00)<br/>           Eastern Time (US &amp; Canada) (-04:00)<br/>           Caracas, La Paz (-04:00)<br/>           Atlantic Time (Canada);<br/>           Santiago, Manaus (-03:30)<br/>           Newfoundland (-03:00)<br/>           Georgetown (-03:00)<br/>           Brasilia, Greenland, Buenos Aires, Montevideo (-02:00)<br/>           Mid-Atlantic (-01:00)<br/>           Cape Verde Is. (-01:00)<br/>           Azores (+00:00)<br/>           Monrovia, Reykjavik (+00:00)<br/>           GMT : Dublin, Edinburgh, Lisbon, London, Casablanca (+01:00)<br/>           West Central Africa (+01:00)<br/>           Amsterdam, Berlin, Rome, Belgrade, Prague, Brussels,</p> |

| Attribute | Attribute Description | Mandatory/ Optional | Validation Constraints  |
|-----------|-----------------------|---------------------|---|
|           |                       |                     | Sarajevo (+02:00)<br>Harare, Pretoria<br>(+02:00) Amman,<br>Athens, Minsk,<br>Beirut, Cairo,<br>Jerusalem, Helsinki,<br>Windhoek (+03:00)<br>Moscow, St.<br>Petersburg,<br>Volgograd (+03:00)<br>Baghdad, Kuwait,<br>Riyadh, Nairobi,<br>Tbilisi (+03:30)<br>Tehran (+04:00) Abu<br>Dhabi, Muscat,<br>Caucasus Standard<br>Time (+04:00) Baku,<br>Tbilisi, Yerevan<br>(+04:30) Kabul<br>(+05:00) Islamabad,<br>Karachi, Tashkent,<br>Ekaterinburg<br>(+05:30) Chennai,<br>Kolkata, Mumbai,<br>New Delhi, Sri<br>Jayawardenepura<br>(+05:45) Kathmandu<br>(+06:00) Astana,<br>Dhaka, Almaty,<br>Novosibirsk (+06:30)<br>Rangoon (+07:00)<br>Bangkok, Hanoi,<br>Jakarta, Krasnoyarsk<br>(+08:00) Perth;<br>Irkutsk, Ulaan Bataar<br>(+08:00) Beijing,<br>Hong Kong,<br>Singapore; Taipei<br>(+09:00) Seoul,<br>Osaka, Sapporo,<br>Tokyo (+09:00)<br>Yakutsk (+09:30)<br>Darwin, Adelaide<br>(+10:00) Brisbane,<br>Guam, Port Moresby<br>(+10:00) Canberra,<br>Melbourne, Sydney,<br>Hobart, Vladivostok |

| Attribute    | Attribute Description  | Mandatory/Optional | Validation Constraints  |
|--------------|--|--------------------|---|
|              |  |                    | (+11:00) Magadan, Solomon Is., New Caledonia (+12:00) Fiji, Kamchatka, Marshall Is. (+12:00) Auckland, Wellington (+13:00) Nuku'alofa |
| title        | The job function of a person in their organizational context.  | Optional           |   |
| userName     | This is the username portion of the loginName field. It is an alphanumeric value that must comply with the userinfo related portion of a URI as described in rfc2396. However, it is further restricted as ASCII characters with only the "_" and "." special characters supported. This is the rfc2798 "uid" attribute. | Mandatory          |   |
| userPassword | The encrypted password for this user's account. A null password is used when the user is authenticated by the enterprise such as with a separate source such as the enterprise LDAP.   | Optional           | Need not specified value for Enterprise User. If the value is not specified for the Basic user, the user will be disabled.            |
| commPassword | The encrypted "subscriber" or communication password with which the user logs can use to authentication with on to any CommProfile SIP   | Optional           |   |

| Attribute         | Attribute Description   | Mandatory/Optional | Validation Constraints   |
|-------------------|---|--------------------|--|
|                   | and non SIP. This attribute is meant to be a shared across different communication profiles and thus different communication services.  |                    |  |
| userType          | This enumerates the possible primary user application types. A User can be associated with multiple user types.   | Optional           | Possible values are administrator, communication_user, agent, supervisor, resident_expert, service_technician, lobby_phone |
| roles             | Text name of a role. This value needs to pre-exist in SMGR DB.  | Optional           |  |
| address           | The address of the user.  | Optional           |  |
| securityIdentity  | The SecurityIdentity is used to hold any additional identities for a user that can be used for authentication such as their loginName, Kerberos account name, or their X509 certificate name. | Optional           |  |
| ownedContactLists | It is a collection of internal or external contacts. ContactList is owned by a specific user and has a name that a unique name within the context of its owner.                               | Optional           | A default contactlist per user will be created.  |
| ownedContacts     | It represents a non Avaya application user (external) contact. Contacts can be collected  | Optional           |  |

| Attribute             | Attribute Description   | Mandatory/Optional | Validation Constraints |
|-----------------------|---|--------------------|------------------------|
|                       | together along with User entities into a contact list. Contacts can be created by an administrator or an end user.  |                    |                        |
| presenceUserDefault   | These are personal rules that are set by presentities to define how much presence information can be shown to watchers that are not explicitly mentioned in an ACL. There may be one User Default rule per presentity (User), or none.        | Optional           |                        |
| presenceUserACL       | These are personal rules defined by presentities themselves on who can monitor their presence information. There may be several entries in the list for a given presentity, each entry corresponding to one watcher.                          | Optional           |                        |
| presenceUserCLDefault | This is a personal rule that is set by presentities to define how much presence information can be shown to watchers that belong to the user's contact list. There may be one User Contact List Default rule per presentity (Person) or none. | Optional           |                        |

| Attribute      | Attribute Description  | Mandatory/ Optional | Validation Constraints                      |
|----------------|--|---------------------|---|
| commProfileSet | A user will have a default Commprofile set. A commprofile set can exist without any handles or commprofiles referencing it. I.e. you can create a commprofile set without needing to also create either a handle or a commprofile. A commprofile set can contain multiple commprofiles, but only one of each specific type. This is enforced by having the CommProfile uniqueness constraint include type, commprofile_set_id. | Optional            | A user will have a default commprofile set. |

### Attribute details defined in the Delete User XSD

| Attribute  | Attribute Description   | Mandatory/ Optional | Validation Constraints        |
|------------|---|---------------------|-------------------------------|
| deleteType | This defines the delete type of the user. If the enduser selects "soft" the user record will not be permanent deleted. This can be recovered. For permanent delete all attributes associated with the user gets deleted. The links to public contacts, shared addresses gets deleted. | Mandatory           | Possible Values: soft; delete |

| Attribute | Attribute Description  | Mandatory/ Optional | Validation Constraints  |
|-----------|--|---------------------|---|
| loginName | This is the unique system login name given to the user. It can take the form of username@domain or just username.  | Mandatory           |   |
| id        | This is the unique identifier for a user record. The field is optional. This has been added in the XSD keeping in mind future enhancement. This is not being used in System Manager 6.0 release. | Optional            | In earlier version of System Manager 6.0, the id tag was not made optional, hence incase of an error such as, <i>"Failed to parse XML user: cvccomplex- type. 2.4.b: The content of element 'tns:user' is not complete. One of '{'http://xml.avaya.com/schema/bulkdelete': id}' is expected. invalid XML file"</i> is thrown , use a dummy value for the id "1234". |

### Attribute details defined in the Endpoint profile XSD

#### Attribute details defined in the Endpoint profile XSD

| Attribute                                      | Attribute Description  | Mandatory/ Optional | Validation Constraints |
|--|--|---------------------|------------------------|
| CM Name<br>cmName                              | CM Name as it appears under 'Applications/ Application Management/ Entities                      | Mandatory           |                        |
| Use Existing Extension<br>useExistingExtension | 'true' if already created extension is to be used. 'false' if available extension is to be used. | Optional            |                        |

| Attribute                 | Attribute Description  | Mandatory/Optional | Validation Constraints  |
|---------------------------|--|--------------------|---|
| Template Name<br>template | Template name to be used to create station. Values defined in Template will be used if not provided. | Optional           |   |
| Set Type<br>setType       | Specifies the set type of the station  | Optional           |   |
| Port<br>port              | Valid values for port  | Optional           | <p>01 to 64 First and second numbers are the cabinet number A to E Third character is the carrier 01 to 20 Fourth and fifth characters are the slot number 01 to 32 Sixth and seventh characters are the circuit number x or X Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) stations, as well as for SBS Extensions. IP Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the</p> |

| Attribute  | Attribute Description   | Mandatory/ Optional | Validation Constraints  |
|--|---|---------------------|---|
|  |   |                     | extension would have an IP set. This is automatically entered for certain IP station set types, but you can enter for a DCP set with softphone permissions. This changes to the s00000 type when the set registers. |
| Delete station is unassigned<br>deleteOnUnassign | Whether the station should be deleted if it unassigned from the user.   | Optional            |   |
| Lock messages feature.<br>lockMessages           | Enable/ Disable lock messages feature.  | Optional            | true/false to enable/disable lock messages feature.   |
| Coverage Path 1<br>coveragePath1                 | A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call.   | Optional            | Valid values: Path Number between 1-2000, time of day table, t1-t999, or blank.   |
| Coverage Path 2                                  | A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call.   | Optional            | Valid values: Path Number between 1-2000, time of day table, t1-t999, or blank.   |
| Hunt To Station<br>huntToStation                 | The extension the system should hunt to for this telephone when the telephone is busy. A station hunting chain can be created by assigning a hunt-to station to a series of telephones. | Optional            |   |
| Tenant Number<br>tn                              | Provides for partitioning of attendant groups and/or stations and trunk groups.   | Optional            | Valid values: 1 to 100  |

| Attribute   | Attribute Description  | Mandatory/Optional | Validation Constraints   |
|---|--|--------------------|--|
|   | Typically this is used for multiple tenants in a building or multiple departments within a company or organization.  |                    |  |
| Class of Restriction<br>cor                                 | This is used for multiple tenants in a building or multiple departments within a company or organization.<br>This is used for multiple tenants in a building or multiple departments within a company or organization. | Optional           | Valid values: 0 to 995   |
| Class of Service<br>cos                                     | Class of Service lets you define groups of users and control those groups' access to features.   | Optional           | Valid values: 1 to 15  |
| speakerphone  | Controls the behavior of speakerphones.  | Optional           | Valid values : none, 1-way, 2-way  |
| Display Language<br>displayLanguage                         | The language that displays on stations.  | Optional           | Time of day is displayed in 24- hour format (00:00 - 23:59) for all languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.). unicode: Displays English messages in a 24- hour format . If no Unicode file is installed, displays messages in English by default. |
| Personalized Ringing Pattern<br>personalizedRinging Pattern | Defines the personalized ringing pattern for the station.  |                    | L = 530 Hz, M = 750 Hz, and H = 1060 Hz<br>Valid Entries Usage:  |

| Attribute  | Attribute Description   | Mandatory/Optional | Validation Constraints   |
|--|---|--------------------|--|
|  | <p>Personalized Ringing allows users of some telephones to have one of 8 ringing patterns for incoming calls. For virtual stations, this field dictates the ringing pattern on its mapped to physical telephone.</p>  |                    | <ol style="list-style-type: none"> <li>1. MMM (standard ringing)</li> <li>2. HHH</li> <li>3. LLL</li> <li>4. LHH</li> <li>5. HHL</li> <li>6. HLL</li> <li>7. HLH</li> <li>8. LHL</li> </ol>  |
| <p>Message Lamp Extension<br/>messageLampExt</p>   | <p>The Message Lamp Extension associated with the current extension.</p>  | <p>Optional</p>    |  |
| <p>muteButtonEnabled</p>                           | <p>Enables or disables the mute button on the station.</p>  |                    |  |
| <p>Media Complex Extension<br/>mediaComplexExt</p> | <p>When used with Multi-media Call Handling, indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to place either a voice or a data call, and voice conversion, coverage, and forwarding apply as if the call were made to the 1-number.</p> | <p>Optional</p>    | <p>Valid Entry Usage A valid BRI data extension For MMCH, enter the extension of the data module that is part of this multimedia complex. H.323 station extension For 4600 series IP Telephones, enter the corresponding H.323 station. For IP Softphone, enter the corresponding H.323 station. If you enter a value in this field, you can register this station for either a road-warrior or elecommuter/Avaya IP Agent application. blank Leave this field blank for single-</p> |

| Attribute                                       | Attribute Description  | Mandatory/Optional | Validation Constraints   |
|---|--|--------------------|--|
|   |  |                    | connect IP applications.   |
| IP Softphone<br>ipSoftphone                     | Whether this is IP soft phone.   | Optional           |  |
| Survivable GK Node Name<br>survivableGkNodeName | Survivable GK Node Name Identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the H.248 gateways. When a valid IP node name is entered into this field, Communication Manager adds the IP address of this gateway to the bottom of the Alternate Gatekeeper List for this IP network region. As H.323 IP stations register with Communication Manager, this list is sent down in the registration confirm message. This allows the IP station to use the IP address of this Survivable Gatekeeper as the call controller of last resort to register with. Available only if the station type is an H.323 station (46xx or 96xx models). | Optional           | Valid Entry Usage<br>Valid IP node name<br>Any valid previously-administered IP node name. |

| Attribute   | Attribute Description  | Mandatory/Optional | Validation Constraints   |
|---|--|--------------------|--|
| Survivable class of restriction<br>survivableCOR    | Sets a level of restriction for stations to be used with the survivable dial plan to limit certain users to only to certain types of calls. You can list the restriction levels in order from the most restrictive to least restrictive. Each level assumes the calling ability of the ones above it. This field is used by PIM module of the Integrated Management to communicate with the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for Standard Local Survivability (SLS) on the H.248 gateways. Available for all analog and IP station types. | Optional           | Valid Entries Usage<br>emergency - This station can only be used to place emergency calls.<br>Internal - This station can only make intra-switch calls. This is the default.<br>local - This station can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables.<br>toll - This station can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables.<br>unrestricted - This station can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users. |
| Survivable Trunk Destination<br>survivableTrunkDest | Designates certain telephones as not being allowed to receive incoming trunk calls when the Media Gateway is in survivable mode. This field is used by the PIM module of the Integrated Management to successfully   | Optional           | Valid Entry Usage:<br>true - Allows this station to be an incoming trunk destination while the Media Gateway is running in survivability mode. This is the default.<br>false - Prevents this station from receiving incoming trunk calls   |

| Attribute  | Attribute Description   | Mandatory/Optional | Validation Constraints   |
|--|---|--------------------|--|
|  | interrogate the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for SLS on the H.248 gateways. Available for all analog and IP station types. |                    | when in survivable mode.   |
| Voice Mail Number<br>voiceMailNumber                 | Enter the complete Voice Mail Dial Up number.   | Optional           | String   |
| offPremisesStation                                   | Analog telephones only.   | Optional           | Valid entries Usage:<br><ul style="list-style-type: none"> <li>• true - Enter true if this telephone is not located in the same building with the system. If you enter true, you must complete R Balance Network.</li> <li>• false - Enter false if the telephone is located in the same building with the system.</li> <li>•</li> </ul> |
| dataOption   | If a second line on the telephone is administered on the I-2 channel, enter analog. Otherwise, enter data module if applicable or none.   | Optional           | Valid entries analog, none.  |
| Message Waiting Indicator<br>messageWaitingIndicator | If led or neon, then messageLampExt should be enable otherwise its blank.   | Optional           | Valid entries: led, neon, none.  |

| Attribute            | Attribute Description   | Mandatory/Optional | Validation Constraints  |
|----------------------|---|--------------------|---|
| remoteOfficePhone    | Enter true to use this station as an endpoint in a remote office configuration.   | Optional           | Valid entries: <ul style="list-style-type: none"> <li>• audix - If LWC is attempted, the messages are stored in AUDIX.</li> <li>• spe - If LWC is attempted, the messages are stored in the system processing element (spe).</li> <li>• none - If LWC is attempted, the messages are not stored.</li> </ul> |
| lwcActivation        | Enter true to allow internal telephone users to leave short LWC messages for this extension. If the system has hospitality, enter true for guest-room telephones if the extension designated to receive failed wakeup messages should receive LWC messages that indicate the wakeup calls failed. Enter true if LWC Reception is audix. | Optional           | Boolean   |
| activeStationRinging | Active station Ringing  | Optional           | Valid entries: <ul style="list-style-type: none"> <li>• single</li> <li>• continuous</li> <li>• if-busy-single</li> <li>• silent</li> </ul>   |
| idleActiveRinging    | Defines how call rings to the   | Optional           | Valid entries <ul style="list-style-type: none"> <li>• continuous - Enter continuous to</li> </ul>  |

| Attribute          | Attribute Description  | Mandatory/Optional | Validation Constraints  |
|--------------------|--|--------------------|---|
|                    | telephone when it is on-hook.  |                    | <p>cause all calls to this telephone to ring continuously.</p> <ul style="list-style-type: none"> <li>• if-busy-single - Enter if-busysingle to cause calls to this telephone to ring continuously when the telephone is off-hook and idle and calls to this telephone to receive one ring cycle and then ring silently when the telephone is off-hook and active.</li> <li>• silent-if-busy - Enter silent-if-busy to cause calls to ring silently when this station is busy.</li> <li>• single - Enter single to cause calls to this telephone to receive one ring cycle and then ring silently.</li> </ul> |
| switchhookFlash    | Must be set to true when the Type field is set to H.323  | Optional           | Boolean   |
| ignoreRotaryDigits | If this field is true, the short switch-hook flash (50 to 150) from a 2500-type set is ignored.                        | Optional           | Boolean   |
| h320Conversion     | H.320 Conversion — Valid entries are true and false (default). This field is optional for non-multimedia complex voice | Optional           | Boolean   |

| Attribute       | Attribute Description   | Mandatory/Optional | Validation Constraints            |
|-----------------|---|--------------------|-----------------------------------|
|                 | <p>stations and for Basic multimedia complex voice stations. It is mandatory for Enhanced multimedia complex voice stations. Because the system can only handle a limited number of conversion calls, you might need to limit the number of telephones with H.320 conversion. Enhanced multimedia complexes must have this flag set to true.</p>  |                    |                                   |
| serviceLinkMode | <p>The service link is the combined hardware and software multimedia connection between an Enhanced mode complex's H.320 DVC system and the Avaya DEFINITY Server which terminates the H.320 protocol. A service link is never used by a Basic mode complex H.320 DVC system. Connecting a service link will take several seconds. When the service link is connected, it uses MMI, VC and system timeslot resources. When the service link is disconnected it does not tie up any resources. The Service Link Mode</p> | Optional           | Valid entries as-needed permanent |

| Attribute | Attribute Description   | Mandatory/ Optional | Validation Constraints |
|-----------|---|---------------------|------------------------|
|           | <p>can be administered as either 'as-needed' or 'permanent' as described below: -</p> <p>As- Needed - Most non-call center multimedia users will be administered with this service link mode. The as-needed mode provides the Enhanced multimedia complex with a connected service link whenever a multimedia call is answered by the station and for a period of 10 seconds after the last multimedia call on the station has been disconnected. Having the service link stay connected for 10 seconds allows a user to disconnect a multimedia call and then make another multimedia call without having to wait for the service link to disconnect and re-establish. -</p> <p>Permanent – Multimedia call center agents and other users who are constantly making or receiving multimedia calls might want to be administered with this service link mode.</p> |                     |                        |

| Attribute         | Attribute Description   | Mandatory/Optional | Validation Constraints  |
|-------------------|---|--------------------|---|
|                   | <p>The permanent mode service link will be connected during the station's first multimedia call and will remain in a connected state until the user disconnects from their PC's multimedia application or the Avaya DEFINITY Server restarts. This provides a multimedia user with a much quicker video cut-through when answering a multimedia call from another permanent mode station or a multimedia call that has been early answered.</p> |                    |   |
| multimediaMode    | <p>There are two multimedia modes, Basic and Enhanced,</p>  | Optional           | <p>Basic - A Basic multimedia complex consists of a BRI-connected multimedia-equipped PC and a non-BRI-connected multifunction telephone set.<br/>Enhanced - An Enhanced multimedia complex consists of a BRI-connected multimedia-equipped PC and a non-BRI-connected multifunction telephone.</p> |
| mwiServedUserType | <p>Controls the auditing or interrogation of a served user's</p>  | Optional           | <p>Valid entries:<br/>1. fp-mwi - Use if the station is a</p>   |

| Attribute      | Attribute Description   | Mandatory/ Optional | Validation Constraints  |
|----------------|---|---------------------|---|
|                | message waiting indicator (MWI).  |                     | <p>served user of an fp-mwi message center.</p> <p>2. qsig-mwi - Use if the station is a served user of a qsig-mwi message center.</p> <p>3. blank - Leave blank if you do not want to audit the served user's MWI or if the user is not a served user of either an fp-mwi or qsigmwi message center.</p> |
| audixName      | The AUDIX associated with the station. Must contain a user-defined adjunct name that was previously administered.   | Optional            | String  |
| automaticMoves | Automatic Moves allows a DCP telephone to be unplugged from one location and moved to a new location without additional Communication Manager administration. Communication Manager automatically associates the extension to the new port. | Optional            | <p>Valid entries:</p> <p>1. always - Enter always and the DCP telephone can be moved anytime without additional administration by unplugging from one location and plugging into a new location.</p> <p>2. once - Enter once and the DCP telephone can be unplugged and plugged into a</p>                |

| Attribute | Attribute Description | Mandatory/Optional | Validation Constraints   |
|-----------|-----------------------|--------------------|--|
|           |                       |                    | <p>new location once. After a move, the field is set to done the next time that routine maintenance runs on the DCP telephone. Use once when moving a large number of DCP telephones so each extension is removed from the move list. Use once to prevent automatic maintenance replacement.</p> <p>3. no - Enter no to require administration in order to move the DCP telephone.</p> <p>4. done - Done is a display-only value. Communication Manager sets the field to done after the telephone is moved and routine maintenance runs on the DCP telephone.</p> <p>5. Error - Error is a display-only value. Communication Manager sets the field to error,</p> |

| Attribute                     | Attribute Description   | Mandatory/Optional | Validation Constraints   |
|-------------------------------|---|--------------------|--|
|                               |   |                    | <p>after routine maintenance runs on the DCP telephone, when a non-serialized telephone is set as a movable telephone.</p>   |
| remoteSoftphoneEmergencyCalls | <p>An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks.</p> | Optional           | <p>Valid entries:</p> <ol style="list-style-type: none"> <li>1. As-on-local - as-on-local sends the extension entered in the Emergency Location Extension field in the Station screen to the Public Safety Answering Point (PSAP)</li> <li>2. Block - Enter block to prevent the completion of emergency calls.</li> <li>3. Cesid - Enter cesid to allow Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP.</li> <li>4. Option - Enter option to allow the user to select the option (extension, block, or cesid) that the user selected during registration and</li> </ol> |

| Attribute             | Attribute Description  | Mandatory/Optional | Validation Constraints     |
|-----------------------|--|--------------------|----------------------------|
|                       |  |                    | the IP Softphone reported. |
| emergencyLocation Ext | <p>This field allows the system to properly identify the location of a caller who dials a 911 emergency call from this station. An entry in this field must be of an extension type included in the dial plan, but does not have to be an extension on the local system. It can be a UDP extension. The entry defaults to blank. A blank entry typically would be used for an IP softphone dialing in through PPP from somewhere outside your network. If you populate the IP Address Mapping screen with emergency numbers, the feature functions as follows: If the Emergency Location Extension field in the Station screen is the same as the Emergency Location Extension field in the IP Address Mapping screen, the feature sends the extension to the Public Safety Answering Point (PSAP). If the Emergency Location Extension field in the Station screen is different from the Emergency Location</p> | Optional           |                            |

| Attribute                   | Attribute Description  | Mandatory/Optional | Validation Constraints |
|-----------------------------|--|--------------------|------------------------|
|                             | Extension field in the IP Address Mapping screen, the feature sends the extension in the IP Address Mapping screen to the Public Safety Answering Point (PSAP).  |                    |                        |
| alwaysUse                   | A softphone can register no matter what emergency call handling settings the user has entered into the softphone. If a softphone dials 911, the administered Emergency Location Extension is used. The softphone's user-entered settings are ignored. If an IP telephone dials 911, the administered Emergency Location Extension is used. If a call center agent dials 911, the physical station extension is displayed, overriding the administered LoginID for ISDN Display . Does not apply to SCCAN wireless telephones, or to extensions administered as type h.323. | Optional           | Boolean                |
| precedenceCallWaiting       | Activates or deactivates Precedence Call Waiting for this station.   | Optional           |                        |
| autoSelectAnyIdleAppearance | Enables or disables automatic selection  | Optional           | Boolean                |

| Attribute            | Attribute Description   | Mandatory/Optional | Validation Constraints   |
|----------------------|---|--------------------|--|
|                      | <p>of any idle appearance for transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being transferred or conferenced has. If that attempt fails, Optional Boolean Communication Manager selects the first idle appearance.</p> <p>coverageMsgRetrieval</p> |                    |  |
| coverageMsgRetrieval | <p>Allows or denies users in the telephone's Coverage Path to retrieve Leave Word Calling (LWC) messages for this telephone. Applies only if the telephone is enabled for LWC Reception.</p>  | Optional           | Boolean  |
| autoAnswer           | <p>In EAS environments, the auto answer setting for the Agent LoginID can override a station's setting when an agent logs in.</p>   | Optional           | <p>Valid entries:</p> <ol style="list-style-type: none"> <li>1. all: All ACD and non-ACD calls terminated to an idle station cut through immediately. Does not allow automatic hands-free answer for intercom calls. With non-ACD calls, the set is also rung while</li> </ol> |

| Attribute | Attribute Description | Mandatory/Optional | Validation Constraints   |
|-----------|-----------------------|--------------------|--|
|           |                       |                    | <p>the call is cut through. The ring can be prevented by activating the ringer-off feature button when the Allow Ringer-off with Auto-Answer is enabled for the system.</p> <p>2. acd: Only ACD split /skill calls and direct agent calls to auto answer. Non-ACD calls terminated to a station ring audibly. For analog stations, the station is off-hook and idle, only the ACD split/skill calls and direct agent calls auto answer; non-ACD calls receive busy treatment. If the station is active on an ACD call and a non-ACD call arrives, the Agent receives call-waiting tone.</p> <p>3. none: All calls terminated to this station receive an audible ringing treatment.</p> <p>4. icom: Allows a telephone user</p> |

| Attribute                | Attribute Description  | Mandatory/Optional | Validation Constraints  |
|--------------------------|--|--------------------|---|
|                          |  |                    | to answer an intercom call from the same intercom group without pressing the intercom button.   |
| dataRestriction          | Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Cannot be assigned if Auto Answer is administered as all or acd. If enabled, whisper page to this station is denied. | Optional           |   |
| idleAppearancePreference | Indicates which call appearance is selected when the user lifts the handset and there is an incoming call.   | Optional           | true - The user connects to an idle call appearance instead of the ringing call.<br>false - The Alerting Appearance Preference is set and the user connects to the ringing call appearance. |
| callWaitingIndication    | enable/disable call waiting for this station   | Optional           |   |
| attCallWaitingIndication | Attendant call waiting allows attendant-originated or attendant-extended calls to a busy single-line   | Optional           | Boolean   |

| Attribute               | Attribute Description   | Mandatory/Optional | Validation Constraints  |
|-------------------------|---|--------------------|---|
|                         | telephone to wait and sends distinctive call-waiting tone to the single-line user. Enable/disable attendant call waiting  |                    |   |
| distinctiveAudibleAlert | Enter true so the telephone can receive the 3 different types of ringing patterns which identify the type of incoming calls. Distinctive ringing might not work properly for off-premises telephones. | Optional           |   |
| restrictLastAppearance  |   | Optional           | Valid entries:<br><ol style="list-style-type: none"> <li>1. true: Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only.</li> <li>2. false: Last idle call appearance is used for incoming priority calls and outgoing call originations.</li> </ol> |
| adjunctSupervision      | Enable / Disable adjunct Supervision.   | Optional           | Valid entries:<br><ol style="list-style-type: none"> <li>1. true: Analog disconnect signal is sent automatically to the port after a call terminates. Analog devices (such as answering machines and</li> </ol>   |

| Attribute                       | Attribute Description | Mandatory/Optional | Validation Constraints   |
|---------------------------------|-----------------------|--------------------|--|
|                                 |                       |                    | <p>speakerphones) use this signal to turn the devices off after a call terminates.</p> <p>2. false: Hunt group agents are alerted to incoming calls. In a hunt group environment, the disconnect signal blocks the reception of zip tone and incoming call notification by an auto-answer station when a call is queued for the station.</p>   |
| perStationCpnSend CallingNumber | Send Calling Number.  | Optional           | <p>Valid entries:</p> <ol style="list-style-type: none"> <li>1. y: All outgoing calls from the station will deliver the Calling Party Number (CPN) information as "Presentation Allowed."</li> <li>2. n: No CPN information is sent for the call</li> <li>3. r: Outgoing non-DCS network calls from the station will deliver the Calling Party Number information as "Presentation Restricted."</li> </ol> |

| Attribute                    | Attribute Description  | Mandatory/Optional | Validation Constraints |
|------------------------------|--|--------------------|------------------------|
| busyAutoCallbackWithoutFlash | Appears on the Station screen for analog telephones, only if the Without Flash field in the ANALOG BUSY AUTO CALLBACK section of the Feature-Related System Parameters screen is set to true. The Busy Auto Callback without Flash field then defaults to true for all analog telephones that allow Analog Automatic Callback. Set true to provide automatic callback for a calling analog station without flashing the hook.            | Optional           |                        |
| audibleMessageWaiting        | Provides audible message waiting   | Optional           | Boolean                |
| displayClientRedirection     | Only administrable if Hospitality is enabled on the System Parameters Customer- Options (Optional Features) screen. This field affects the telephone display on calls that originated from a station with Client Room Class of Service. Note: For stations with an audix station type, AUDIX Voice Power ports, or ports for any other type of messaging that needs display information, Display Client Redirection must be enabled. Set | Optional           | Boolean                |

| Attribute                | Attribute Description  | Mandatory/Optional | Validation Constraints   |
|--------------------------|--|--------------------|--|
|                          | true to redirect information for a call originating from a Client Room and terminating to this station displays. |                    |  |
| selectLastUsedAppearance |  | Optional           | <p>Valid entries:</p> <ol style="list-style-type: none"> <li>1. True: Indicates that a station's line selection is not to be moved from the currently selected line button to a different, non-alerting line button. If you enter true, the line selection on an on-hook station only moves from the last used line button to a line button with an audibly alerting call. If there are no alerting calls, the line selection remains on the button last used for a call.</li> <li>2. false: The line selection on an on-hook station with no alerting calls can be moved to a different line button, which might be serving a different extension.</li> </ol> |
| coverageAfterForwarding  | Whether an unanswered  | Optional           |  |

| Attribute                  | Attribute Description   | Mandatory/Optional | Validation Constraints    |
|----------------------------|---|--------------------|---------------------------|
|                            | forwarded call is provided coverage treatment.                            |                    |                           |
| directIplpAudioConnections | Allow/disallow direct audio connections between IP endpoints.             | Optional           |                           |
| ipAudioHairpinning         | Allows IP endpoints to be connected through the server's IP circuit pack. | Optional           |                           |
| primeAppearancePreference  | Set prime appearance preference.  | Optional           |                           |
| stationSiteData            | This is complex type for Site Data fields                                 |                    |                           |
| room                       | This is field of Site Data  | Optional           | Max length 10             |
| jack                       | This is field of Site Data  | Optional           | Max length 5              |
| cable                      | This is field of Site Data  | Optional           | Max length 5              |
| floor                      | This is field of Site Data  | Optional           |                           |
| building                   | This is field of Site Data  | Optional           |                           |
| headset                    | This is field of Site Data  | Optional           |                           |
| speaker                    | This is field of Site Data  | Optional           |                           |
| mounting                   | This is field of Site Data  | Optional           | Valid values d, w.        |
| cordLength                 | This is field of Site Data  | Optional           | Valid range from 0 to 99. |
| setColor                   | This is field of Site Data  | Optional           |                           |
| abbrList                   | This is complex type for Station  | Optional           |                           |

| Attribute                | Attribute Description                              | Mandatory/Optional | Validation Constraints                          |
|--------------------------|--|--------------------|---|
|                          | Abbreviated Dialing Data fields.                   |                    |   |
| listType                 | This is field of Station Abbreviated Dialing Data. | Mandatory          | Valid values enhanced, group, personal, system. |
| number                   | This is field of Station Abbreviated Dialing Data. | Mandatory          | A number.                                       |
| buttons                  | This is complex type for button data               | Optional           |   |
| Number                   | This is field of button data.                      | Mandatory          |   |
| Type                     | This is field of button data.                      | Optional           |   |
| data1                    | This is field of button data.                      | Optional           |   |
| data2                    | This is field of button data.                      | Optional           |   |
| data3                    | This is field of button data.                      | Optional           |   |
| data4                    | This is field of button data.                      | Optional           |   |
| data5                    | This is field of button data.                      | Optional           |   |
| data6                    | This is field of button data.                      | Optional           |   |
| stationDataModule        | This is complex type for Station Data module.      | Optional           |   |
| dataExtension            | This is field of Station Data module.              | Mandatory          |   |
| name                     | This is field of Station Data module.              | Optional           | Max length 29                                   |
| Class of restriction cor | This is field of Station Data module.              | Mandatory          | Valid range from 0 to 995.                      |
| Class of Service Cos     | This is field of Station Data module.              | Mandatory          | Valid range from 0 to 15.                       |

| Attribute                  | Attribute Description                     | Mandatory/Optional | Validation Constraints   |
|----------------------------|---|--------------------|--|
| itc                        | This is field of Station Data module.     | Mandatory          | Valid values:<br>1. restricted<br>2. unrestricted                    |
| Tenant Number              | This is field of Station Data module.     | Mandatory          | Valid range from 0 to 100.   |
| listType                   | This is field of Station Data module.     | Optional           | Valid values:<br>1. enhanced<br>2. group<br>3. personal<br>4. system |
| listId                     | This is field of Station Data module.     | Optional           |  |
| specialDialingOption       | This is field of Station Data module.     | Optional           | Valid values:<br>1. default<br>2. hot-line                           |
| specialDialingAbbrDialCode | This is field of Station Data module.     | Optional           |  |
| hotLineDestAbbrevList      | This is field of Station Hot Line Data.   | Optional           | Valid range 1 to 3   |
| hotLineAbbrevDialCode      | This is field of Station Hot Line Data.   | Optional           | Numeric string   |
| nativeName                 | This is complex type of Native Name Data. | Optional           |  |
| locale                     | This is field of Native Name Data.        | Mandatory          |  |
| Name                       | This is field of Native Name Data.        | Mandatory          | Max length 27  |

### Attribute details defined in the Messaging communication profile XSD

| Attribute             | Attribute Description    | Mandatory/Optional | Validation Constraints |
|-----------------------|--------------------------|--------------------|------------------------|
| Messaging System Name | Name of Messaging System | Mandatory          |                        |

| Attribute                                  | Attribute Description   | Mandatory/Optional | Validation Constraints  |
|--|---|--------------------|---|
| messagingName                              |   |                    |   |
| Use Existing Mailbox number<br>useExisting | 'true' if already created mailbox number is to be used. 'false' if available mailbox number is to be used.  | Optional           |   |
| Messaging Template<br>messagingTemplate    | Specifies the messaging template of a subscriber.   | Optional           |   |
| Password<br>password                       | Specifies the default password the subscriber must use to log in to his or her mailbox.   | Mandatory          | The password can be from one digit in length to a maximum of 15 digits. |
| deleteOnUnassign                           |   | Optional           |   |
| Class of service<br>cos                    | The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size.  | Optional           | Valid ranges from 0 to 995  |
| Community ID<br>communityID                | Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers.   | Optional           | The default value is 1.   |
| Email Handle<br>emailHandle                | Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the | Optional           |   |

| Attribute                 | Attribute Description   | Mandatory/Optional | Validation Constraints                                  |
|---------------------------|---|--------------------|---|
|                           | subscriber sends or receives an e-mail.   |                    |   |
| Common Name<br>commonName | Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications.  | Optional           | The name you enter can be 1 to 64 characters in length. |
| secondaryExtension        | Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers. | Optional           | Valid values 0 to 9 number values of length 10          |
| mmSpecific                | This is complex type for Messaging specific fields data.  | Optional           |   |
| numericAddress            | This is field of Messaging specific data. Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.  | Optional           |   |
| pbxExtension              | This is field of Messaging specific data. The primary telephone extension of the subscriber.  | Optional           |   |

| Attribute               | Attribute Description   | Mandatory/Optional | Validation Constraints  |
|-------------------------|---|--------------------|---|
| telephoneNumber         | This is field of Messaging specific data.<br>The telephone number of the subscriber as displayed in address book listings and client applications.                                    | Optional           | The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses (()) and (()). |
| asciiVersionOfName      | This is field of Messaging specific data.<br>If the subscriber name is entered in multibyte character format, then this field specifies the ASCII translation of the subscriber name. | Optional           |   |
| expirePassword          | This is field of Messaging specific data.<br>Specifies whether your password expires or not.  | Optional           | You can choose one of the following: <ul style="list-style-type: none"> <li>• yes: for password to expire</li> <li>• no: if you do not want your password to expire</li> </ul>              |
| mailBoxLocked           | This is field of Messaging specific data.<br>Specifies whether you want your mailbox to be locked. A subscriber mailbox can become locked after two unsuccessful login attempts.      | Optional           | You can choose one of the following: <ul style="list-style-type: none"> <li>• no: to unlock your mailbox</li> <li>• yes: to lock your mailbox and prevent access to it</li> </ul>           |
| personalOperatorMailbox | This is field of Messaging specific data.<br>Specifies the mailbox number or transfer dial string of the subscriber's   | Optional           |   |

| Attribute                       | Attribute Description   | Mandatory/Optional | Validation Constraints  |
|---------------------------------|---|--------------------|---|
|                                 | <p>personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.</p> |                    |   |
| <p>personalOperatorSchedule</p> | <p>This is field of Messaging specific data. Specifies when to route calls to the backup operator mailbox. The default value for this field is Always Active.</p>             | <p>Optional</p>    |   |
| <p>tuiMessageOrder</p>          | <p>This is field of Messaging specific data. Specifies the order in which the subscriber hears the voice messages.</p>  | <p>Optional</p>    | <p>You can choose one of the following:</p> <ul style="list-style-type: none"> <li>• urgent first then newest: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received.</li> <li>• oldest messages first: to direct the system to play messages in the order they were received.</li> <li>• urgent first then oldest: to direct the system to play any messages marked as urgent prior to</li> </ul> |

| Attribute        | Attribute Description   | Mandatory/Optional | Validation Constraints  |
|------------------|---|--------------------|---|
|                  |   |                    | <p>playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received.</p> <ul style="list-style-type: none"> <li>• newest messages first: to direct the system to play messages in the reverse order of how they were received.</li> </ul>   |
| intercomPaging   | <p>This is field of Messaging specific data. Specifies the intercom paging settings for a subscriber.</p>   | Optional           | <p>You can choose one of the following:</p> <ul style="list-style-type: none"> <li>• paging is off: to disable intercom paging for this subscriber.</li> <li>• paging is manual: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber.</li> <li>• paging is automatic: if the TUI automatically allows callers to page the subscriber.</li> </ul> |
| voiceMailEnabled | <p>This is field of Messaging specific data. Specifies whether a subscriber can receive messages, e-mail messages and callanswer messages from other subscribers. You can</p> | Optional           |   |

| Attribute      | Attribute Description   | Mandatory/ Optional | Validation Constraints |
|----------------|---|---------------------|------------------------|
|                | choose one of the following: - yes: to allow the subscriber to create, forward, and receive messages. - no: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber. |                     |                        |
| miscellaneous1 | This is field of Messaging specific data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.  |                     | Max length 51          |
| miscellaneous2 | This is field of Messaging specific data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.  |                     | Max length 51          |
| miscellaneous3 | This is field of Messaging specific data.   |                     | Max length 51          |

| Attribute      | Attribute Description   | Mandatory/Optional | Validation Constraints  |
|----------------|---|--------------------|---|
|                | <p>Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.</p>   |                    |   |
| miscellaneous4 | <p>This is field of Messaging specific data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.</p> |                    | Max length 51   |
| cmmSpecific    | <p>This is field of Messaging specific data. Specifies the number of the switch on which this subscriber's extension is administered.</p>   | Optional           | <p>You can enter "0" through "99", or leave this field blank.</p> <ul style="list-style-type: none"> <li>• Leave this field blank if the host switch number should be used.</li> <li>• Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.</li> </ul> |
| accountCode    | <p>This is field of CMM data. Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail</p>  | Optional           |   |

| Attribute         | Attribute Description  | Mandatory/Optional | Validation Constraints   |
|-------------------|--|--------------------|--|
|                   | Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code. |                    |  |
| coveringExtension | This is field of CMM data. Specifies the number to be used as the default destination for the Transfer Out of Messaging feature.   | Optional           | You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank. |
| miscellaneous1    | This is field of CMM data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.  | Optional           | Max length 11  |
| Miscellaneous2    | This is field of CMM data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.  | Optional           | Max length 11  |
| Miscellaneous2    | This is field of CMM data. Specifies additional, useful information  | Optional           | Max length 11  |

| Attribute      | Attribute Description   | Mandatory/Optional | Validation Constraints |
|----------------|---|--------------------|------------------------|
|                | about a subscriber. Entries in this field are for convenience and are not used by the messaging system.   |                    |                        |
| Miscellaneous4 | This is field of CMM data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. | Optional           | Max length 11          |

**Attribute details defined in the Session Manager communication profile XSD**

| Attribute                                | Attribute Description  | Mandatory/Optional | Validation Constraints |
|--|--|--------------------|------------------------|
| Primary Session Manager<br>primarySM     | Specify the name of the Session Manager instance that should be used as the home server for a Communication Profile. As a home server, the primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. | Mandatory          |                        |
| Secondary Session Manager<br>secondarySM | If a secondary Session Manager instance is specified, this Session   | Optional           |                        |

| Attribute  | Attribute Description   | Mandatory/Optional | Validation Constraints |
|--|---|--------------------|------------------------|
|  | <p>Manager will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available.</p>   |                    |                        |
| <p>Origination Application Sequence<br/>originationAppSequence</p> | <p>Specify an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. Note: if both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.</p> | <p>Optional</p>    |                        |
| <p>Termination Application Sequence<br/>terminationAppSequence</p> | <p>Specify an Application Sequence that will be invoked when calls are routed to this user. A selection is optional. Note: if both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.</p>   | <p>Optional</p>    |                        |
| <p>Survivability Server<br/>survivabilityServer</p>                | <p>For local survivability, the name of a Survivability Server (a SIP Entity) can be specified to provide survivability communication</p>   | <p>Optional</p>    |                        |

| Attribute                             | Attribute Description   | Mandatory/Optional | Validation Constraints |
|---------------------------------------|---|--------------------|------------------------|
|                                       | <p>services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is specified, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. A selection is optional. Note: if a termination or origination application sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager.</p> |                    |                        |
| <p>Home Location<br/>homeLocation</p> | <p>A Home Location can be specified (the name of a Location – navigate to Routing &gt; Locations) to support mobility for a user. When this user calls numbers that are not associated with an administered user, dial-plan rules (Routing &gt; Dial Patterns) will be</p>  | <p>Mandatory</p>   |                        |

| Attribute | Attribute Description   | Mandatory/Optional | Validation Constraints |
|-----------|---|--------------------|------------------------|
|           | applied to complete the call based on this "home" location regardless of the physical location of the SIP device used to make the call. A selection is mandatory. |                    |                        |

## Import Users field descriptions

Use this page to bulk import user records from a valid XML file.

### File Selection

| Name               | Description  |
|--------------------|--|
| <b>Select File</b> | The path and name of the XML file from which you want to import the users. |

| Button        | Description   |
|---------------|---|
| <b>Browse</b> | Opens a dialog box that you can use to select the file from which you want to import the users. |

### General

| Name                                       | Description  |
|--|--|
| <b>Select Error Configuration</b>          | <p>The options are:</p> <ul style="list-style-type: none"> <li>• Abort on First Error: Aborts importing the user records when the import user operation encounters the first error in the import file containing the user records.</li> <li>• Continue Processing other records: Imports the next user record if the import user operation encounters an error while importing a user record.</li> </ul> |
| <b>Select Import Type</b>                  | <p>The options are:</p> <ul style="list-style-type: none"> <li>• Complete: Imports users with all the user attributes.</li> <li>• Partial: Imports users with selected user attributes.</li> </ul>   |
| <b>If a matching record already exists</b> | <p>The options are:</p> <ul style="list-style-type: none"> <li>• Skip: Skips a matching user record that already exists in the system during an import operation. Currently Using this option you can add</li> </ul>   |

| Name | Description  |
|------|--|
|      | <p>a new commprofile to a commprofile set but you cannot update an existing commprofile in a commprofile set.</p> <p> <b>Note:</b><br/>This option is not available if you select the <b>Partial</b> option for the <b>Select Import Type</b>.</p> <ul style="list-style-type: none"> <li>• <b>Replace:</b> Re-imports or replaces all the data for a user including access control lists, contact lists and so on. This is essentially the ability to replace a user along with the other data related to the user.</li> <li>• <b>Merge:</b> Imports the user data at an even greater degree of granularity. Using this option you can simultaneously perform both add and update operation of users. For example, add a contact to a contact list and update a surname.</li> <li>• <b>Delete:</b> Deletes the user records from the database that match the records in the input XML file.</li> </ul> <p> <b>Note:</b><br/>The system confirms that a user already exists in the database by matching the login name of the user in the database with the login name of the user in the imported file.</p> |

### Job Schedule

| Name                | Description   |
|---------------------|---|
| <b>Schedule Job</b> | <p>The options for configuring the schedule of the job:</p> <ul style="list-style-type: none"> <li>• <b>Run immediately:</b> Use this option if you want to run the import job immediately.</li> <li>• <b>Schedule later:</b> Use this option to run the job at the specified date and time.</li> </ul> |
| <b>Date</b>         | <p>Date when you want to run the import users job. The date format is mm dd yyyy. You can use the calendar icon to choose a date. This field is available when you select the <b>Schedule later</b> option for scheduling a job.</p>  |
| <b>Time</b>         | <p>Time of running the import users job. The time format is hh:mm:ss and 12 (AM or PM) or 24 hour format. This field is available when you select the <b>Schedule later</b> option for scheduling a job.</p>  |
| <b>Time Zone</b>    | <p>Time zone of your region. This field is available when you select the <b>Schedule later</b> option for scheduling a job.</p>   |

| Button        | Description   |
|---------------|---|
| <b>Import</b> | Imports or schedules the import operation based on the option you selected. |

## Manage Jobs

| Name                  | Description   |
|-----------------------|---|
| <b>Check box</b>      | Use this check box to select a job.   |
| <b>Scheduled Time</b> | The time and date of scheduling the job   |
| <b>Status</b>         | The current status of the job. The following are the different status of the job: <ol style="list-style-type: none"> <li>1. PENDING EXECUTION: The job is in queue.</li> <li>2. RUNNING: The job execution is in progress.</li> <li>3. SUCCESSFUL: The job execution is completed.</li> <li>4. INTERRUPTED: The job execution is cancelled.</li> <li>5. PARTIAL FAILURE: The job execution has partially failed.</li> <li>6. FAILED: The job execution has failed.</li> </ol> |
| <b>Job Name</b>       | A link to the Scheduler user interface. You can cancel the job from the Scheduler user interface too.   |
| <b>% Complete</b>     | The job completion status in percentage.  |
| <b>User Records</b>   | The total user records in the input file.   |
| <b>Error</b>          | Number of user records in the input file that failed to import.   |

| Button              | Description  |
|---------------------|--|
| <b>View Job</b>     | Shows the details of the selected job.   |
| <b>Cancel Job</b>   | Cancels the import operation for the selected job. You can cancel a job that is in progress or queued for import.  |
| <b>Delete Job</b>   | Deletes the selected job.  |
| <b>Refresh</b>      | Refreshes the job information in the table.  |
| <b>Show</b>         | Provides you an option to view all the jobs on the same page. If the table displaying scheduled jobs are spanning multiple pages, select <b>All</b> to view all the jobs on a single page. |
| <b>Select: All</b>  | Selects all the jobs in the table.   |
| <b>Select: None</b> | Clears the check box selections.   |
| <b>Previous</b>     | Displays jobs in the previous page.  |
| <b>Next</b>         | Displays jobs in the next page.  |
| <b>Done</b>         | Takes you back to the <b>User Management</b> page.   |

## Import Users – Job Details field descriptions

The Import Users-Job Details page displays the details of the selected Job.

| Name             | Description  |
|------------------|--|
| <b>Start</b>     | Start date and time of the job.  |
| <b>End</b>       | End date and time of the job.  |
| <b>Status</b>    | Status of the job.   |
| <b>File</b>      | Name of the file that is used to import the user records.              |
| <b>Count</b>     | Total number of user records in the input file.                        |
| <b>Success</b>   | Total number of user records that are successfully imported.           |
| <b>Fail</b>      | Total number of user records that failed to import.                    |
| <b>Message</b>   | The message that indicate whether the import is successful or failure. |
| <b>Completed</b> | Displays the percentage completion of the import.                      |

| Name                 | Description   |
|----------------------|---|
| <b>Line Number</b>   | Line number in the file where the error occurred.         |
| <b>Login Name</b>    | Login Name of the user record that failed to be imported. |
| <b>Error Message</b> | A brief description of the error.                         |

| Button          | Description   |
|-----------------|---|
| <b>Download</b> | Exports and saves the user import error records in an XML file to the specified destination.<br><br> <b>Note:</b><br>This button is not available if there are no error records for user Import Jobs or if the import job type is set to <b>Abort On First Error</b> . |
| <b>Cancel</b>   | Takes you back to the Import Users page.  |

## Import Global Settings field descriptions

Use this page to bulk import shared addresses, public contacts and presence ACLs (access control list) records also called global user settings from a valid XML file.

## File Selection

| Name               | Description  |
|--------------------|--|
| <b>Select File</b> | The path and name of the XML file from which you want to import the global settings records. |

| Button        | Description   |
|---------------|---|
| <b>Browse</b> | Opens a dialog box that allows you to select the file from which you want to import the global user settings. |

## General

| Name                                       | Description  |
|--|--|
| <b>Select Error Configuration</b>          | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Abort on First Error:</b> Aborts importing the global user settings records when User Management encounters the first error in the import file containing the global user settings records.</li> <li>• <b>Continue Processing other records:</b> Imports the next global user settings record if User Management encounters an error while importing a global user settings record.</li> </ul>   |
| <b>If a matching record already exists</b> | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Skip:</b> Skips a matching global user settings record that already exists in the system database during an import operation. Currently, using this option you can add a new public contact to a public contact set but you cannot update an existing public contact in a public contact set.</li> <li>• <b>Replace:</b> Re-imports or replaces all the global user setting records in the import file. This is essentially the ability to replace a user along with the other data related to the global user settings.</li> <li>• <b>Merge:</b> Imports the global user settings data at an even greater degree of granularity. For example, add a shared address to a shared address list or update a public contact.</li> <li>• <b>Delete:</b> Deletes the global setting records from the database that matches the records in the input XML file.</li> </ul> |

## Job Schedule

| Name                | Description   |
|---------------------|---|
| <b>Schedule Job</b> | The settings for configuring the schedule of the job: <ul style="list-style-type: none"> <li>• Run immediately: Use this option if you want to run the import job immediately.</li> <li>• Schedule later: Use this option to run the job at the specified date and time.</li> </ul> |
| <b>Date</b>         | Date when you want to run the import job. The date format is mm dd yyyy. You can use the calendar icon to choose a date. This field is available when you select the <b>Schedule later</b> option for scheduling a job.   |
| <b>Time</b>         | Time of running the import job. The time format is hh:mm:ss and 12 (AM or PM) or 24 hour format. This field is available when you select the <b>Schedule later</b> option for scheduling a job.   |
| <b>Time Zone</b>    | Time zone of your region. This field is available when you select the <b>Schedule later</b> option for scheduling a job.  |

| Button        | Description   |
|---------------|---|
| <b>Import</b> | Imports or schedules the import operation based on the option you selected. |

## Manage Jobs

| Name                  | Description   |
|-----------------------|---|
| <b>Check box</b>      | Use this check box to select a job.   |
| <b>Scheduled Time</b> | The date and time when job was scheduled.   |
| <b>Status</b>         | The current status of the job. The following are the different status of the job: <ol style="list-style-type: none"> <li>1. PENDING EXECUTION: The job is in queue.</li> <li>2. RUNNING: The job execution is in progress.</li> <li>3. SUCCESSFUL: The job execution is completed.</li> <li>4. INTERRUPTED: The job execution is cancelled.</li> <li>5. PARTIAL FAILURE: The job execution has partially failed.</li> <li>6. FAILED: The job execution has failed.</li> </ol> |
| <b>Job Name</b>       | A link to the Scheduler user interface. You can cancel the job from the Scheduler user interface too.   |
| <b>% Complete</b>     | The job completion status in percentage.  |

| Name           | Description   |
|----------------|---|
| <b>Records</b> | The total number of global user settings records in the input file.             |
| <b>Error</b>   | Number of global user settings records in the input file that failed to import. |

| Button              | Description  |
|---------------------|--|
| <b>View Job</b>     | Shows the details of the selected job.   |
| <b>Cancel Job</b>   | Cancels the import operation for the selected job. You can cancel a job that is in progress or queued for import.  |
| <b>Delete Job</b>   | Deletes the selected job.  |
| <b>Refresh</b>      | Refreshes the job information in the table.  |
| <b>Show</b>         | Provides you an option to view all the jobs on the same page. If the table displaying scheduled jobs are spanning multiple pages, select <b>All</b> to view all the jobs on a single page. |
| <b>Select: All</b>  | Selects all the jobs in the table.   |
| <b>Select: None</b> | Clears the check box selections.   |
| <b>Previous</b>     | Displays jobs in the previous page.  |
| <b>Next</b>         | Displays jobs in the next page.  |
| <b>Done</b>         | Takes you back to the <b>User Management</b> page.   |
| <b>Cancel</b>       | Cancels the import operation and takes you back to the User Management page.   |

## Job Details field descriptions

The Job Details page displays the details of the selected Job.

| Name           | Description  |
|----------------|--|
| <b>Start</b>   | Start date and time of the job.  |
| <b>End</b>     | End date and time of the job.  |
| <b>Status</b>  | Status of the job.   |
| <b>File</b>    | Name of the file that is used to import the global user settings records.    |
| <b>Count</b>   | Total number of global user settings records in the input file.              |
| <b>Success</b> | Total number of global user settings records that are successfully imported. |
| <b>Fail</b>    | Total number of global user settings records that failed to import.          |
| <b>Message</b> | The message that indicates whether the import is successful or failure.      |

| Name             | Description                                       |
|------------------|---|
| <b>Completed</b> | Displays the percentage completion of the import. |

| Name                 | Description                               |
|----------------------|---|
| <b>Record Number</b> | Failed XML element in the input XML file. |
| <b>Name</b>          | Name of the failed XML element.           |
| <b>Error Message</b> | A brief description of the error.         |

| Button        | Description                              |
|---------------|--|
| <b>Cancel</b> | Takes you back to the Import Users page. |

---

## Managing communication profiles

### Creating a new communication profile

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, click **New**.
  3. Perform one of the following steps:
    - If you are creating a new user account, on the User Management page, click **New**
    - On the User Management page, select a user and click **Edit** for an existing user account.
    - On the User Management page, select a user and click **View > Edit** for an existing user account.
  4. Click the **Communication Profile** link at the top of the page.
  5. In the communication profile section, click **New**.
  6. In the **Name** field, enter the name of the communication profile.
  7. If you want to make the profile default profile, select the **Default** check box.
  8. Click **Done**.
  9. Click **Commit**.
-

**Related topics:**

[User Profile Edit field descriptions](#) on page 1577

[New User Profile field descriptions](#) on page 1586

## Deleting a communication profile

You cannot delete the default communication profile.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Perform one of the following steps:
    - On the User Management page, select a user and click **Edit**.
    - On the User Management page, select a user and click **View > Edit**.
  3. On the User Profile Edit page, click the Communication Profile link at the top of the page.
  4. In the communication profile section, click a profile.
  5. Click **Delete**.
  6. Click **Commit**.
- 

### Result

When you delete a communication profile, the System Manager application deletes all the communication addresses associated with the communication profile.

**Related topics:**

[User Profile Edit field descriptions](#) on page 1577

[New User Profile field descriptions](#) on page 1586

## Creating a new communication address for a communication profile

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, click **New**.
  3. Perform one of the following steps:
    - If you are creating a new user account, on the User Management page, click **New**

- On the User Management page, select a user and click **Edit** for an existing user account.
  - On the User Management page, select a user and click **View** > **Edit** for an existing user account.
4. Click the **Communication Profile** link at the top of the page.
  5. In the Communication Profile section, click a communication profile.
  6. In the communication address section, click **New**.
  7. From the **Type** drop-down, select a communication protocol.
  8. From the **Sub Type** drop-down, select a application type.
  9. In the **Fully Qualified Address** field, enter the contact address in the format supported by the value that you selected in the **Sub Type** field. Contact address can be an e-mail id, instant messenger id, sip address of a sip enabled device and so on.
  10. From the drop-down field next to **Fully Qualified Address** field, select or enter the domain name.
  11. Click **Save**.
  12. Click **Commit**.
- 

### Related topics:

[User Profile Edit field descriptions](#) on page 1577

[New User Profile field descriptions](#) on page 1586

## Modifying a communication address of a user

---

1. On the System Manager console, click **Users** > **Manage Users** in the left navigation pane.
2. Perform one of the following steps:
  - On the User Management page, select a user and click **Edit**.
  - On the User Management page, select a user and click **View** > **Edit**.
3. On the User Profile Edit page, click the Communication Profile link at the top of the page.
4. In the Communication Profile section, select a profile.
5. In the Communication Address section, select a communication address.
6. Click **Edit**.

7. Modify the information in the respective fields.
  8. Click **Save** .
  9. Click **Commit**.
- 

**Related topics:**

[User Profile Edit field descriptions](#) on page 1577

[New User Profile field descriptions](#) on page 1586

## Deleting a communication address from a communication profile

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Perform one of the following steps:
    - On the User Management page, select a user and click **Edit**.
    - On the User Management page, select a user and click **View > Edit**.
  3. On the User Profile Edit page, click the Communication Profile link at the top of the page.
  4. In the Communication Profile section, click a Communication Profile.
  5. In the Communication Address section, select a communication address.
  6. Click **Delete** .  
You can find the **Delete** button in the Communication Address section.
  7. Click **Save**.  
You can find the **Save** button in the Communication Profile section.
  8. Click **Commit**.
- 

**Related topics:**

[User Profile Edit field descriptions](#) on page 1577

[New User Profile field descriptions](#) on page 1586

## Session Manager Communication profile administration

The Session Manager Profile sub-section of the Communication Profile section enables associating a primary Session Manager instance as a home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will

be used as the default access point for connecting devices associated with the Communication Profile to the Aura network.

All Communication Addresses (handles) of type SIP for the Communication Profile will be associated with the Aura network. If a secondary Session Manager instance has been selected, it will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available.

Application Sequences may be specified to be invoked when routing calls from (origination application sequence) or to (termination application sequence) the currently displayed user.

For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager.

A Home Location can be specified to support mobility for the currently displayed user. When this user calls numbers that are not associated with an administered user, dial-plan rules (Routing > Dial Patterns) will be applied to complete the call based on this home location (Routing > Locations) regardless of the physical location of the SIP device used to make the call.

## Station and Messaging profiles of a user

Using User Profile Management, you can create the following two types of communication profiles for a user:

1. Station Profile: to create an association between a station and a user
2. Messaging Profile: to create an association between a subscriber mailbox and a user

You can add, view, modify and delete station and messaging profiles. You can go to Station or Subscriber Management to modify any of the station or subscriber fields that are not available through User Profile Management.

### Login name of station or messaging profile

The login name in the Identity section on the New User Profile and Edit User Profile pages is the user name that is associated with the communication profile (station and messaging). This user name appears in the User column in the Station List or Subscriber List.

For stations, the **Localized Display Name** and **Endpoint Display Name** fields in the Identity section of UPM user profile are mapped to the **Name** and **Native Name** fields of Station. The **Localized Display Name** and **Endpoint Display Name** fields are optional. They default to the **Last Name** and **First Name** as given in the General section of the UPM user profile. You can also fill in any other name of your choice.

For Subscribers, the **Last Name** and **First Name** fields in the General section of the UPM user profile directly map to the **Last Name** and **First Name** fields in Subscriber. The **Localized Display Name** and **Endpoint Display Name** fields are not applicable for Subscribers.

## Creating stations and messaging profiles

You can create one default or primary Communication Profile for a user. To this default profile, you can add one station and one messaging profile. In addition, you can add two more station profiles. You can add a maximum of three station profiles and one messaging profile per user.

## Adding a messaging profile for a user

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, perform one of the following steps:
    - If you are creating a messaging profile for a new user profile, click **New**.
    - If you are creating a messaging profile for an existing user, select the user and click **Edit**.
  3. Click the **Communication Profile** link at the top of the page.
  4. In the messaging Profile section, select the **Messaging Profile** check box beside the **Messaging Profile** label.
  5. Enter the relevant information in the fields provided in the Messaging Profile section.

 **Note:**

You must select the **Delete Messaging on Unassign of Subscriber from User** check box if you want to delete the subscriber mailbox from the communication management device after removing the association between the subscriber and the user.

6. Click **Commit** to add the messaging profile.

The field names that are marked with \* are mandatory fields. You must enter valid information in these fields for the successful creation of the station profile. If you want to cancel the action and return to the previous page, click **Cancel**.

 **Note:**

You should add the messaging devices through Runtime Topology System (RTS) before you add a messaging profile for a user. Once you create the user-subscriber association, the user name appears in the User column in the Subscriber list.

---

### Related topics:

[New User Profile field descriptions](#) on page 1586

## Modifying a messaging profile of a user

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select a user and perform one of the following steps:
    - Click **Edit**.
    - Click **View > Edit**.
  3. On the User Profile Edit page, click the **Communication Profile** link at the top of the page.
  4. In the Messaging Profile section, modify the information in the fields and click **Commit** to save the changes to the database.  
If you want to cancel the action and return to the previous page, click **Cancel**.

---

### Related topics:

[New User Profile field descriptions](#) on page 1586

## Removing an association between a subscriber mailbox and a user

### Prerequisites

Ensure that you have not selected the **Delete Subscriber on Unassign of Subscriber from User** check box while associating a mailbox with a user.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select a user and perform one of the following steps:
    - Click **Edit**.
    - Click **View > Edit**.
  3. On the User Profile Edit page, click the **Communication Profile** link at the top of the page.

4. In the Communication Profile section, clear the **Messaging Profile** check box beside the **Messaging Profile** label.
5. Click **Commit**.

---

## Result

This removes the association between the subscriber mailbox and the user. The subscriber mailbox is still provisioned on the communication management device.

## Related topics:

[New User Profile field descriptions](#) on page 1586

## Deleting a subscriber mailbox

### Prerequisites

Ensure that you have selected the **Delete Subscriber on Unassign of Subscriber from User** check box while associating a subscriber mailbox to a user.

---

This functionality deletes the subscriber mailbox from the messaging device after removing the association between the subscriber mailbox and the user.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select a user and perform one of the following steps:
    - Click **Edit**.
    - Click **View > Edit**.
  3. On the User Profile Edit page, click the **Communication Profile** link at the top of the page.
  4. In the Communication Profile section, clear the **Messaging Profile** check box beside the **Messaging Profile** label.
  5. Click **Commit**.

 **Note:**

You can delete only those subscribers that are associated with a user, through User Profile Management. You can delete the non-user associated subscriber mailboxes only through subscriber management.

---

**Related topics:**

[New User Profile field descriptions](#) on page 1586

## Adding a station profile for a user

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. On the User Management page, perform one of the following steps:
  - If you are creating a station profile for a new user profile, click **New**.
  - If you are creating a station profile for an existing user, select the user and click **Edit**.
3. Click the **Communication Profile** link at the top of the page.
4. In the Station Profile section, select the **Station Profile** check box beside the **Station Profile** label.
5. Enter the relevant information in the fields provided in the Station Profile section.

 **Note:**

You must select the **Delete Station on Unassign of Station from User** check box if you want to delete the station from the communication management device after removing the association between the station and the user.

6. Click **Commit** to add the station profile.

The field names that are marked with \* are mandatory fields. You must enter valid information in these fields for the successful creation of the station profile. If you want to cancel the action and return to the previous page, click **Cancel**.

Through User Profile Management, you can create or add stations. After you select the Communication Manager in which you want add a station, the system allows you to complete the fields for creating a new station.

 **Note:**

You should add the Communication Manager through RTS before you add the station profile for the users. Once you create the user-station association, the user name appears in the User column in the Station list.

---

**Related topics:**

[New User Profile field descriptions](#) on page 1586

## Modifying a station profile of a user

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select a user and perform one of the following steps:
    - Click **Edit**.
    - Click **View > Edit**.
  3. On the User Profile Edit page, click the **Communication Profile** link at the top of the page.
  4. In the Station Profile section, modify the information in the fields and click **Commit** to save the changes to the database.  
If you want to cancel the action and return to the previous page, click **Cancel**.
- 

### Related topics:

[New User Profile field descriptions](#) on page 1586

## Removing an association between a station and a user

### Prerequisites

Ensure that you have not selected the **Delete Station on Unassign of Station from User** check box while associating a station with a user.

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. On the User Management page, select a user and perform one of the following steps:
  - Click **Edit**.
  - Click **View > Edit**.
3. On the User Profile Edit page, click the **Communication Profile** link at the top of the page.

4. In the Communication Profile section, clear the **Station Profile** check box beside the **Station Profile** label.
5. Click **Commit** .

---

### Result

This removes the association between the station and the user. The station is still provisioned on the communication management device.

## Deleting a station profile of a user

### Prerequisites

Ensure that you have selected the **Delete Station on Unassign of Station from User** check box while associating a station to a user.

---

This functionality deletes the station from the communication management device after removing the association between the station and the user.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select a user and perform one of the following steps:
    - Click **Edit**.
    - Click **View > Edit**.
  3. On the User Profile Edit page, click the **Communication Profile** link at the top of the page.
  4. In the Communication Profile section, clear the **Station Profile** check box beside the **Station Profile** label.
  5. Click **Commit** .

 **Note:**

You can delete only those stations that are associated with a user, through User Profile Management. You can delete the non-user associated stations through station management.

---

### Related topics:

[New User Profile field descriptions](#) on page 1586

## User Profile View field descriptions

Use this page to view the details of the selected user account.

### General section

| Name               | Description                      |
|--------------------|----------------------------------|
| <b>Last Name</b>   | The last name of the user.       |
| <b>First Name</b>  | The first name of the user.      |
| <b>Description</b> | A brief description of the user. |
| <b>User Type</b>   | The primary user types.          |

### Identity section

| Name                          | Description  |
|-------------------------------|--|
| <b>Login Name</b>             | The unique system login name given to the user. It takes the form of username@domain. You can use the login name to create the user's primary handle.  |
| <b>Authentication Type</b>    | Authentication type defines how the system performs user's authentication. The options are: <ul style="list-style-type: none"> <li>• <b>enterprise</b> — User's login is authenticated by the enterprise.</li> <li>• <b>basic</b> — User's login is authenticated by an Avaya Authentication Service.</li> </ul> |
| <b>Password</b>               | The initial password for logging in to the system.   |
| <b>Confirm Password</b>       | The initial password for verification.   |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.   |
| <b>Endpoint Display Name</b>  | The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.  |
| <b>Honorific</b>              | The personal title for address a user. This is typically a social title and not the work title.  |
| <b>Language Preference</b>    | The user's preferred written or spoken language.   |
| <b>Time Zone</b>              | The preferred time zone of the user.   |

### Identity > Address section

| Name                 | Description  |
|----------------------|--|
| <b>Name</b>          | The name of the user.  |
| <b>Address Type</b>  | Type of the address. The following are the types: <ul style="list-style-type: none"> <li>• Office</li> <li>• Home</li> </ul> |
| <b>Street</b>        | The name of the street.  |
| <b>Locality Name</b> | The name of the city or town.  |
| <b>Postal Code</b>   | The postal code used by postal services to route mail to a destination. In United States this is Zip code.                   |
| <b>Province</b>      | The full name of the province.   |
| <b>Country</b>       | The name of the country.   |

### Communication Profile section

| Name                 | Description  |
|----------------------|--|
| <b>Option button</b> | Use this button to view the details of the selected communication profile. |
| <b>Name</b>          | Name of the communication profile.   |

| Name           | Description   |
|----------------|---|
| <b>Name</b>    | The name of the communication profile for the user.   |
| <b>Default</b> | The profile that is made default is the active profile. There can be only one active profile at a time. |

### Communication Address section

| Name           | Description   |
|----------------|---|
| <b>Type</b>    | The type of the handle.                                     |
| <b>SubType</b> | The sub type of the handle.                                 |
| <b>Handle</b>  | .A unique communication address for the user.               |
| <b>Domain</b>  | The name of the domain with which the handle is registered. |

### Session Manager



**Note:**

The page displays the following fields if a communication profile of the user exists for the product.

| Name                                    | Description   |
|---|---|
| <b>Primary Session Manager</b>          | Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.   |
| <b>Secondary Session Manager</b>        | If a secondary Session Manager instance is selected, this Session Manager will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available. A selection is optional.   |
| <b>Origination Application Sequence</b> | Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. Note: if both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.   |
| <b>Termination Application Sequence</b> | Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional.<br><br> <b>Note:</b><br>If both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.  |
| <b>Survivability Server</b>             | For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. A selection is optional. Note: if a termination or origination application sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager. |
| <b>Home Location</b>                    | A Home Location can be specified to support mobility for the currently displayed user. When this user calls numbers that are not associated with an administered user, dial-plan rules (Routing > Dial Patterns) will be applied to complete the call based on this home location (Routing > Locations) regardless of the physical location of the SIP device used to make the call. A selection is optional  |

## Messaging Profile

### Note:

The page displays the following fields if a messaging profile exists for the user.

| Name          | Description   |
|---------------|---|
| <b>System</b> | The Messaging System on which you need to add the subscriber. |

| Name   | Description  |
|--|--|
| <b>Template</b>  | The template (system defined and user defined) you want to associate with the subscriber.  |
| <b>Use Existing Subscriber on System</b>                     | Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.   |
| <b>Existing Mailbox Number</b>                               | The existing mailbox number that you want to associate with this profile. This value in the field is valid only if you select the <b>Use Existing Subscriber on System</b> check box.                            |
| <b>Mailbox Number</b>  | The mailbox number of the subscriber.  |
| <b>Password</b>  | The password for logging into the mailbox.   |
| <b>Delete Subscriber on Unassign of Subscriber from User</b> | Use this check box to specify whether you want to delete the subscriber mailbox from the Messaging Device or Communication System Management when you remove this messaging profile or when you delete the user. |

### Endpoint Profile



**Note:**

The page displays the following fields if an endpoint profile exists for the user.

| Name/Button                           | Description   |
|---------------------------------------|---|
| <b>System</b>                         | The Communication Manager on which you need to add the endpoint.  |
| <b>Use Existing Endpoints</b>         | Use the check box if you want to use an existing endpoint extension to associate with this profile. If you do not select this check box, the available extensions are used. |
| <b>Extension</b>                      | The extension of the station you want to associate.   |
| <b>Search</b>                         | Lists the endpoints (existing or available) based on check box status of the <b>Use Existing Endpoints</b> field.   |
| <b>Template</b>                       | The template (system defined or user defined) you want to associate with the endpoint. Select the template based on the set type you want to add.                           |
| <b>Set Type</b>                       | The set type of the endpoint you want to associate. When you select a template, the system populates the corresponding set types.   |
| <b>Security Code</b>                  | The security code for authorized access to the endpoint.  |
| <b>Port</b>                           | The relevant port for the set type you select.  |
| <b>Search</b>                         | Lists the possible ports based on the selected set type.  |
| <b>Delete Endpoint on Unassign of</b> | Use this check box to specify whether you want to delete the endpoint from the Communication Manager device when you remove the   |

| Name/Button               | Description   |
|---------------------------|---|
| <b>Endpoint from User</b> | association between the endpoint and the user or when you delete the user.  |
| <b>dtmfOverlap</b>        | <p>Appears when the <b>Set Type</b> field is H.323. This field specifies the touchtone signals that are used for dual-tone multifrequency (DTMF) telephone signaling. Valid entries include:</p> <ul style="list-style-type: none"> <li>• <b>in-band</b>- All G711 and G729 calls pass DTMF <b>in-band</b>. DTMF digits encoded within existing RTP media stream for G.711/G.729 calls. G.723 is sent <b>out-of-band</b>.</li> <li>• <b>in-band-g711</b> – Only G711 calls pass DTMF in-band.</li> <li>• <b>out-of-band</b>- All IP calls pass DTMF <b>out-of-band</b>. For IP trunks, the digits are done with either Keypad IEs or H245 indications. This is the default for newly added H.323 signaling groups.</li> </ul> |

### Roles section

| Name               | Description                         |
|--------------------|-------------------------------------|
| <b>Name</b>        | The name of the role.               |
| <b>Description</b> | A brief description about the role. |

### Group Membership section

| Name                    | Description                             |
|-------------------------|---|
| <b>Select check box</b> | Select the group.                       |
| <b>Name</b>             | Name of the group.                      |
| <b>Type</b>             | Group type based on the resources.      |
| <b>Hierarchy</b>        | Position of the group in the hierarchy. |
| <b>Description</b>      | A brief description about the group.    |

### Attribute Sets section

| Name                          | Description  |
|-------------------------------|--|
| <b>Select check box</b>       | Select the attribute set.                            |
| <b>Attribute Set</b>          | Name of the attribute set.                           |
| <b>Attribute Set Instance</b> | Name of the attribute set instance.                  |
| <b>Application</b>            | Name of the application that owns the attribute set. |
| <b>Description</b>            | A brief description about the attribute set.         |

### Default Contact List section

| Name               | Description   |
|--------------------|---|
| <b>Name</b>        | Name of the contact list. The default name of the contact list is Default. You can change the name to any other appropriate name. |
| <b>Description</b> | A brief description of the contact list.  |

### Associated Contacts section

| Name                    | Description   |
|-------------------------|---|
| <b>Last Name</b>        | Last name of the contact.   |
| <b>First Name</b>       | First name of the contact.  |
| <b>Scope</b>            | Categorization of the contact based on whether the contact is a public or private contact.  |
| <b>Speed Dial</b>       | The value specifies whether the speed dial is set for the contact or not.   |
| <b>Speed Dial Entry</b> | The reduced number that represents the speed dial number.   |
| <b>Presence Buddy</b>   | The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact. |

| Button                 | Description  |
|------------------------|--|
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.               |
| <b>Filter: Enable</b>  | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.   |

### Private Contacts section

Use this section to add new private contacts, modify and deletes existing contacts.

| Name                   | Description                            |
|------------------------|--|
| <b>Last Name</b>       | Last name of the private contact.      |
| <b>First Name</b>      | First name of the private contact.     |
| <b>Display Name</b>    | Display name of the private contact.   |
| <b>Contact Address</b> | Address of the private contact.        |
| <b>Description</b>     | A brief description about the contact. |

| Button                 | Description  |
|------------------------|--|
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.               |
| <b>Filter: Enable</b>  | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.   |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the User Profile Edit page. Use the User Profile Edit page to modify the details of the user account. |
| <b>Done</b> | Closes the User Profile View page and takes you back to the User Management page.                           |

**Related topics:**

[Viewing details of a user](#) on page 1390

## User Profile Edit field descriptions

Use this page to modify the details of a user account.

### General section

| Name               | Description                         |
|--------------------|-------------------------------------|
| <b>Last Name</b>   | The last name of the user.          |
| <b>First Name</b>  | The first name of the user.         |
| <b>Description</b> | A brief description about the user. |

### Identity section

| Name                       | Description  |
|----------------------------|--|
| <b>Login Name</b>          | This is the unique system login name given to the user. It takes the form of username@domain. It is used to create the user's primary handle.  |
| <b>Authentication Type</b> | Authentication type defines how the system performs user's authentication. The options are: <ul style="list-style-type: none"> <li>• <b>enterprise</b> — User's login is authenticated by the enterprise.</li> <li>• <b>basic</b> — User's login is authenticated by an Avaya Authentication Service.</li> </ul> |
| <b>Password</b>            | The initial password for logging in to the system.   |

| Name                          | Description   |
|-------------------------------|---|
| <b>Confirm Password</b>       | The initial password for verification.  |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.  |
| <b>Endpoint Display Name</b>  | The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints. |
| <b>Honorific</b>              | The personal title for address a user. This is typically a social title and not the work title.   |
| <b>Language Preference</b>    | The user's preferred written or spoken language.  |
| <b>Time Zone</b>              | The preferred time zone of the user.  |

### Identity > Address section

| Name                    | Description   |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select the address.   |
| <b>Name</b>             | The name of the user.   |
| <b>Address Type</b>     | The type of address. The values are: <ul style="list-style-type: none"> <li>• Office</li> <li>• Home</li> </ul> |
| <b>Street</b>           | The name of the street.   |
| <b>Locality Name</b>    | The name of the city or town.   |
| <b>Postal Code</b>      | The postal code used by postal services to route mail to a destination. In United States this is Zip code.      |
| <b>Province</b>         | The full name of the province.  |
| <b>Country</b>          | The name of the country.  |

| Button                       | Description   |
|------------------------------|---|
| <b>New</b>                   | Opens the Add Address page that you can use to add the address details.     |
| <b>Edit</b>                  | Opens the Edit Address page that you can use to modify the address details. |
| <b>Delete</b>                | Deletes the selected address.   |
| <b>Choose Shared Address</b> | Opens the Choose Address page that you can use to choose a address.         |

## Communication Profile section

Use this section to create, modify and delete a communication profile for the user. Each communication profile may contain one or more communication addresses for a user.

| Name                 | Description  |
|----------------------|--|
| <b>Option button</b> | Use this button to view the details of the selected communication profile. |
| <b>Name</b>          | Name of the communication profile.   |

| Name          | Description  |
|---------------|--|
| <b>New</b>    | Creates a new communication profile for the user.                                    |
| <b>Delete</b> | Deletes the selected communication profile.  |
| <b>Save</b>   | Saves the communication profile information that you updated or added for a profile. |
| <b>Cancel</b> | Cancel the operation for adding a communication profile.                             |

The page displays the following fields when you click the **Add** button in the Communication Profile section.

| Name           | Description   |
|----------------|---|
| <b>Name</b>    | The name of the communication profile for the user.   |
| <b>Default</b> | The profile that is made default is the active profile. There can be only one active profile at a time. |

## Communication Address section

Use this section to create, modify and delete one or more communication addresses for the user.

| Name           | Description   |
|----------------|---|
| <b>Type</b>    | The type of the handle.                                     |
| <b>SubType</b> | The sub type of the handle.                                 |
| <b>Handle</b>  | .A unique communication address for the user.               |
| <b>Domain</b>  | The name of the domain with which the handle is registered. |

| Name          | Description  |
|---------------|--|
| <b>New</b>    | Displays the fields for adding a new communication address.                  |
| <b>Edit</b>   | Use this button to edit the information of a selected communication address. |
| <b>Delete</b> | Deletes the selected communication address.                                  |

The page displays the following fields when you click **New** and **Edit** in the Communication Address section.

| Name                           | Description  |
|--------------------------------|--|
| <b>Type</b>                    | <p>The types of the handle. The following are the different handle types:</p> <ul style="list-style-type: none"> <li>• sip: Indicates that the handle supports SIP based communication.</li> <li>• smtp: Indicates that the handle is an e-mail address and supports Simple Mail Transfer Protocol (SMTP) based communication.</li> <li>• ibm: Indicates that the handle is an IBM address.</li> <li>• xmpp: Indicates that the handle supports Extensible Messaging and Presence Protocol (XMPP) based communication.</li> </ul>  |
| <b>SubType</b>                 | <p>The sub types of the handle. The following are the subtypes:</p> <ul style="list-style-type: none"> <li>• Subtypes for SIP based handles: <ul style="list-style-type: none"> <li>- <b>e164</b>: Type signifies that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix.</li> <li>- <b>username</b>: Type signifies that the handle is an alphanumeric value. For example, 1234567, xyz, or abc.xyz</li> <li>- <b>msrtc</b>: Type signifies that the handle supports communication with the Microsoft RTC server.</li> </ul> </li> <li>• Subtypes for SMTP: <ul style="list-style-type: none"> <li>msexchange: Type signifies that the handle supports communication with Microsoft SMTP server.</li> </ul> </li> <li>• Subtypes for ibm: <ol style="list-style-type: none"> <li>a. lotusnotes: Type signifies that handle is for lotus notes and domino calender.</li> <li>b. ibmsametime: Type signifies that handle is for IBM sametime</li> </ol> </li> <li>• Subtypes for xmpp: <ol style="list-style-type: none"> <li>a. jabber: Type signifies that handle supports communication with the Jabber service.</li> <li>b. googletalk: Type signifies that handle supports communication with the googletalk service.</li> </ol> </li> </ul> |
| <b>Fully Qualified Address</b> | <p>The fully qualified domain name or uniform resource identifier. The address can be an e-mail address, IM user or of an communication device using which user can send or receive messages.</p>  |

| Name          | Description  |
|---------------|--|
| <b>Add</b>    | Saves the new communication address or modified communication address information to the database. |
| <b>Cancel</b> | Cancels the adding a communication address operation.  |

## Session Manager

 **Note:**

The page displays the following fields if a communication profile of the user exists for the product.

| Name                                    | Description   |
|---|---|
| <b>Primary Session Manager</b>          | Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.   |
| <b>Secondary Session Manager</b>        | If a secondary Session Manager instance is selected, this Session Manager will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available. A selection is optional.   |
| <b>Origination Application Sequence</b> | Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. Note: if both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.   |
| <b>Termination Application Sequence</b> | <p>Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional.</p> <p> <b>Note:</b></p> <p>If both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.</p>   |
| <b>Survivability Server</b>             | For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. A selection is optional. Note: if a termination or origination application sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager. |
| <b>Home Location</b>                    | A Home Location can be specified to support mobility for the currently displayed user. When this user calls numbers that are not associated with an administered user, dial-plan rules (Routing > Dial Patterns) will be applied to complete the call based on this home location (Routing > Locations) regardless of the physical location of the SIP device used to make the call. A selection is mandatory.  |

## Messaging Profile

 **Note:**

The page displays the following fields if a messaging profile exists for the user.

| Name   | Description  |
|--|--|
| <b>System</b>  | The Messaging System on which you need to add the subscriber.  |
| <b>Template</b>  | The template (system defined and user defined) you want to associate with the subscriber.  |
| <b>Use Existing Subscriber on System</b>                     | Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.   |
| <b>Existing Mailbox Number</b>                               | The existing mailbox number that you want to associate with this profile. This value in the field is valid only if you select the <b>Use Existing Subscriber on System</b> check box.                            |
| <b>Mailbox Number</b>  | The mailbox number of the subscriber.  |
| <b>Password</b>  | The password for logging into the mailbox.   |
| <b>Delete Subscriber on Unassign of Subscriber from User</b> | Use this check box to specify whether you want to delete the subscriber mailbox from the Messaging Device or Communication System Management when you remove this messaging profile or when you delete the user. |

## Endpoint Profile

 **Note:**

The page displays the following fields if an endpoint profile exists for the user.

| Name/Button                   | Description   |
|-------------------------------|---|
| <b>System</b>                 | The Communication Manager on which you need to add the endpoint.  |
| <b>Use Existing Endpoints</b> | Use the check box if you want to use an existing endpoint extension to associate with this profile. If you do not select this check box, the available extensions are used. |
| <b>Extension</b>              | The extension of the endpoint you want to associate.  |
| <b>Search</b>                 | Lists the endpoints (existing or available) based on check box status of the <b>Use Existing Endpoints</b> field.   |
| <b>Template</b>               | The template (system defined or user defined) you want to associate with the endpoint. Select the template based on the set type you want to add.                           |
| <b>Set Type</b>               | The set type of the endpoint you want to associate. When you select a template, the system populates the corresponding set types.   |
| <b>Security Code</b>          | The security code for authorized access to the endpoint.  |

| Name/Button  | Description  |
|--|--|
| <b>Port</b>  | The relevant port for the set type you select.   |
| <b>Search</b>  | Lists the possible ports based on the selected set type.   |
| <b>Delete Endpoint on Unassign of Endpoint from User</b> | Use this check box to specify whether you want to delete the endpoint from the Communication Manager Device when you remove the association between the endpoint and the user or when you delete the user.   |
| <b>dtmfOverlp</b>  | <p>Appears when the <b>Set Type</b> field is H.323. This field specifies the touchtone signals that are used for dual-tone multifrequency (DTMF) telephone signaling. Valid entries include:</p> <ul style="list-style-type: none"> <li>• <b>in-band</b>- All G711 and G729 calls pass DTMF <b>in-band</b>. DTMF digits encoded within existing RTP media stream for G.711/G.729 calls. G. 723 is sent <b>out-of-band</b>.</li> <li>• <b>in-band-g711</b> – Only G711 calls pass DTMF in-band.</li> <li>• <b>out-of-band</b>- All IP calls pass DTMF <b>out-of-band</b>. For IP trunks, the digits are done with either Keypad IEs or H245 indications. This is the default for newly added H.323 signaling groups.</li> </ul> |

### Roles section

| Name                    | Description  |
|-------------------------|--|
| <b>Select check box</b> | Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account. |
| <b>Name</b>             | The name of the role.  |
| <b>Description</b>      | A brief description about the role.  |

| Button              | Description  |
|---------------------|--|
| <b>Assign Roles</b> | Opens the Assign Role page that you can use to assign roles to the user account.   |
| <b>Remove Roles</b> | Removes the selected role from the list of roles associated with the user account. |

### Group Membership section

| Name                    | Description                             |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select the group. |
| <b>Name</b>             | Name of the group.                      |
| <b>Type</b>             | Group type based on the resources.      |
| <b>Hierarchy</b>        | Position of the group in the hierarchy. |

| Name               | Description                          |
|--------------------|--------------------------------------|
| <b>Description</b> | A brief description about the group. |

| Button                   | Description   |
|--------------------------|---|
| <b>Add To group</b>      | Opens the Assign Groups page that you can use to add the user to a group. |
| <b>Remove From Group</b> | Removes the user from the selected group.                                 |

### Attribute Sets section

| Name                          | Description  |
|-------------------------------|--|
| <b>Select check box</b>       | Use this check box to select the attribute set.      |
| <b>Attribute Set</b>          | Name of the attribute set.                           |
| <b>Attribute Set Instance</b> | Name of the attribute set instance.                  |
| <b>Application</b>            | Name of the application that owns the attribute set. |
| <b>Description</b>            | A brief description about the attribute set.         |

| Button                       | Description   |
|------------------------------|---|
| <b>Assign Attribute Sets</b> | Opens the Select Attribute page that allows you to assign attribute sets to the user. |
| <b>Remove Attribute Set</b>  | Removes the selected attribute sets for a user .                                      |

### Default Contact List

| Name               | Description   |
|--------------------|---|
| <b>Name</b>        | Name of the contact list. The default name of the contact list is Default. You can change the name to any other appropriate name. |
| <b>Description</b> | A brief description of the contact list.  |

### Associated Contacts

| Name                    | Description  |
|-------------------------|--|
| <b>Last Name</b>        | Last name of the contact.  |
| <b>First Name</b>       | First name of the contact.   |
| <b>Scope</b>            | Categorization of the contact based on whether the contact is a public or private contact. |
| <b>Speed Dial</b>       | The value specifies whether the speed dial is set for the contact or not.                  |
| <b>Speed Dial Entry</b> | The reduced number that represents the speed dial number.                                  |

| Name                  | Description   |
|-----------------------|---|
| <b>Presence Buddy</b> | The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact. |

| Button                 | Description  |
|------------------------|--|
| <b>Edit</b>            | Opens the <b>Edit Contact List Member</b> page. Use this page to modify the information of the selected contact. |
| <b>New</b>             | Opens the <b>Attach Contacts</b> page. Use this page to select one or more contacts from the list of contacts.   |
| <b>Remove</b>          | Removes one or more contacts from the list of the associated contacts.   |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                   |
| <b>Filter: Enable</b>  | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.     |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.   |

### Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

| Name                   | Description                            |
|------------------------|--|
| <b>Last Name</b>       | Last name of the private contact.      |
| <b>First Name</b>      | First name of the private contact.     |
| <b>Display Name</b>    | Display name of the private contact.   |
| <b>Contact Address</b> | Address of the private contact.        |
| <b>Description</b>     | A brief description about the contact. |

| Button                 | Description  |
|------------------------|--|
| <b>Edit</b>            | Opens the <b>Edit Private Contact</b> page. Use this page to modify the information of the selected contact. |
| <b>New</b>             | Opens the <b>New Private Contact</b> page. Use this page to add a new private contact.                       |
| <b>Delete</b>          | Deletes the selected contacts.   |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.               |
| <b>Filter: Enable</b>  | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.   |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | <p>Modifies the user account.</p> <p> <b>Note:</b><br/>While restoring a deleted user, use this button to restore a deleted user.</p> |
| <b>Cancel</b> | <p>Cancels the operation of modifying the user information and takes you back to the User Management or User Profile View page.</p>  |

**Related topics:**

- [Modifying user accounts](#) on page 1390
- [Creating a new communication profile](#) on page 1560
- [Deleting a communication profile](#) on page 1561
- [Creating a new communication address for a communication profile](#) on page 1561
- [Modifying a communication address of a user](#) on page 1562
- [Deleting a communication address from a communication profile](#) on page 1563

## New User Profile field descriptions

Use this page to create a new user. This page has the following sections:

- General
- Identity
- Communication Profile
- Roles
- Group Membership
- Default Contact List
- Private Contacts

 **Note:**

The fields that are marked with an asterisk are mandatory and you must enter appropriate information in these fields.

### General section

| Name               | Description                         |
|--------------------|-------------------------------------|
| <b>Last Name</b>   | The last name of the user.          |
| <b>First Name</b>  | The first name of the user.         |
| <b>Description</b> | A brief description about the user. |

## Identity section

| Name                          | Description   |
|-------------------------------|---|
| <b>Login Name</b>             | A unique system login name for users that includes the users marked as deleted. It takes the form of username@domain. It is used to create the user's primary handle.   |
| <b>Authentication Type</b>    | Authentication type defines how the system performs user's authentication. The options are: <ul style="list-style-type: none"> <li>• <b>enterprise</b> — The enterprise authenticates user's login.</li> <li>• <b>basic</b> — The Avaya Authentication Service authenticates user's login.</li> </ul> |
| <b>Password</b>               | The initial password for logging in to the system.  |
| <b>Confirm Password</b>       | The initial password for verification.  |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.  |
| <b>Endpoint Display Name</b>  | The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.   |
| <b>Honorific</b>              | The personal title for address a user. This is typically a social title and not the work title.   |
| <b>Language Preference</b>    | The user's preferred written or spoken language.  |
| <b>Time Zone</b>              | The preferred time zone of the user.  |

## Identity > Address section

| Name                    | Description   |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select a address in the table.  |
| <b>Name</b>             | The name of the addressee.  |
| <b>Address Type</b>     | The type of address. The values are: <ul style="list-style-type: none"> <li>• Office</li> <li>• Home</li> </ul> |
| <b>Street</b>           | The name of the street.   |
| <b>Locality Name</b>    | The name of the city or town.   |
| <b>Postal Code</b>      | The postal code used by postal services to route mail to a destination. In United States this is Zip code.      |
| <b>Province</b>         | The full name of the province.  |
| <b>Country</b>          | The name of the country.  |

| Button                       | Description  |
|------------------------------|--|
| <b>New</b>                   | Opens the Add Address page. Use the page to add the address details. |
| <b>Edit</b>                  | Allows you to modify the address.                                    |
| <b>Delete</b>                | Deletes the selected address.  |
| <b>Choose Shared Address</b> | Opens the Choose Address page that you can use to choose a address.  |

### Communication Profile section

Use this section to create, modify and delete a communication profile for the user. Each communication profile may contain one or more communication addresses for a user.

| Name                 | Description  |
|----------------------|--|
| <b>Option button</b> | Use this button to view the details of the selected communication profile. |
| <b>Name</b>          | Name of the communication profile.   |

| Name          | Description  |
|---------------|--|
| <b>New</b>    | Creates a new communication profile for the user.                                    |
| <b>Delete</b> | Deletes the selected communication profile.  |
| <b>Save</b>   | Saves the communication profile information that you updated or added for a profile. |
| <b>Cancel</b> | Cancel the operation for adding a communication profile.                             |

This page displays the following fields when you click the **Add** button in the Communication Profile section.

| Name           | Description   |
|----------------|---|
| <b>Name</b>    | The name of the communication profile for the user.   |
| <b>Default</b> | The profile that is made default is the active profile. There can be only one active profile at a time. |

### Communication Address section

Use this section to create, modify and delete one or more communication addresses for the user.

| Name           | Description   |
|----------------|---|
| <b>Type</b>    | The type of the handle.                                     |
| <b>SubType</b> | The sub type of the handle.                                 |
| <b>Handle</b>  | A unique communication address of the user.                 |
| <b>Domain</b>  | The name of the domain with which the handle is registered. |

| Name          | Description  |
|---------------|--|
| <b>New</b>    | Displays the fields for adding a new communication address.                  |
| <b>Edit</b>   | Use this button to edit the information of a selected communication address. |
| <b>Delete</b> | Deletes the selected communication address.                                  |

The page displays the following fields when you click **New** and **Edit** in the Communication Address section. The following fields define the communication address for the user.

| Name           | Description  |
|----------------|--|
| <b>Type</b>    | <p>The types of the handle. The following are the different handle types:</p> <ul style="list-style-type: none"> <li>• sip: Indicates that the handle supports SIP based communication.</li> <li>• smtp: Indicates that the handle is an e-mail address and supports Simple Mail Transfer Protocol (SMTP) based communication.</li> <li>• ibm: Indicates that the handle is an IBM address.</li> <li>• xmpp: Indicates that the handle supports Extensible Messaging and Presence Protocol (XMPP) based communication.</li> </ul>  |
| <b>SubType</b> | <p>The sub types of the handle. The following are the subtypes:</p> <ul style="list-style-type: none"> <li>• Subtypes for SIP based handles: <ul style="list-style-type: none"> <li>a. e164: Type signifies that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix.</li> <li>b. username: Type signifies that the handle is an alphanumeric value. For example, 1234567, xyz, or abc.xyz</li> <li>c. msrtc: Type signifies that the handle supports communication with the Microsoft RTC server.</li> </ul> </li> <li>• Subtypes for SMTP: <ul style="list-style-type: none"> <li>msexchange: Type signifies that the handle supports communication with Microsoft SMTP server.</li> </ul> </li> <li>• Subtypes for ibm: <ul style="list-style-type: none"> <li>a. lotusnotes: Type signifies that the handle is for lotus notes and domino calender.</li> <li>b. ibmsametime: Type signifies that the handle is for IBM sametime</li> </ul> </li> <li>• Subtypes for xmpp: <ul style="list-style-type: none"> <li>a. jabber: Type signifies that the handle supports communication with the Jabber service.</li> <li>b. googletalk: Type signifies that the handle supports communication with the googletalk service.</li> </ul> </li> </ul> |

| Name                           | Description   |
|--------------------------------|---|
| <b>Fully Qualified Address</b> | The fully qualified domain name or uniform resource identifier. The address can be an e-mail address, IM user or an address of an communication device using which user can send or receive messages. |

| Name          | Description  |
|---------------|--|
| <b>Add</b>    | Saves the new communication address or modified communication address information in the database. |
| <b>Cancel</b> | Cancel the adding a communication address operation.   |

### Session Manager

 **Note:**

You may see these fields only if a communication profile for the user can be configured using the product.

| Name                                    | Description   |
|---|---|
| <b>Primary Session Manager</b>          | Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.   |
| <b>Secondary Session Manager</b>        | If a secondary Session Manager instance is selected, this Session Manager will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available. A selection is optional.   |
| <b>Origination Application Sequence</b> | Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. Note: if both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.   |
| <b>Termination Application Sequence</b> | Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional.<br><br> <b>Note:</b><br>If both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.  |
| <b>Survivability Server</b>             | For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. A selection is optional. Note: if a termination or origination application |

| Name                 | Description  |
|----------------------|--|
|                      | sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager.  |
| <b>Home Location</b> | A Home Location can be specified to support mobility for the currently displayed user. When this user calls numbers that are not associated with an administered user, dial-plan rules (Routing > Dial Patterns) will be applied to complete the call based on this home location (Routing > Locations) regardless of the physical location of the SIP device used to make the call. A selection is mandatory. |

## Messaging Profile



### Note:

You may see these fields only if a messaging profile can be configured for the user.

| Name   | Description  |
|--|--|
| <b>System</b>  | The Messaging System on which you need to add the subscriber.  |
| <b>Template</b>  | The template (system defined and user defined) you want to associate with the subscriber.  |
| <b>Use Existing Subscriber on System</b>                     | Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.   |
| <b>Existing Mailbox Number</b>                               | The existing mailbox number that you want to associate with this profile. This value in the field is valid only if you select the <b>Use Existing Subscriber on System</b> check box.                            |
| <b>Mailbox Number</b>  | The mailbox number of the subscriber.  |
| <b>Password</b>  | The password for logging into the mailbox.   |
| <b>Delete Subscriber on Unassign of Subscriber from User</b> | Use this check box to specify whether you want to delete the subscriber mailbox from the Messaging Device or Communication System Management when you remove this messaging profile or when you delete the user. |

## Endpoint Profile



### Note:

You may see these fields only if an endpoint profile can be configured for the user .

| Name/Button                   | Description   |
|-------------------------------|---|
| <b>System</b>                 | The Communication Manager on which you need to add the endpoint.  |
| <b>Use Existing Endpoints</b> | Use the check box if you want to use an existing endpoint extension to associate with this profile. If you do not select this check box, the available extensions are used. |

| Name/Button  | Description  |
|--|--|
| <b>Extension</b>   | The extension of the endpoint you want to associate.   |
| <b>Search</b>  | Lists the endpoints (existing or available) based on check box status of the <b>Use Existing Endpoint</b> field.   |
| <b>Template</b>  | The template (system defined or user defined) you want to associate with the endpoint. Select the template based on the set type you want to add.  |
| <b>Set Type</b>  | The set type of the endpoint you want to associate. When you select a template, the system populates the corresponding set types.  |
| <b>Security Code</b>                                     | The security code for authorized access to the endpoint.   |
| <b>Port</b>  | The relevant port for the set type you select.   |
| <b>Search</b>  | Lists the possible ports based on the selected set type.   |
| <b>Delete Endpoint on Unassign of Endpoint from User</b> | Use this check box to specify whether you want to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.   |
| <b>dtmfOverlp</b>  | <p>Appears when the <b>Set Type</b> field is H.323. This field specifies the touchtone signals that are used for dual-tone multifrequency (DTMF) telephone signaling. Valid entries include:</p> <ul style="list-style-type: none"> <li>• <b>in-band</b>- All G711 and G729 calls pass DTMF <b>in-band</b>. DTMF digits encoded within existing RTP media stream for G.711/G.729 calls. G. 723 is sent <b>out-of-band</b>.</li> <li>• <b>in-band-g711</b> – Only G711 calls pass DTMF in-band.</li> <li>• <b>out-of-band</b>- All IP calls pass DTMF <b>out-of-band</b>. For IP trunks, the digits are done with either Keypad IEs or H245 indications. This is the default for newly added H.323 signaling groups.</li> </ul> |

**Roles section**

| Name                    | Description  |
|-------------------------|--|
| <b>Select check box</b> | Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account. |
| <b>Name</b>             | The name of the role.  |
| <b>Description</b>      | A brief description about the role.  |

| Button              | Description  |
|---------------------|--|
| <b>Assign Roles</b> | Opens the Assign Role page that you can use to assign the roles to the user account. |

| Button              | Description  |
|---------------------|--|
| <b>Remove Roles</b> | Removes the selected role from the list of roles associated with the user account. |

### Group Membership section

| Name                    | Description                             |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select the group. |
| <b>Name</b>             | Name of the group.                      |
| <b>Type</b>             | Group type based on the resources.      |
| <b>Hierarchy</b>        | Position of the group in the hierarchy. |
| <b>Description</b>      | A brief description about the group.    |

| Button                   | Description   |
|--------------------------|---|
| <b>Add To group</b>      | Opens the Assign Groups page that you can use to add the user to a group. |
| <b>Remove From Group</b> | Removes the user from the selected group.                                 |

### Default Contact List

| Name               | Description   |
|--------------------|---|
| <b>Name</b>        | Name of the contact list. The default name of the contact list is Default. You can change the name to any other appropriate name. |
| <b>Description</b> | A brief description of the contact list.  |

### Associated Contacts

| Name                    | Description   |
|-------------------------|---|
| <b>Last Name</b>        | Last name of the contact.   |
| <b>First Name</b>       | First name of the contact.  |
| <b>Scope</b>            | Categorization of the contact based on whether the contact is a public or private contact.  |
| <b>Speed Dial</b>       | The value specifies whether the speed dial is set for the contact or not.   |
| <b>Speed Dial Entry</b> | The reduced number that represents the speed dial number.   |
| <b>Presence Buddy</b>   | The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact. |

| Button                 | Description  |
|------------------------|--|
| <b>Edit</b>            | Opens the <b>Edit Contact List Member</b> page. Use this page to modify the information of the selected contact. |
| <b>New</b>             | Opens the <b>Attach Contacts</b> page. Use this page to select one or more contacts from the list of contacts.   |
| <b>Remove</b>          | Removes one or more contacts from the list of the associated contacts.   |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                   |
| <b>Filter: Enable</b>  | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.     |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.   |

### Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

| Name                   | Description                            |
|------------------------|--|
| <b>Last Name</b>       | Last name of the private contact.      |
| <b>First Name</b>      | First name of the private contact.     |
| <b>Display Name</b>    | Display name of the private contact.   |
| <b>Contact Address</b> | Address of the private contact.        |
| <b>Description</b>     | A brief description about the contact. |

| Button                 | Description  |
|------------------------|--|
| <b>Edit</b>            | Opens the <b>Edit Contact List Member</b> page. Use this page to modify the information of the selected contact. |
| <b>New</b>             | Opens the <b>New Private Contact</b> page. Use this page to add a new private contact.                           |
| <b>Delete</b>          | Deletes the selected contacts.   |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                   |
| <b>Filter: Enable</b>  | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.     |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.   |

| Button        | Description                          |
|---------------|--------------------------------------|
| <b>Commit</b> | Creates the user account.            |
| <b>Cancel</b> | Cancels the user creation operation. |

**Related topics:**

- [Creating a new user profile](#) on page 1391
- [Creating a new communication profile](#) on page 1560
- [Deleting a communication profile](#) on page 1561
- [Creating a new communication address for a communication profile](#) on page 1561
- [Modifying a communication address of a user](#) on page 1562
- [Deleting a communication address from a communication profile](#) on page 1563
- [Adding a messaging profile for a user](#) on page 1565
- [Modifying a messaging profile of a user](#) on page 1566
- [Removing an association between a subscriber mailbox and a user](#) on page 1566
- [Deleting a subscriber mailbox](#) on page 1567
- [Adding a station profile for a user](#) on page 1568
- [Modifying a station profile of a user](#) on page 1569
- [Deleting a station profile of a user](#) on page 1570

---

## Managing default contact list of the user

### Adding a contact in the Default Contact list

You can use this feature to add a contact in the contact list of the user.

 **Note:**

To add a private contact, you must first create the private contact for the user. See “Adding a private contact for a user” for more information.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, perform one of the following steps:
    - Click **New** if you are adding a new contact for the user.
    - Select a user and click **Edit** if you are adding a new contact for an existing user.
  3. Click the **Default Contact List** link at the top of the page.
  4. Enter a brief description of the contact list in the **Description** field.
  5. Click **Add** in the Associated Contacts section.
  6. On the Attach Contacts page, select one or more contacts and click **Select**.
-

## Result

You can view the new contacts in the table displayed in the Associated Contacts section.

### Related topics:

- [Creating a new user profile](#) on page 1391
- [Assigning roles to a user](#) on page 1394
- [Assigning roles to a user](#) on page 1394
- [Assigning groups to a user](#) on page 1396
- [Assigning groups to a user](#) on page 1396
- [Adding a mailing address of the user](#) on page 1400
- [Adding a mailing address of the user](#) on page 1400
- [Creating a new communication profile](#) on page 1560
- [Creating a new communication profile](#) on page 1560
- [Attach Contacts field descriptions](#) on page 1598
- [Attach Contacts field descriptions](#) on page 1598
- [Adding a private contact for a user](#) on page 1602
- [Adding a private contact for a user](#) on page 1602
- [Adding a private contact for a user](#) on page 1602

## Modifying the membership details of a contact in a contact list

You can use this feature to set speed dial and presence buddy information for the contacts in the default contact list.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select a user and click **Edit**.
  3. On the User Profile Edit page, click the **Default Contact List** link at the top of the page.
  4. Select a contact from the Associated Contacts section and click **Edit**.
  5. Enter or modify the information in the fields in the Contact Membership Details section.  
You can only modify the information in the fields displayed in the Contact Membership Details section. The fields marked with an asterisk are mandatory fields.
  6. Click **Add** to save the changes.
-

**Related topics:**

[Edit Contact List Member field descriptions](#) on page 1599

[Edit Contact List Member field descriptions](#) on page 1599

## Viewing the membership details of a contact in the contact list

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select a user and click **View**.
  3. On the User Profile View page, click the **Default Contact List** link at the top of the page and select a contact.
  4. In the **Last Name** column, click the last name link.
- 

**Result**

The View Contact List Member page displays the details of the contact whose last name you have clicked.

**Related topics:**

[View Contact List Member field descriptions](#) on page 1600

## Deleting contacts from the default contact list

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select a user and click **Edit**.
  3. On the User Profile Edit page, click the **Default Contact List** link at the top of the page.
  4. Select one or more contacts from the Associated Contacts section and click **Delete**.
-

## Attach Contacts field descriptions

| Name                      | Description   |
|---------------------------|---|
| <b>Last Name</b>          | Last name of the contact.   |
| <b>First Name</b>         | First name of the contact.  |
| <b>Scope</b>              | Categorization of the contact based on whether the contact is a user, public or private contact.                  |
| <b>Display/Login Name</b> | Unique login name or display name of the contact.   |
| <b>Contact Address</b>    | Address of a private or public contact. No contact address is associated with a contact type user.                |
| <b>User Handles</b>       | Communication handles associated with the user. These handles are defined in the communication profile of a user. |
| <b>Filter: Disable</b>    | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                    |
| <b>Filter: Enable</b>     | Displays fields under selected columns that you can use to set the filter criteria. This is a toggle button.      |
| <b>Filter: Apply</b>      | Filters contacts based on the filter criteria.  |
| <b>Advanced Search</b>    | Displays fields that you can use to specify the search criteria to search for contacts.                           |

| Button        | Description   |
|---------------|---|
| <b>Select</b> | Adds the selected contact in the list of associated contacts. |

The page displays the following field when you click the **Advanced Search** button at the upper-right corner of the contact table.

| Name            | Description  |
|-----------------|--|
| <b>Criteria</b> | <p>Defines the search criteria for searching the contacts. Displays the following three fields:</p> <ul style="list-style-type: none"> <li>• Drop-down 1 - The list of criteria that you can use to search the contacts.</li> <li>• Drop-down 2 – The operators for evaluating the expression. Based on the search criterion which you select in the first drop-down field, only those operators that are applicable for the selected criterion are displayed in the second drop-down field.</li> <li>• Field 3 – The value for the search criterion.</li> </ul> |

### Related topics:

[Adding a contact in the Default Contact list](#) on page 1595

[Adding a contact in the Default Contact list](#) on page 1595

## Edit Contact List Member field descriptions

### Contact Membership Details

| Name                     | Description   |
|--------------------------|---|
| <b>Label</b>             | A text description for classifying this contact.  |
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.    |
| <b>Description</b>       | A brief description about the contact.  |
| <b>Presence Buddy</b>    | Use this check box to indicate whether you want to allow monitoring of the presence information of the contact.                       |
| <b>Speed Dial</b>        | Use this check box to indicate whether you want to allow speed dial for the contact.  |
| <b>Address/Handle</b>    | A fully qualified URI for interacting with the contact. This field is available only if you select the <b>Speed Dial</b> check box.   |
| <b>Speed Dial Entry</b>  | The reduced number that represents the speed dial number. This field is available only if you select the <b>Speed Dial</b> check box. |

### Contact Details

| Name                          | Description  |
|-------------------------------|--|
| <b>Last Name</b>              | Last name of the contact.  |
| <b>First Name</b>             | First name of the contact.   |
| <b>Middle Name</b>            | Middle name of the contact.  |
| <b>Description</b>            | A brief description about the contact.   |
| <b>Company</b>                | Name of contact's company  |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.                 |
| <b>Endpoint Display Name</b>  | Endpoint display name of the contact.  |
| <b>Language Preference</b>    | A list of languages from which you set one language as the preferred language for the contact. |
| <b>Update Time</b>            | The time when the contact information was last updated.  |
| <b>Source</b>                 | The source of provisioning the contact.  |

### Postal Address

| Name                 | Description   |
|----------------------|---|
| <b>Name</b>          | The name of the contact.  |
| <b>Address Type</b>  | The type that identifies whether mailing address is a home or office address. |
| <b>Street</b>        | The name of the street.   |
| <b>Locality Name</b> | The name of the city or town.   |
| <b>Postal Code</b>   | Postal code of the locality of the city or town.                              |
| <b>Province</b>      | The full name of the contact's province.                                      |
| <b>Country</b>       | The name of the contact's country.  |

### Contact Address

| Name                     | Description  |
|--------------------------|--|
| <b>Address</b>           | An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.      |
| <b>Type</b>              | Type signifies the communication medium used to interact with the user.  |
| <b>Category</b>          | Categorization of the address based on the location.   |
| <b>Label</b>             | A text description for classifying this contact.   |
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language. |

| Button     | Description                                     |
|------------|---|
| <b>Add</b> | Saves the modified information in the database. |

**Related topics:**

[Modifying the membership details of a contact in a contact list](#) on page 1596

[Modifying the membership details of a contact in a contact list](#) on page 1596

## View Contact List Member field descriptions

### Contact Membership Details

| Name         | Description                                      |
|--------------|--|
| <b>Label</b> | A text description for classifying this contact. |

| Name                     | Description   |
|--------------------------|---|
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.    |
| <b>Description</b>       | A brief description about the contact.  |
| <b>Presence Buddy</b>    | Use this check box to indicate whether you want to allow monitoring of the presence information of the contact.                       |
| <b>Speed Dial</b>        | Use this check box to indicate whether you want to allow speed dial for the contact.  |
| <b>Address/Handle</b>    | A fully qualified URI for interacting with the contact. This field is available only if you select the <b>Speed Dial</b> check box.   |
| <b>Speed Dial Entry</b>  | The reduced number that represents the speed dial number. This field is available only if you select the <b>Speed Dial</b> check box. |

### Contact Details

| Name                          | Description  |
|-------------------------------|--|
| <b>Last Name</b>              | Last name of the contact.  |
| <b>First Name</b>             | First name of the contact.   |
| <b>Middle Name</b>            | Middle name of the contact.  |
| <b>Description</b>            | A brief description about the contact.   |
| <b>Company</b>                | Name of contact's company  |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.                 |
| <b>Endpoint Display Name</b>  | Endpoint display name of the contact.  |
| <b>Language Preference</b>    | A list of languages from which you set one language as the preferred language for the contact. |
| <b>Update Time</b>            | The time when the contact information was last updated.  |
| <b>Source</b>                 | The source of provisioning the contact.  |

### Postal Address

| Name                 | Description   |
|----------------------|---|
| <b>Name</b>          | The name of the contact.  |
| <b>Address Type</b>  | The type that identifies whether mailing address is a home or office address. |
| <b>Street</b>        | The name of the street.   |
| <b>Locality Name</b> | The name of the city or town.   |

| Name        | Description                              |
|-------------|--|
| Postal Code | Name of the contact's company.           |
| Province    | The full name of the contact's province. |
| Country     | The name of the contact's country.       |

### Contact Address

| Name              | Description  |
|-------------------|--|
| Address           | An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.      |
| Type              | Type signifies the communication medium used to interact with the user.  |
| Category          | Categorization of the address based on the location.   |
| Label             | A text description for classifying this contact.   |
| Alternative Label | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language. |

#### Related topics:

[Viewing the membership details of a contact in the contact list](#) on page 1597

---

## Managing private contacts of a user

### Adding a private contact for a user

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. On the User Management page, perform one of the following steps:
  - Click **New** if you are adding a private contact for a new user.
  - Select a user and click **Edit** if you are adding a private contact for an existing user.
3. Click the **Private Contacts** link at the top of the page and click **New**.
4. On the New Private Contact page, enter the last name, first name, middle name, description, company name, localized display name, endpoint display name, language in the Contact Details section.

The fields marked with an asterisk are mandatory. You must enter a valid information in these fields.

5. In the Postal Address section, click **New** to choose a postal address for the contact. You can click **Choose Shared Address** to choose a shared address for a contact.
6. In the Contact Address section, click **New** to choose a contact address for the contact.
7. Click **Add** to add the private contact.
8. Click **Commit** to save the contact as the private contact of the user.

**Note:**

Ensure that all the mandatory fields marked with an asterisk have valid information, before you click **Commit**.

---

**Related topics:**

- [Creating a new user profile](#) on page 1391
- [Assigning roles to a user](#) on page 1394
- [Assigning roles to a user](#) on page 1394
- [Assigning groups to a user](#) on page 1396
- [Assigning groups to a user](#) on page 1396
- [Adding a mailing address of the user](#) on page 1400
- [Adding a mailing address of the user](#) on page 1400
- [Creating a new communication profile](#) on page 1560
- [Creating a new communication profile](#) on page 1560
- [Adding a contact in the Default Contact list](#) on page 1595
- [Adding a contact in the Default Contact list](#) on page 1595
- [Adding a contact in the Default Contact list](#) on page 1595
- [New Private Contact field descriptions](#) on page 1609

## Modifying the details of a private contact

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. On the User Management page, Select a user and click **Edit**.
3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page and select a contact.
4. click **Edit**

5. On the Edit Private Contact page, modify the contact's information.
6. Click **Add** to save the modified information.

---

**Related topics:**

[Edit Private Contact field descriptions](#) on page 1611

## Viewing the details of a private contact

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. On the User Management page, select a user and click **View**.
3. On the User Profile View page, click the **Private Contacts** link at the top of the page. When you click the **Private Contacts** link, you are taken to the Private Contacts section.
4. In the **Last Name** column, click the last name link.

---

**Result**

The View Contact page displays the details of the contact whose last name you have clicked.

**Related topics:**

[View Private Contact field descriptions](#) on page 1612

## Deleting private contacts of a user

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, select a user and click **Edit**.
  3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page.
  4. Select one or more contacts from the table displaying private contacts in the Private Contacts section.
  5. Click **Delete**.
  6. On the **Contact Delete Confirmation** page, click **Delete**.
-

## Adding a postal address of a private contact

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. On the User Management page, perform one of the following steps:
  - Click **New** if you are adding a postal address of a private contact for a new user.
  - Select a user and click **Edit** if you are adding a postal address of a private contact for an existing user.
3. Click the **Private Contacts** link at the top of the page and perform one of the following steps:
  - Click **New** if you are adding a postal address for a new private contact.
  - Select a private contact and click **Edit** if you are adding a postal address for an existing private contact.
4. On the New Private Contact page, click **New** in the Postal Address section.
5. On the Add Address page, enter the appropriate information in the respective fields. The fields marked with asterisk are mandatory. You must enter valid information in these fields.
6. Click **Add** to create a new postal address for the private contact.

---

### Related topics:

[Add Address field descriptions](#) on page 1402

## Modifying a postal address of a private contact

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. On the User Management page, select a user and click **Edit**.
3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page and select a contact.
4. Click **Edit**
5. On the Edit Private Contact page, select an address from the Postal Address section.

6. Click **Edit**.
  7. On the Edit Address page, modify the information in the respective fields.  
The fields marked with asterisk are mandatory. You must enter valid information in these fields.
  8. Click **Add** to save the modified address.
- 

**Related topics:**

[Edit Address field descriptions](#) on page 1403

## Deleting postal addresses of a private contact

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. On the User Management page, Select a user and click **Edit**.
  3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page and select a contact.
  4. click **Edit**
  5. On the Edit Private Contact page, select one or more addresses from the Postal Address section.
  6. Click **Delete**.
- 

## Choosing a shared address for a private contact

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. On the User Management page, perform one of the following steps:
  - Click **New** if you are choosing a shared address for a private contact of a new user.
  - Select a user and click **Edit** if you are choosing a shared address for a private contact of an existing user.
3. Click the **Private Contacts** link at the top of the page perform on of the following actions:

- Click **New** if you are adding the address for a new contact.
  - Select a contact and click **Edit** if you are adding the address for an existing contact.
4. Click **Choose Shared Address** in the Postal Address section.
  5. On the Choose Address page, select one or more shared addresses.
  6. Click **Select** to add these addresses for the private contact.

---

**Related topics:**

[Choose Address field descriptions](#) on page 1403

## Adding a contact address of a private contact

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. On the User Management page, perform one of the following steps:
  - Click **New** if you are adding a contact address of a private contact for a new user.
  - Select a user and click **Edit** if you are adding a contact address of a private contact for an existing user.
3. Click the **Private Contacts** link at the top of the page and perform one of the following steps:
  - Click **New** if you are adding a contact address for a new private contact.
  - Select a public contact and click **Edit** if you are adding a contact address for an existing private contact.
4. On the New Private Contact page, click **New** in the Contact Address section.
5. On the Add Address page, enter the appropriate information in the respective fields. The fields marked with asterisk are mandatory. You must enter a valid information in these fields to successfully create a private contact.
6. Click **Add** to create a new contact address for the private contact.

---

**Related topics:**

[Add Address field descriptions](#) on page 1614

## Modifying a contact address of a private contact

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. On the User Management page, Select a user and click **Edit**.
3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page and select a contact.
4. click **Edit**
5. On the Edit Private Contact page, select a contact address from the Contact Address section.
6. Click **Edit**.
7. On the Edit Address page, modify the information in the respective fields.  
The fields marked with asterisk are mandatory. You must enter valid information in these fields.
8. Click **Add** to save the modified address.
9. On the User Profile Edit page, click **Commit**.



**Note:**

Ensure that all the mandatory fields that is fields marked with red asterisk have valid information, before you click **Commit**.

---

**Related topics:**

[Edit Address field descriptions](#) on page 1615

## Deleting contact addresses of a private contact

---

1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
2. On the User Management page, select a user and click **Edit**.
3. On the User Profile Edit page, click the **Private Contacts** link at the top of the page and select a contact.
4. click **Edit**.

5. On the Edit Private Contact page, select one or more addresses from the Contact Address section.
6. Click **Delete**.

## New Private Contact field descriptions

### Contact Details

| Name                          | Description  |
|-------------------------------|--|
| <b>Last Name</b>              | Last name of the contact.  |
| <b>First Name</b>             | First name of the contact.   |
| <b>Middle Name</b>            | Middle name of the contact.  |
| <b>Description</b>            | A brief description about the contact.   |
| <b>Company</b>                | Name of contact's company  |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.                 |
| <b>Endpoint Display Name</b>  | Endpoint display name of the contact.  |
| <b>Language Preference</b>    | A list of languages from which you set one language as the preferred language for the contact. |
| <b>Update Time</b>            | The time when the contact information was last updated.  |
| <b>Source</b>                 | The source of provisioning the contact.  |

### Postal Address

| Name                 | Description   |
|----------------------|---|
| <b>Name</b>          | The name of the contact.  |
| <b>Address Type</b>  | The type that identifies whether mailing address is a home or office address.         |
| <b>Street</b>        | The name of the street.   |
| <b>Locality Name</b> | The name of the city or town of the contact.  |
| <b>Postal Code</b>   | Postal code of the of the city or town where the contact's office or home is located. |
| <b>Province</b>      | The full name of the province where the contact's office or home is located.          |
| <b>Country</b>       | The name of the country where the contact's office or home is located.                |

| Button                       | Description   |
|------------------------------|---|
| <b>Edit</b>                  | Opens the <b>Edit Address</b> page. Use this page to add a new postal address of the private contact.         |
| <b>New</b>                   | Opens the <b>Add Address</b> page. Use this page to modify an existing postal address of the private contact. |
| <b>Delete</b>                | Deletes the selected private contacts.  |
| <b>Choose Shared Address</b> | Opens the <b>Choose Address</b> page. Use this page to choose addresses of the private contact.               |

### Contact Address

| Name                     | Description  |
|--------------------------|--|
| <b>Address</b>           | An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.      |
| <b>Type</b>              | Type signifies the communication medium used to interact with the user.  |
| <b>Category</b>          | Categorization of the address based on the location.   |
| <b>Label</b>             | A text description for classifying this contact.   |
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language. |

| Button        | Description   |
|---------------|---|
| <b>Edit</b>   | Opens the <b>Edit Address</b> page. Use this page to edit a contact address of the private contact. |
| <b>New</b>    | Opens the <b>Add Address</b> page. Use this page to add a contact address of the private contact.   |
| <b>Delete</b> | Deletes the selected private contacts.  |

| Button     | Description  |
|------------|--|
| <b>Add</b> | Creates a new contact.<br><br> <b>Note:</b><br>You must enter valid information in the mandatory fields to successfully create a new contact. |

**Related topics:**

[Adding a private contact for a user](#) on page 1602

## Edit Private Contact field descriptions

### Contact Details

| Name                          | Description  |
|-------------------------------|--|
| <b>Last Name</b>              | Last name of the contact.  |
| <b>First Name</b>             | First name of the contact.   |
| <b>Middle Name</b>            | Middle name of the contact.  |
| <b>Description</b>            | A brief description about the contact.   |
| <b>Company</b>                | Name of contact's company  |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.                 |
| <b>Endpoint Display Name</b>  | Endpoint display name of the contact.  |
| <b>Language Preference</b>    | A list of languages from which you set one language as the preferred language for the contact. |
| <b>Update Time</b>            | The time when the contact information was last updated.  |
| <b>Source</b>                 | The source of provisioning the contact.  |

### Postal Address

| Name                 | Description   |
|----------------------|---|
| <b>Name</b>          | The name of the contact.  |
| <b>Address Type</b>  | The type that identifies whether mailing address is a home or office address.         |
| <b>Street</b>        | The name of the street.   |
| <b>Locality Name</b> | The name of the city or town.   |
| <b>Postal Code</b>   | Postal code of the of the city or town where the contact's office or home is located. |
| <b>Province</b>      | The full name of the province where the contact's office or home is located.          |
| <b>Country</b>       | The name of the country where the contact's office or home is located.                |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the <b>Edit Address</b> page. Use this page to add a new postal address of the private contact.         |
| <b>New</b>  | Opens the <b>Add Address</b> page. Use this page to modify an existing postal address of the private contact. |

| Button                       | Description   |
|------------------------------|---|
| <b>Delete</b>                | Deletes the selected private contacts.  |
| <b>Choose Shared Address</b> | Opens the <b>Choose Address</b> page. Use this page to choose addresses of the private contact. |

### Contact Address

| Name                     | Description  |
|--------------------------|--|
| <b>Address</b>           | An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.      |
| <b>Type</b>              | Type signifies the communication medium used to interact with the user.  |
| <b>Category</b>          | Categorization of the address based on the location.   |
| <b>Label</b>             | A text description for classifying this contact.   |
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language. |

| Button        | Description   |
|---------------|---|
| <b>Edit</b>   | Opens the <b>Edit Address</b> page. Use this page to edit a contact address of the private contact. |
| <b>New</b>    | Opens the <b>Add Address</b> page. Use this page to add a contact address of the private contact.   |
| <b>Delete</b> | Deletes the selected private contacts.  |

| Button     | Description                                     |
|------------|---|
| <b>Add</b> | Saves the modified information in the database. |

#### Related topics:

[Modifying the details of a private contact](#) on page 1603

## View Private Contact field descriptions

### Contact Details

| Name               | Description                 |
|--------------------|-----------------------------|
| <b>Last Name</b>   | Last name of the contact.   |
| <b>First Name</b>  | First name of the contact.  |
| <b>Middle Name</b> | Middle name of the contact. |

| Name                          | Description  |
|-------------------------------|--|
| <b>Description</b>            | A brief description about the contact.   |
| <b>Company</b>                | Name of contact's company  |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.                 |
| <b>Endpoint Display Name</b>  | Endpoint display name of the contact.  |
| <b>Language Preference</b>    | A list of languages from which you set one language as the preferred language for the contact. |
| <b>Update Time</b>            | The time when the contact information was last updated.  |
| <b>Source</b>                 | The source of provisioning the contact.  |

### Postal Address

| Name                 | Description   |
|----------------------|---|
| <b>Name</b>          | The name of the contact.  |
| <b>Address Type</b>  | The type that identifies whether mailing address is a home or office address. |
| <b>Street</b>        | The name of the street.   |
| <b>Locality Name</b> | The name of the city or town.   |
| <b>Postal Code</b>   | Name of the contact's company.  |
| <b>Province</b>      | The full name of the contact's province.                                      |
| <b>Country</b>       | The name of the contact's country.  |

### Contact Address

| Name                     | Description  |
|--------------------------|--|
| <b>Address</b>           | An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.      |
| <b>Type</b>              | Type signifies the communication medium used to interact with the user.  |
| <b>Category</b>          | Categorization of the address based on the location.   |
| <b>Label</b>             | A text description for classifying this contact.   |
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language. |

| Button      | Description  |
|-------------|--|
| <b>Edit</b> | Opens the View Private Contact page. You can use this page to edit the details of the contact. |

**Related topics:**

[Viewing the details of a private contact](#) on page 1604

## Add Address field descriptions

Use this page to add communication address of the contact.

| Name                     | Description  |
|--------------------------|--|
| <b>Address</b>           | An address that you can use to communicate with the contact. This can be a phone number, e-mail address, sip or IM of the contact. The format of the address must conform to the type of address that you selected in the <b>Type</b> field.   |
| <b>Type</b>              | Type of address. The following are the types of address: <ul style="list-style-type: none"> <li>• phone: An address of this type supports phone numbers.</li> <li>• sip: An address of this type supports sip based communication.</li> <li>• msrtc An address of this type supports communication with a Microsoft RTC Server.</li> <li>• ibmsametime: An address of this type supports communication with IBM Sametime,</li> <li>• xmpp: An address of this type supports xmpp based communication.</li> <li>• smtp: An address of this type supports communication with the SMTP server.</li> </ul> |
| <b>Category</b>          | Categorization of the address based on the location.   |
| <b>Label</b>             | A text description for classifying this contact.   |
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.   |

| Button     | Description   |
|------------|---|
| <b>Add</b> | Adds the contact address of the public contact in the database. |

**Related topics:**

[Adding a contact address of a private contact](#) on page 1607

[Adding a contact address of a public contact](#) on page 1659

## Edit Address field descriptions

Use this page to edit the details of a contact's communication address.

| Name                     | Description  |
|--------------------------|--|
| <b>Address</b>           | An address that you can use to communicate with the contact. This can be a phone number, e-mail address, sip or IM of the contact. The format of the address must conform to the type of address that you selected in the <b>Type</b> field.   |
| <b>Type</b>              | Type of address. The following are the types of address: <ul style="list-style-type: none"> <li>• phone: An address of this type supports phone numbers.</li> <li>• sip: An address of this type supports sip based communication.</li> <li>• msrtc An address of this type supports communication with a Microsoft RTC Server.</li> <li>• ibmsametime: An address of this type supports communication with IBM Sametime,</li> <li>• xmpp: An address of this type supports xmpp based communication.</li> <li>• smtp: An address of this type supports communication with the SMTP server.</li> </ul> |
| <b>Category</b>          | Categorization of the address based on the location.   |
| <b>Label</b>             | A text description for classifying this contact.   |
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.   |

| Button     | Description                                     |
|------------|---|
| <b>Add</b> | Saves the modified information in the database. |

### Related topics:

[Modifying a contact address of a private contact](#) on page 1608

[Modifying the details of a public contact](#) on page 1660

---

## User Management field descriptions

The User Management module is the primary master of the user profile. It provides Avaya's customers and Avaya's products with a single point of administration for creating, viewing, modifying, and deleting users. The page has two sections. The upper section contains buttons that you can use to:

- create, view, modify and delete users
- assign roles, attributes to a user
- add a user to a group
- perform Lightweight Directory Access Protocol (LDAP) synchronization

The lower section contains a table that displays information about the user.

| Name              | Description   |
|-------------------|---|
| <b>Status</b>     | The current login status of the user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status. |
| <b>Name</b>       | Name of the user.   |
| <b>Login Name</b> | Unique name that gives access to the system.  |
| <b>Last Login</b> | Date and time when the user successfully logged into the system   |
| <b>Handle</b>     | A unique communication address of the user.   |

| Button                                     | Description  |
|--|--|
| <b>View</b>                                | Opens User Profile View page that you can use to view the details of the selected user.                    |
| <b>Edit</b>                                | Opens the User Profile Edit page that you can use to modify the details of the selected user.              |
| <b>New</b>                                 | Opens the New User Profile page that you can use to create a new user.                                     |
| <b>Duplicate</b>                           | Opens the User Profile Duplicate page that you can use create a duplicate user.                            |
| <b>Delete</b>                              | Opens the User Delete Confirmation page that you can use to temporarily delete the selected users.         |
| <b>More Actions &gt; Assign Roles</b>      | Opens the Assign Roles page that you can use to assign roles to the selected users.                        |
| <b>More Actions &gt; Add To Group</b>      | Opens the Assign Groups page that you can use to assign groups to the selected users .                     |
| <b>More Actions &gt; Show Deleted User</b> | Opens the Deleted Users page that you can use to view, permanently delete, and restore the deleted users . |
| <b>Advanced Search</b>                     | Displays fields that you can use to specify the search criteria for searching a user.                      |
| <b>Filter: Enable</b>                      | Displays fields under select columns that you can use to set filter criteria. This is a toggle button.     |
| <b>Filter: Disable</b>                     | Hides the column filter fields without resetting the filter criteria. This is a toggle button.             |

| Button               | Description                                    |
|----------------------|--|
| <b>Filter: Apply</b> | Filters users based on the filter criteria.    |
| <b>Select: All</b>   | Selects all the users in the table.            |
| <b>Select: None</b>  | Clears the check box selections.               |
| <b>Refresh</b>       | Refreshes the user's information in the table. |

### Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the upper-right corner of the page.

| Name            | Description  |
|-----------------|--|
| <b>Criteria</b> | <p>Displays the following three fields:</p> <ul style="list-style-type: none"> <li>• Drop-down 1 - The list of criteria that you can use to search users.</li> <li>• Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field.</li> <li>• Field 3 – The value for the search criterion. The Users Management service retrieves and displays users that match this value.</li> </ul> |

---

## User Profile View field descriptions

Use this page to view the details of the selected user account.

### General section

| Name               | Description                      |
|--------------------|----------------------------------|
| <b>Last Name</b>   | The last name of the user.       |
| <b>First Name</b>  | The first name of the user.      |
| <b>Description</b> | A brief description of the user. |
| <b>User Type</b>   | The primary user types.          |

### Identity section

| Name                       | Description   |
|----------------------------|---|
| <b>Login Name</b>          | The unique system login name given to the user. It takes the form of username@domain. You can use the login name to create the user's primary handle. |
| <b>Authentication Type</b> | Authentication type defines how the system performs user's authentication. The options are:   |

| Name                          | Description  |
|-------------------------------|--|
|                               | <ul style="list-style-type: none"> <li>• <b>enterprise</b> — User's login is authenticated by the enterprise.</li> <li>• <b>basic</b> — User's login is authenticated by an Avaya Authentication Service.</li> </ul> |
| <b>Password</b>               | The initial password for logging in to the system.   |
| <b>Confirm Password</b>       | The initial password for verification.   |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.   |
| <b>Endpoint Display Name</b>  | The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.  |
| <b>Honorific</b>              | The personal title for address a user. This is typically a social title and not the work title.  |
| <b>Language Preference</b>    | The user's preferred written or spoken language.   |
| <b>Time Zone</b>              | The preferred time zone of the user.   |

### Identity > Address section

| Name                 | Description  |
|----------------------|--|
| <b>Name</b>          | The name of the user.  |
| <b>Address Type</b>  | Type of the address. The following are the types: <ul style="list-style-type: none"> <li>• Office</li> <li>• Home</li> </ul> |
| <b>Street</b>        | The name of the street.  |
| <b>Locality Name</b> | The name of the city or town.  |
| <b>Postal Code</b>   | The postal code used by postal services to route mail to a destination. In United States this is Zip code.                   |
| <b>Province</b>      | The full name of the province.   |
| <b>Country</b>       | The name of the country.   |

### Communication Profile section

| Name                 | Description  |
|----------------------|--|
| <b>Option button</b> | Use this button to view the details of the selected communication profile. |
| <b>Name</b>          | Name of the communication profile.   |

| Name           | Description   |
|----------------|---|
| <b>Name</b>    | The name of the communication profile for the user.   |
| <b>Default</b> | The profile that is made default is the active profile. There can be only one active profile at a time. |

### Communication Address section

| Name           | Description   |
|----------------|---|
| <b>Type</b>    | The type of the handle.                                     |
| <b>SubType</b> | The sub type of the handle.                                 |
| <b>Handle</b>  | .A unique communication address for the user.               |
| <b>Domain</b>  | The name of the domain with which the handle is registered. |

### Session Manager



**Note:**

The page displays the following fields if a communication profile of the user exists for the product.

| Name                                    | Description  |
|---|--|
| <b>Primary Session Manager</b>          | Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.                                    |
| <b>Secondary Session Manager</b>        | If a secondary Session Manager instance is selected, this Session Manager will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available. A selection is optional.  |
| <b>Origination Application Sequence</b> | Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. Note: if both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.  |
| <b>Termination Application Sequence</b> | Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional.<br><br> <b>Note:</b><br>If both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences. |
| <b>Survivability Server</b>             | For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session   |

| Name                 | Description   |
|----------------------|---|
|                      | <p>Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. A selection is optional. Note: if a termination or origination application sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager.</p> |
| <b>Home Location</b> | <p>A Home Location can be specified to support mobility for the currently displayed user. When this user calls numbers that are not associated with an administered user, dial-plan rules (Routing &gt; Dial Patterns) will be applied to complete the call based on this home location (Routing &gt; Locations) regardless of the physical location of the SIP device used to make the call. A selection is optional</p>   |

### Messaging Profile



**Note:**

The page displays the following fields if a messaging profile exists for the user.

| Name   | Description  |
|--|--|
| <b>System</b>  | The Messaging System on which you need to add the subscriber.  |
| <b>Template</b>  | The template (system defined and user defined) you want to associate with the subscriber.  |
| <b>Use Existing Subscriber on System</b>                     | Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.   |
| <b>Existing Mailbox Number</b>                               | The existing mailbox number that you want to associate with this profile. This value in the field is valid only if you select the <b>Use Existing Subscriber on System</b> check box.                            |
| <b>Mailbox Number</b>  | The mailbox number of the subscriber.  |
| <b>Password</b>  | The password for logging into the mailbox.   |
| <b>Delete Subscriber on Unassign of Subscriber from User</b> | Use this check box to specify whether you want to delete the subscriber mailbox from the Messaging Device or Communication System Management when you remove this messaging profile or when you delete the user. |

### Endpoint Profile



**Note:**

The page displays the following fields if an endpoint profile exists for the user.

| Name/Button  | Description   |
|--|---|
| <b>System</b>  | The Communication Manager on which you need to add the endpoint.  |
| <b>Use Existing Endpoints</b>                            | Use the check box if you want to use an existing endpoint extension to associate with this profile. If you do not select this check box, the available extensions are used.   |
| <b>Extension</b>   | The extension of the station you want to associate.   |
| <b>Search</b>  | Lists the endpoints (existing or available) based on check box status of the <b>Use Existing Endpoints</b> field.   |
| <b>Template</b>  | The template (system defined or user defined) you want to associate with the endpoint. Select the template based on the set type you want to add.   |
| <b>Set Type</b>  | The set type of the endpoint you want to associate. When you select a template, the system populates the corresponding set types.   |
| <b>Security Code</b>                                     | The security code for authorized access to the endpoint.  |
| <b>Port</b>  | The relevant port for the set type you select.  |
| <b>Search</b>  | Lists the possible ports based on the selected set type.  |
| <b>Delete Endpoint on Unassign of Endpoint from User</b> | Use this check box to specify whether you want to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.  |
| <b>dtmfOverlp</b>  | <p>Appears when the <b>Set Type</b> field is H.323. This field specifies the touchtone signals that are used for dual-tone multifrequency (DTMF) telephone signaling. Valid entries include:</p> <ul style="list-style-type: none"> <li>• <b>in-band</b>- All G711 and G729 calls pass DTMF <b>in-band</b>. DTMF digits encoded within existing RTP media stream for G.711/G.729 calls. G.723 is sent <b>out-of-band</b>.</li> <li>• <b>in-band-g711</b> – Only G711 calls pass DTMF in-band.</li> <li>• <b>out-of-band</b>- All IP calls pass DTMF <b>out-of-band</b>. For IP trunks, the digits are done with either Keypad IEs or H245 indications. This is the default for newly added H.323 signaling groups.</li> </ul> |

## Roles section

| Name               | Description                         |
|--------------------|-------------------------------------|
| <b>Name</b>        | The name of the role.               |
| <b>Description</b> | A brief description about the role. |

### Group Membership section

| Name             | Description                             |
|------------------|---|
| Select check box | Select the group.                       |
| Name             | Name of the group.                      |
| Type             | Group type based on the resources.      |
| Hierarchy        | Position of the group in the hierarchy. |
| Description      | A brief description about the group.    |

### Attribute Sets section

| Name                   | Description  |
|------------------------|--|
| Select check box       | Select the attribute set.                            |
| Attribute Set          | Name of the attribute set.                           |
| Attribute Set Instance | Name of the attribute set instance.                  |
| Application            | Name of the application that owns the attribute set. |
| Description            | A brief description about the attribute set.         |

### Default Contact List section

| Name        | Description   |
|-------------|---|
| Name        | Name of the contact list. The default name of the contact list is Default. You can change the name to any other appropriate name. |
| Description | A brief description of the contact list.  |

### Associated Contacts section

| Name             | Description   |
|------------------|---|
| Last Name        | Last name of the contact.   |
| First Name       | First name of the contact.  |
| Scope            | Categorization of the contact based on whether the contact is a public or private contact.  |
| Speed Dial       | The value specifies whether the speed dial is set for the contact or not.   |
| Speed Dial Entry | The reduced number that represents the speed dial number.   |
| Presence Buddy   | The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact. |

| Button                 | Description  |
|------------------------|--|
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.               |
| <b>Filter: Enable</b>  | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.   |

### Private Contacts section

Use this section to add new private contacts, modify and deletes existing contacts.

| Name                   | Description                            |
|------------------------|--|
| <b>Last Name</b>       | Last name of the private contact.      |
| <b>First Name</b>      | First name of the private contact.     |
| <b>Display Name</b>    | Display name of the private contact.   |
| <b>Contact Address</b> | Address of the private contact.        |
| <b>Description</b>     | A brief description about the contact. |

| Button                 | Description  |
|------------------------|--|
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.               |
| <b>Filter: Enable</b>  | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.   |

| Button      | Description   |
|-------------|---|
| <b>Edit</b> | Opens the User Profile Edit page. Use the User Profile Edit page to modify the details of the user account. |
| <b>Done</b> | Closes the User Profile View page and takes you back to the User Management page.                           |

#### Related topics:

[Viewing details of a user](#) on page 1390

---

## User Profile Edit field descriptions

Use this page to modify the details of a user account.

### General section

| Name               | Description                         |
|--------------------|-------------------------------------|
| <b>Last Name</b>   | The last name of the user.          |
| <b>First Name</b>  | The first name of the user.         |
| <b>Description</b> | A brief description about the user. |

### Identity section

| Name                          | Description  |
|-------------------------------|--|
| <b>Login Name</b>             | This is the unique system login name given to the user. It takes the form of username@domain. It is used to create the user's primary handle.  |
| <b>Authentication Type</b>    | Authentication type defines how the system performs user's authentication. The options are: <ul style="list-style-type: none"> <li>• <b>enterprise</b> — User's login is authenticated by the enterprise.</li> <li>• <b>basic</b> — User's login is authenticated by an Avaya Authentication Service.</li> </ul> |
| <b>Password</b>               | The initial password for logging in to the system.   |
| <b>Confirm Password</b>       | The initial password for verification.   |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.   |
| <b>Endpoint Display Name</b>  | The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.  |
| <b>Honorific</b>              | The personal title for address a user. This is typically a social title and not the work title.  |
| <b>Language Preference</b>    | The user's preferred written or spoken language.   |
| <b>Time Zone</b>              | The preferred time zone of the user.   |

### Identity > Address section

| Name                    | Description   |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select the address.   |
| <b>Name</b>             | The name of the user.   |
| <b>Address Type</b>     | The type of address. The values are: <ul style="list-style-type: none"> <li>• Office</li> <li>• Home</li> </ul> |

| Name                 | Description  |
|----------------------|--|
| <b>Street</b>        | The name of the street.  |
| <b>Locality Name</b> | The name of the city or town.  |
| <b>Postal Code</b>   | The postal code used by postal services to route mail to a destination. In United States this is Zip code. |
| <b>Province</b>      | The full name of the province.   |
| <b>Country</b>       | The name of the country.   |

| Button                       | Description   |
|------------------------------|---|
| <b>New</b>                   | Opens the Add Address page that you can use to add the address details.     |
| <b>Edit</b>                  | Opens the Edit Address page that you can use to modify the address details. |
| <b>Delete</b>                | Deletes the selected address.   |
| <b>Choose Shared Address</b> | Opens the Choose Address page that you can use to choose a address.         |

### Communication Profile section

Use this section to create, modify and delete a communication profile for the user. Each communication profile may contain one or more communication addresses for a user.

| Name                 | Description  |
|----------------------|--|
| <b>Option button</b> | Use this button to view the details of the selected communication profile. |
| <b>Name</b>          | Name of the communication profile.   |

| Name          | Description  |
|---------------|--|
| <b>New</b>    | Creates a new communication profile for the user.                                    |
| <b>Delete</b> | Deletes the selected communication profile.  |
| <b>Save</b>   | Saves the communication profile information that you updated or added for a profile. |
| <b>Cancel</b> | Cancel the operation for adding a communication profile.                             |

The page displays the following fields when you click the **Add** button in the Communication Profile section.

| Name           | Description   |
|----------------|---|
| <b>Name</b>    | The name of the communication profile for the user.   |
| <b>Default</b> | The profile that is made default is the active profile. There can be only one active profile at a time. |

### Communication Address section

Use this section to create, modify and delete one or more communication addresses for the user.

| Name           | Description   |
|----------------|---|
| <b>Type</b>    | The type of the handle.                                     |
| <b>SubType</b> | The sub type of the handle.                                 |
| <b>Handle</b>  | .A unique communication address for the user.               |
| <b>Domain</b>  | The name of the domain with which the handle is registered. |

| Name          | Description  |
|---------------|--|
| <b>New</b>    | Displays the fields for adding a new communication address.                  |
| <b>Edit</b>   | Use this button to edit the information of a selected communication address. |
| <b>Delete</b> | Deletes the selected communication address.                                  |

The page displays the following fields when you click **New** and **Edit** in the Communication Address section.

| Name           | Description   |
|----------------|---|
| <b>Type</b>    | <p>The types of the handle. The following are the different handle types:</p> <ul style="list-style-type: none"> <li>• sip: Indicates that the handle supports SIP based communication.</li> <li>• smtp: Indicates that the handle is an e-mail address and supports Simple Mail Transfer Protocol (SMTP) based communication.</li> <li>• ibm: Indicates that the handle is an IBM address.</li> <li>• xmpp: Indicates that the handle supports Extensible Messaging and Presence Protocol (XMPP) based communication.</li> </ul>   |
| <b>SubType</b> | <p>The sub types of the handle. The following are the subtypes:</p> <ul style="list-style-type: none"> <li>• Subtypes for SIP based handles: <ul style="list-style-type: none"> <li>- <b>e164</b>: Type signifies that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix.</li> <li>- <b>username</b>: Type signifies that the handle is an alphanumeric value. For example, 1234567, xyz, or abc.xyz</li> <li>- <b>msrtc</b>: Type signifies that the handle supports communication with the Microsoft RTC server.</li> </ul> </li> <li>• Subtypes for SMTP: <ul style="list-style-type: none"> <li>msexchange: Type signifies that the handle supports communication with Microsoft SMTP server.</li> </ul> </li> <li>• Subtypes for ibm:</li> </ul> |

| Name                           | Description   |
|--------------------------------|---|
|                                | <ul style="list-style-type: none"> <li>a. lotusnotes: Type signifies that handle is for lotus notes and domino calender.</li> <li>b. ibmsametime: Type signifies that handle is for IBM sametime</li> <li>• Subtypes for xmpp: <ul style="list-style-type: none"> <li>a. jabber: Type signifies that handle supports communication with the Jabber service.</li> <li>b. googletalk: Type signifies that handle supports communication with the googletalk service.</li> </ul> </li> </ul> |
| <b>Fully Qualified Address</b> | The fully qualified domain name or uniform resource identifier. The address can be an e-mail address, IM user or of an communication device using which user can send or receive messages.  |

| Name          | Description  |
|---------------|--|
| <b>Add</b>    | Saves the new communication address or modified communication address information to the database. |
| <b>Cancel</b> | Cancel the adding a communication address operation.   |

## Session Manager

 **Note:**

The page displays the following fields if a communication profile of the user exists for the product.

| Name                                    | Description   |
|---|---|
| <b>Primary Session Manager</b>          | Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required. |
| <b>Secondary Session Manager</b>        | If a secondary Session Manager instance is selected, this Session Manager will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available. A selection is optional.   |
| <b>Origination Application Sequence</b> | Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. Note: if both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.   |
| <b>Termination Application Sequence</b> | Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional.  |

| Name                        | Description   |
|-----------------------------|---|
|                             |  <b>Note:</b><br>If both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.  |
| <b>Survivability Server</b> | For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. A selection is optional. Note: if a termination or origination application sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager. |
| <b>Home Location</b>        | A Home Location can be specified to support mobility for the currently displayed user. When this user calls numbers that are not associated with an administered user, dial-plan rules (Routing > Dial Patterns) will be applied to complete the call based on this home location (Routing > Locations) regardless of the physical location of the SIP device used to make the call. A selection is mandatory.  |

### Messaging Profile

 **Note:**

The page displays the following fields if a messaging profile exists for the user.

| Name                                     | Description   |
|--|---|
| <b>System</b>                            | The Messaging System on which you need to add the subscriber.   |
| <b>Template</b>                          | The template (system defined and user defined) you want to associate with the subscriber.   |
| <b>Use Existing Subscriber on System</b> | Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.  |
| <b>Existing Mailbox Number</b>           | The existing mailbox number that you want to associate with this profile. This value in the field is valid only if you select the <b>Use Existing Subscriber on System</b> check box. |
| <b>Mailbox Number</b>                    | The mailbox number of the subscriber.   |
| <b>Password</b>                          | The password for logging into the mailbox.  |
| <b>Delete Subscriber on Unassign of</b>  | Use this check box to specify whether you want to delete the subscriber mailbox from the Messaging Device or Communication  |

| Name                        | Description   |
|-----------------------------|---|
| <b>Subscriber from User</b> | System Management when you remove this messaging profile or when you delete the user. |

## Endpoint Profile



### Note:

The page displays the following fields if an endpoint profile exists for the user.

| Name/Button  | Description   |
|--|---|
| <b>System</b>  | The Communication Manager on which you need to add the endpoint.  |
| <b>Use Existing Endpoints</b>                            | Use the check box if you want to use an existing endpoint extension to associate with this profile. If you do not select this check box, the available extensions are used.   |
| <b>Extension</b>   | The extension of the endpoint you want to associate.  |
| <b>Search</b>  | Lists the endpoints (existing or available) based on check box status of the <b>Use Existing Endpoints</b> field.   |
| <b>Template</b>  | The template (system defined or user defined) you want to associate with the endpoint. Select the template based on the set type you want to add.   |
| <b>Set Type</b>  | The set type of the endpoint you want to associate. When you select a template, the system populates the corresponding set types.   |
| <b>Security Code</b>                                     | The security code for authorized access to the endpoint.  |
| <b>Port</b>  | The relevant port for the set type you select.  |
| <b>Search</b>  | Lists the possible ports based on the selected set type.  |
| <b>Delete Endpoint on Unassign of Endpoint from User</b> | Use this check box to specify whether you want to delete the endpoint from the Communication Manager Device when you remove the association between the endpoint and the user or when you delete the user.  |
| <b>dtmfOverlp</b>  | <p>Appears when the <b>Set Type</b> field is H.323. This field specifies the touchtone signals that are used for dual-tone multifrequency (DTMF) telephone signaling. Valid entries include:</p> <ul style="list-style-type: none"> <li>• <b>in-band</b>- All G711 and G729 calls pass DTMF <b>in-band</b>. DTMF digits encoded within existing RTP media stream for G.711/G.729 calls. G.723 is sent <b>out-of-band</b>.</li> <li>• <b>in-band-g711</b> – Only G711 calls pass DTMF in-band.</li> <li>• <b>out-of-band</b>- All IP calls pass DTMF <b>out-of-band</b>. For IP trunks, the digits are done with either Keypad IEs or H245 indications. This is the default for newly added H.323 signaling groups.</li> </ul> |

### Roles section

| Name                    | Description  |
|-------------------------|--|
| <b>Select check box</b> | Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account. |
| <b>Name</b>             | The name of the role.  |
| <b>Description</b>      | A brief description about the role.  |

| Button              | Description  |
|---------------------|--|
| <b>Assign Roles</b> | Opens the Assign Role page that you can use to assign roles to the user account.   |
| <b>Remove Roles</b> | Removes the selected role from the list of roles associated with the user account. |

### Group Membership section

| Name                    | Description                             |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select the group. |
| <b>Name</b>             | Name of the group.                      |
| <b>Type</b>             | Group type based on the resources.      |
| <b>Hierarchy</b>        | Position of the group in the hierarchy. |
| <b>Description</b>      | A brief description about the group.    |

| Button                   | Description   |
|--------------------------|---|
| <b>Add To group</b>      | Opens the Assign Groups page that you can use to add the user to a group. |
| <b>Remove From Group</b> | Removes the user from the selected group.                                 |

### Attribute Sets section

| Name                          | Description  |
|-------------------------------|--|
| <b>Select check box</b>       | Use this check box to select the attribute set.      |
| <b>Attribute Set</b>          | Name of the attribute set.                           |
| <b>Attribute Set Instance</b> | Name of the attribute set instance.                  |
| <b>Application</b>            | Name of the application that owns the attribute set. |
| <b>Description</b>            | A brief description about the attribute set.         |

| Button                       | Description   |
|------------------------------|---|
| <b>Assign Attribute Sets</b> | Opens the Select Attribute page that allows you to assign attribute sets to the user. |
| <b>Remove Attribute Set</b>  | Removes the selected attribute sets for a user .                                      |

### Default Contact List

| Name               | Description   |
|--------------------|---|
| <b>Name</b>        | Name of the contact list. The default name of the contact list is Default. You can change the name to any other appropriate name. |
| <b>Description</b> | A brief description of the contact list.  |

### Associated Contacts

| Name                    | Description   |
|-------------------------|---|
| <b>Last Name</b>        | Last name of the contact.   |
| <b>First Name</b>       | First name of the contact.  |
| <b>Scope</b>            | Categorization of the contact based on whether the contact is a public or private contact.  |
| <b>Speed Dial</b>       | The value specifies whether the speed dial is set for the contact or not.   |
| <b>Speed Dial Entry</b> | The reduced number that represents the speed dial number.   |
| <b>Presence Buddy</b>   | The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact. |

| Button                 | Description  |
|------------------------|--|
| <b>Edit</b>            | Opens the <b>Edit Contact List Member</b> page. Use this page to modify the information of the selected contact. |
| <b>New</b>             | Opens the <b>Attach Contacts</b> page. Use this page to select one or more contacts from the list of contacts.   |
| <b>Remove</b>          | Removes one or more contacts from the list of the associated contacts.   |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                   |
| <b>Filter: Enable</b>  | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.     |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.   |

### Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

| Name                   | Description                            |
|------------------------|--|
| <b>Last Name</b>       | Last name of the private contact.      |
| <b>First Name</b>      | First name of the private contact.     |
| <b>Display Name</b>    | Display name of the private contact.   |
| <b>Contact Address</b> | Address of the private contact.        |
| <b>Description</b>     | A brief description about the contact. |

| Button                 | Description  |
|------------------------|--|
| <b>Edit</b>            | Opens the <b>Edit Private Contact</b> page. Use this page to modify the information of the selected contact. |
| <b>New</b>             | Opens the <b>New Private Contact</b> page. Use this page to add a new private contact.                       |
| <b>Delete</b>          | Deletes the selected contacts.   |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.               |
| <b>Filter: Enable</b>  | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.   |

| Button        | Description  |
|---------------|--|
| <b>Commit</b> | <p>Modifies the user account.</p> <p> <b>Note:</b><br/>While restoring a deleted user, use this button to restore a deleted user.</p> |
| <b>Cancel</b> | Cancels the operation of modifying the user information and takes you back to the User Management or User Profile View page.   |

**Related topics:**

- [Modifying user accounts](#) on page 1390
- [Creating a new communication profile](#) on page 1560
- [Deleting a communication profile](#) on page 1561
- [Creating a new communication address for a communication profile](#) on page 1561
- [Modifying a communication address of a user](#) on page 1562
- [Deleting a communication address from a communication profile](#) on page 1563

## New User Profile field descriptions

Use this page to create a new user. This page has the following sections:

- General
- Identity
- Communication Profile
- Roles
- Group Membership
- Default Contact List
- Private Contacts

 **Note:**

The fields that are marked with an asterisk are mandatory and you must enter appropriate information in these fields.

### General section

| Name               | Description                         |
|--------------------|-------------------------------------|
| <b>Last Name</b>   | The last name of the user.          |
| <b>First Name</b>  | The first name of the user.         |
| <b>Description</b> | A brief description about the user. |

### Identity section

| Name                          | Description   |
|-------------------------------|---|
| <b>Login Name</b>             | A unique system login name for users that includes the users marked as deleted. It takes the form of username@domain. It is used to create the user's primary handle.   |
| <b>Authentication Type</b>    | Authentication type defines how the system performs user's authentication. The options are: <ul style="list-style-type: none"> <li>• <b>enterprise</b> — The enterprise authenticates user's login.</li> <li>• <b>basic</b> — The Avaya Authentication Service authenticates user's login.</li> </ul> |
| <b>Password</b>               | The initial password for logging in to the system.  |
| <b>Confirm Password</b>       | The initial password for verification.  |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.  |

| Name                         | Description   |
|------------------------------|---|
| <b>Endpoint Display Name</b> | The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints. |
| <b>Honorific</b>             | The personal title for address a user. This is typically a social title and not the work title.   |
| <b>Language Preference</b>   | The user's preferred written or spoken language.  |
| <b>Time Zone</b>             | The preferred time zone of the user.  |

### Identity > Address section

| Name                    | Description   |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select a address in the table.  |
| <b>Name</b>             | The name of the addressee.  |
| <b>Address Type</b>     | The type of address. The values are: <ul style="list-style-type: none"> <li>• Office</li> <li>• Home</li> </ul> |
| <b>Street</b>           | The name of the street.   |
| <b>Locality Name</b>    | The name of the city or town.   |
| <b>Postal Code</b>      | The postal code used by postal services to route mail to a destination. In United States this is Zip code.      |
| <b>Province</b>         | The full name of the province.  |
| <b>Country</b>          | The name of the country.  |

| Button                       | Description  |
|------------------------------|--|
| <b>New</b>                   | Opens the Add Address page. Use the page to add the address details. |
| <b>Edit</b>                  | Allows you to modify the address.                                    |
| <b>Delete</b>                | Deletes the selected address.  |
| <b>Choose Shared Address</b> | Opens the Choose Address page that you can use to choose a address.  |

### Communication Profile section

Use this section to create, modify and delete a communication profile for the user. Each communication profile may contain one or more communication addresses for a user.

| Name                 | Description  |
|----------------------|--|
| <b>Option button</b> | Use this button to view the details of the selected communication profile. |

| Name        | Description                        |
|-------------|------------------------------------|
| <b>Name</b> | Name of the communication profile. |

| Name          | Description  |
|---------------|--|
| <b>New</b>    | Creates a new communication profile for the user.                                    |
| <b>Delete</b> | Deletes the selected communication profile.  |
| <b>Save</b>   | Saves the communication profile information that you updated or added for a profile. |
| <b>Cancel</b> | Cancel the operation for adding a communication profile.                             |

This page displays the following fields when you click the **Add** button in the Communication Profile section.

| Name           | Description   |
|----------------|---|
| <b>Name</b>    | The name of the communication profile for the user.   |
| <b>Default</b> | The profile that is made default is the active profile. There can be only one active profile at a time. |

### Communication Address section

Use this section to create, modify and delete one or more communication addresses for the user.

| Name           | Description   |
|----------------|---|
| <b>Type</b>    | The type of the handle.                                     |
| <b>SubType</b> | The sub type of the handle.                                 |
| <b>Handle</b>  | A unique communication address of the user.                 |
| <b>Domain</b>  | The name of the domain with which the handle is registered. |

| Name          | Description  |
|---------------|--|
| <b>New</b>    | Displays the fields for adding a new communication address.                  |
| <b>Edit</b>   | Use this button to edit the information of a selected communication address. |
| <b>Delete</b> | Deletes the selected communication address.                                  |

The page displays the following fields when you click **New** and **Edit** in the Communication Address section. The following fields define the communication address for the user.

| Name                           | Description  |
|--------------------------------|--|
| <b>Type</b>                    | <p>The types of the handle. The following are the different handle types:</p> <ul style="list-style-type: none"> <li>• sip: Indicates that the handle supports SIP based communication.</li> <li>• smtp: Indicates that the handle is an e-mail address and supports Simple Mail Transfer Protocol (SMTP) based communication.</li> <li>• ibm: Indicates that the handle is an IBM address.</li> <li>• xmpp: Indicates that the handle supports Extensible Messaging and Presence Protocol (XMPP) based communication.</li> </ul>  |
| <b>SubType</b>                 | <p>The sub types of the handle. The following are the subtypes:</p> <ul style="list-style-type: none"> <li>• Subtypes for SIP based handles:               <ol style="list-style-type: none"> <li>a. e164: Type signifies that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix.</li> <li>b. username: Type signifies that the handle is an alphanumeric value. For example, 1234567, xyz, or abc.xyz</li> <li>c. msrtc: Type signifies that the handle supports communication with the Microsoft RTC server.</li> </ol> </li> <li>• Subtypes for SMTP:               <ul style="list-style-type: none"> <li>msexchange: Type signifies that the handle supports communication with Microsoft SMTP server.</li> </ul> </li> <li>• Subtypes for ibm:               <ol style="list-style-type: none"> <li>a. lotusnotes: Type signifies that the handle is for lotus notes and domino calender.</li> <li>b. ibmsametime: Type signifies that the handle is for IBM sametime</li> </ol> </li> <li>• Subtypes for xmpp:               <ol style="list-style-type: none"> <li>a. jabber: Type signifies that the handle supports communication with the Jabber service.</li> <li>b. googletalk: Type signifies that the handle supports communication with the googletalk service.</li> </ol> </li> </ul> |
| <b>Fully Qualified Address</b> | <p>The fully qualified domain name or uniform resource identifier. The address can be an e-mail address, IM user or an address of an communication device using which user can send or receive messages.</p>   |

| Name          | Description  |
|---------------|--|
| <b>Add</b>    | Saves the new communication address or modified communication address information in the database. |
| <b>Cancel</b> | Cancels the adding a communication address operation.  |

## Session Manager

 **Note:**

You may see these fields only if a communication profile for the user can be configured using the product.

| Name                                    | Description   |
|---|---|
| <b>Primary Session Manager</b>          | Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required.   |
| <b>Secondary Session Manager</b>        | If a secondary Session Manager instance is selected, this Session Manager will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available. A selection is optional.   |
| <b>Origination Application Sequence</b> | Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. Note: if both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.   |
| <b>Termination Application Sequence</b> | <p>Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional.</p> <p> <b>Note:</b></p> <p>If both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.</p>   |
| <b>Survivability Server</b>             | For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. A selection is optional. Note: if a termination or origination application sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager. |
| <b>Home Location</b>                    | A Home Location can be specified to support mobility for the currently displayed user. When this user calls numbers that are not associated with an administered user, dial-plan rules (Routing > Dial Patterns) will be applied to complete the call based on this home location (Routing > Locations) regardless of the physical location of the SIP device used to make the call. A selection is mandatory.  |

## Messaging Profile

 **Note:**

You may see these fields only if a messaging profile can be configured for the user.

| Name   | Description  |
|--|--|
| <b>System</b>  | The Messaging System on which you need to add the subscriber.  |
| <b>Template</b>  | The template (system defined and user defined) you want to associate with the subscriber.  |
| <b>Use Existing Subscriber on System</b>                     | Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.   |
| <b>Existing Mailbox Number</b>                               | The existing mailbox number that you want to associate with this profile. This value in the field is valid only if you select the <b>Use Existing Subscriber on System</b> check box.                            |
| <b>Mailbox Number</b>  | The mailbox number of the subscriber.  |
| <b>Password</b>  | The password for logging into the mailbox.   |
| <b>Delete Subscriber on Unassign of Subscriber from User</b> | Use this check box to specify whether you want to delete the subscriber mailbox from the Messaging Device or Communication System Management when you remove this messaging profile or when you delete the user. |

## Endpoint Profile

 **Note:**

You may see these fields only if an endpoint profile can be configured for the user .

| Name/Button                   | Description   |
|-------------------------------|---|
| <b>System</b>                 | The Communication Manager on which you need to add the endpoint.  |
| <b>Use Existing Endpoints</b> | Use the check box if you want to use an existing endpoint extension to associate with this profile. If you do not select this check box, the available extensions are used. |
| <b>Extension</b>              | The extension of the endpoint you want to associate.  |
| <b>Search</b>                 | Lists the endpoints (existing or available) based on check box status of the <b>Use Existing Endpoint</b> field.  |
| <b>Template</b>               | The template (system defined or user defined) you want to associate with the endpoint. Select the template based on the set type you want to add.                           |
| <b>Set Type</b>               | The set type of the endpoint you want to associate. When you select a template, the system populates the corresponding set types.   |
| <b>Security Code</b>          | The security code for authorized access to the endpoint.  |

| Name/Button  | Description  |
|--|--|
| <b>Port</b>  | The relevant port for the set type you select.   |
| <b>Search</b>  | Lists the possible ports based on the selected set type.   |
| <b>Delete Endpoint on Unassign of Endpoint from User</b> | Use this check box to specify whether you want to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.   |
| <b>dtmfOverlp</b>  | <p>Appears when the <b>Set Type</b> field is H.323. This field specifies the touchtone signals that are used for dual-tone multifrequency (DTMF) telephone signaling. Valid entries include:</p> <ul style="list-style-type: none"> <li>• <b>in-band</b>- All G711 and G729 calls pass DTMF <b>in-band</b>. DTMF digits encoded within existing RTP media stream for G.711/G.729 calls. G. 723 is sent <b>out-of-band</b>.</li> <li>• <b>in-band-g711</b> – Only G711 calls pass DTMF in-band.</li> <li>• <b>out-of-band</b>- All IP calls pass DTMF <b>out-of-band</b>. For IP trunks, the digits are done with either Keypad IEs or H245 indications. This is the default for newly added H.323 signaling groups.</li> </ul> |

### Roles section

| Name                    | Description  |
|-------------------------|--|
| <b>Select check box</b> | Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account. |
| <b>Name</b>             | The name of the role.  |
| <b>Description</b>      | A brief description about the role.  |

| Button              | Description  |
|---------------------|--|
| <b>Assign Roles</b> | Opens the Assign Role page that you can use to assign the roles to the user account. |
| <b>Remove Roles</b> | Removes the selected role from the list of roles associated with the user account.   |

### Group Membership section

| Name                    | Description                             |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select the group. |
| <b>Name</b>             | Name of the group.                      |
| <b>Type</b>             | Group type based on the resources.      |
| <b>Hierarchy</b>        | Position of the group in the hierarchy. |

| Name               | Description                          |
|--------------------|--------------------------------------|
| <b>Description</b> | A brief description about the group. |

| Button                   | Description   |
|--------------------------|---|
| <b>Add To group</b>      | Opens the Assign Groups page that you can use to add the user to a group. |
| <b>Remove From Group</b> | Removes the user from the selected group.                                 |

### Default Contact List

| Name               | Description   |
|--------------------|---|
| <b>Name</b>        | Name of the contact list. The default name of the contact list is Default. You can change the name to any other appropriate name. |
| <b>Description</b> | A brief description of the contact list.  |

### Associated Contacts

| Name                    | Description   |
|-------------------------|---|
| <b>Last Name</b>        | Last name of the contact.   |
| <b>First Name</b>       | First name of the contact.  |
| <b>Scope</b>            | Categorization of the contact based on whether the contact is a public or private contact.  |
| <b>Speed Dial</b>       | The value specifies whether the speed dial is set for the contact or not.   |
| <b>Speed Dial Entry</b> | The reduced number that represents the speed dial number.   |
| <b>Presence Buddy</b>   | The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact. |

| Button                 | Description  |
|------------------------|--|
| <b>Edit</b>            | Opens the <b>Edit Contact List Member</b> page. Use this page to modify the information of the selected contact. |
| <b>New</b>             | Opens the <b>Attach Contacts</b> page. Use this page to select one or more contacts from the list of contacts.   |
| <b>Remove</b>          | Removes one or more contacts from the list of the associated contacts.   |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                   |
| <b>Filter: Enable</b>  | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.     |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.   |

## Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

| Name                   | Description                            |
|------------------------|--|
| <b>Last Name</b>       | Last name of the private contact.      |
| <b>First Name</b>      | First name of the private contact.     |
| <b>Display Name</b>    | Display name of the private contact.   |
| <b>Contact Address</b> | Address of the private contact.        |
| <b>Description</b>     | A brief description about the contact. |

| Button                 | Description  |
|------------------------|--|
| <b>Edit</b>            | Opens the <b>Edit Contact List Member</b> page. Use this page to modify the information of the selected contact. |
| <b>New</b>             | Opens the <b>New Private Contact</b> page. Use this page to add a new private contact.                           |
| <b>Delete</b>          | Deletes the selected contacts.   |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                   |
| <b>Filter: Enable</b>  | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.     |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.   |

| Button        | Description                          |
|---------------|--------------------------------------|
| <b>Commit</b> | Creates the user account.            |
| <b>Cancel</b> | Cancels the user creation operation. |

### Related topics:

[Creating a new user profile](#) on page 1391

[Creating a new communication profile](#) on page 1560

[Deleting a communication profile](#) on page 1561

[Creating a new communication address for a communication profile](#) on page 1561

[Modifying a communication address of a user](#) on page 1562

[Deleting a communication address from a communication profile](#) on page 1563

[Adding a messaging profile for a user](#) on page 1565

[Modifying a messaging profile of a user](#) on page 1566

[Removing an association between a subscriber mailbox and a user](#) on page 1566

[Deleting a subscriber mailbox](#) on page 1567

[Adding a station profile for a user](#) on page 1568

[Modifying a station profile of a user](#) on page 1569

[Deleting a station profile of a user](#) on page 1570

## User Profile Duplicate field descriptions

Use this page to create a duplicate user. This page has the following sections:

- General
- Identity

### General section

| Name               | Description  |
|--------------------|--|
| <b>Last Name</b>   | The last name of the user.   |
| <b>First Name</b>  | The first name of the user.  |
| <b>Description</b> | A brief description about the user.  |
| <b>User Type</b>   | <p>The primary user types. You can associate an user account with the following user types:</p> <ul style="list-style-type: none"> <li>• Administrator</li> <li>• Communication User</li> <li>• Agent</li> <li>• Supervisor</li> <li>• Resident Expert</li> <li>• Service Technician</li> <li>• Lobby Phone</li> </ul> |

### Identity section

| Name                       | Description   |
|----------------------------|---|
| <b>Login Name</b>          | This is the unique system login name given to the user. It takes the form of username@domain. It will typically be used to create the user's primary handle.  |
| <b>Authentication Type</b> | <p>Authentication type defines how the system performs user's authentication. The options are:</p> <ul style="list-style-type: none"> <li>• <b>enterprise</b> — User's login is authenticated by the enterprise.</li> <li>• <b>basic</b> — User's login is authenticated by an Avaya Authentication Service.</li> </ul> |
| <b>Password</b>            | The initial password for logging in to the system.  |
| <b>Confirm Password</b>    | The initial password for verification.  |

| Name                          | Description   |
|-------------------------------|---|
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.  |
| <b>Endpoint Display Name</b>  | The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints. |
| <b>Honorific</b>              | The personal title for address a user. This is typically a social title and not the work title.   |
| <b>Language Preference</b>    | The user's preferred written or spoken language.  |
| <b>Time Zone</b>              | The preferred time zone of the user.  |

### Identity > Address section

| Name                    | Description   |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select the address.   |
| <b>Name</b>             | The name of the user.   |
| <b>Address Type</b>     | The type of address. The values are: <ul style="list-style-type: none"> <li>• Office</li> <li>• Home</li> </ul> |
| <b>Street</b>           | The name of the street.   |
| <b>Locality Name</b>    | The name of the city or town.   |
| <b>Postal Code</b>      | The postal code used by postal services to route mail to a destination. In United States this is Zip code.      |
| <b>Province</b>         | The full name of the province.  |
| <b>Country</b>          | The name of the country.  |

| Button                       | Description   |
|------------------------------|---|
| <b>New</b>                   | Opens the Add Address page that allows you to add the address details.      |
| <b>Edit</b>                  | Opens the Edit Address page that you can use to modify the address details. |
| <b>Delete</b>                | Deletes the selected address.   |
| <b>Choose Shared Address</b> | Opens the Choose Address page that you can use to choose a address.         |

| Button        | Description                 |
|---------------|-----------------------------|
| <b>Commit</b> | Creates the duplicate user. |

| Button | Description  |
|--------|--|
| Cancel | Cancels the duplicate user creation and returns to the User Management page. |

### Communication Profile section

| Name          | Description  |
|---------------|--|
| Option button | Use this button to view the details of the selected communication profile. |
| Name          | Name of the communication profile.   |

| Name   | Description  |
|--------|--|
| New    | Creates a new communication profile for the user.                                    |
| Delete | Deletes the selected communication profile.  |
| Save   | Saves the communication profile information that you updated or added for a profile. |
| Cancel | Cancels the operation for adding a communication profile.                            |

The page displays the following fields when you click the **Add** button in the Communication Profile section.

| Name    | Description   |
|---------|---|
| Name    | Name of the communication profile for the user.   |
| Default | The profile that is made default is the active profile. There can be only one active profile at a time. |

### Communication Address section

| Name    | Description   |
|---------|---|
| Type    | Type of the communication protocol to be used for the user. |
| SubType | Sub type of the communication protocol.                     |
| Handle  | A unique communication address for the user.                |
| Domain  | Name of the domain with which the handle is registered.     |

| Name   | Description  |
|--------|--|
| New    | Displays the fields for adding a new communication address.                  |
| Edit   | Use this button to edit the information of a selected communication address. |
| Delete | Deletes the selected communication address.                                  |

The page displays the following fields when you click **New** and **Edit** in the Communication Address section.

| Name                           | Description  |
|--------------------------------|--|
| <b>Type</b>                    | Type of the communication protocol used for establishing communication with the user. The following are the communication protocols for the user: <ul style="list-style-type: none"> <li>• sip</li> <li>• smtp</li> <li>• ibm</li> <li>• xmpp</li> </ul> |
| <b>SubType</b>                 | Displays the sub types of the communication protocol.  |
| <b>Fully Qualified Address</b> | The fully qualified domain name or uniform resource identifier. The address can be an e-mail address, IM user or of an communication device using which user can send or receive messages.   |

| Name          | Description  |
|---------------|--|
| <b>Add</b>    | Saves the new communication address or modified communication address information to the database. |
| <b>Cancel</b> | Cancel the adding a communication address operation.   |

## Session Manager



### Note:

You may see these fields only if a communication profile for the user can be configured using the product.

| Name                                    | Description   |
|---|---|
| <b>Primary Session Manager</b>          | Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required. |
| <b>Secondary Session Manager</b>        | If a secondary Session Manager instance is selected, this Session Manager will provide continued service to SIP devices associated with this Communication Profile in the event that the primary Session Manager is not available. A selection is optional.   |
| <b>Origination Application Sequence</b> | Select an Application Sequence that will be invoked when calls are routed from this user. A selection is optional. Note: if both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.   |
| <b>Termination Application Sequence</b> | Select an Application Sequence that will be invoked when calls are routed to this user. A selection is optional.  |

| Name                        | Description   |
|-----------------------------|---|
|                             |  <b>Note:</b><br>If both an origination and a termination application sequence are specified and each contains a CM application, the CM should be the same in both sequences.  |
| <b>Survivability Server</b> | For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a CM application, sequencing to this application will continue, locally, to the CM LSP resident with the Branch Session Manager. A selection is optional. Note: if a termination or origination application sequence contains a CM application, the CM associated with the application must be the main CM for the CM LSP that is resident with the Branch Session Manager. |
| <b>Home Location</b>        | A Home Location can be specified to support mobility for the currently displayed user. When this user calls numbers that are not associated with an administered user, dial-plan rules (Routing > Dial Patterns) will be applied to complete the call based on this home location (Routing > Locations) regardless of the physical location of the SIP device used to make the call. A selection is optional  |

### Messaging Profile

 **Note:**

You may see these fields only if a messaging profile can be configured for the user.

| Name                                     | Description   |
|--|---|
| <b>System</b>                            | The Messaging System on which you need to add the subscriber.   |
| <b>Template</b>                          | The template (system defined and user defined) you want to associate with the subscriber.   |
| <b>Use Existing Subscriber on System</b> | Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.  |
| <b>Existing Mailbox Number</b>           | The existing mailbox number that you want to associate with this profile. This value in the field is valid only if you select the <b>Use Existing Subscriber on System</b> check box. |
| <b>Mailbox Number</b>                    | The mailbox number of the subscriber.   |
| <b>Password</b>                          | The password for logging into the mailbox.  |
| <b>Delete Subscriber on Unassign of</b>  | Use this check box to specify whether you want to delete the subscriber mailbox from the Messaging Device or Communication  |

| Name                        | Description   |
|-----------------------------|---|
| <b>Subscriber from User</b> | System Management when you remove this messaging profile or when you delete the user. |

## Endpoint Profile



### Note:

You may see these fields only if an endpoint profile can be configured for the user .

| Name/Button  | Description  |
|--|--|
| <b>System</b>  | The Communication Manager on which you need to add the endpoint.   |
| <b>Use Existing Endpoints</b>                            | Use the check box if you want to use an existing endpoint extension to associate with this profile. If you do not select this check box, the available extensions are used.  |
| <b>Extension</b>   | The extension of the endpoint you want to associate.   |
| <b>Search</b>  | Lists the endpoints (existing or available) based on check box status of the <b>Use Existing Endpoints</b> field.  |
| <b>Template</b>  | The template (system defined or user defined) you want to associate with the endpoint. Select the template based on the set type you want to add.  |
| <b>Set Type</b>  | The set type of the endpoint you want to associate. When you select a template, the system populates the corresponding set types.  |
| <b>Security Code</b>                                     | The security code for authorized access to the endpoint.   |
| <b>Port</b>  | The relevant port for the set type you select.   |
| <b>Search</b>  | Lists the possible ports based on the selected set type.   |
| <b>Delete Endpoint on Unassign of Endpoint from User</b> | Use this check box to specify whether you want to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.   |
| <b>dtmfOverlp</b>  | Appears when the <b>Set Type</b> field is H.323. This field specifies the touchtone signals that are used for dual-tone multifrequency (DTMF) telephone signaling. Valid entries include: <ul style="list-style-type: none"> <li>• <b>in-band</b>- All G711 and G729 calls pass DTMF <b>in-band</b>. DTMF digits encoded within existing RTP media stream for G.711/G.729 calls. G.723 is sent <b>out-of-band</b>.</li> <li>• <b>in-band-g711</b> – Only G711 calls pass DTMF in-band.</li> <li>• <b>out-of-band</b>- All IP calls pass DTMF <b>out-of-band</b>. For IP trunks, the digits are done with either Keypad IEs or H245 indications. This is the default for newly added H.323 signaling groups.</li> </ul> |

## User Delete Confirmation field descriptions

Use this page to delete an user account.

| Name              | Description  |
|-------------------|--|
| <b>Status</b>     | The status indicates whether the user is currently online or offline.          |
| <b>Name</b>       | The localized display name of a user. It is typically the localized full name. |
| <b>Last login</b> | The date and time of last successful login into System Manager.                |

| Button        | Description  |
|---------------|--|
| <b>Delete</b> | Deletes an user.   |
| <b>Cancel</b> | Closes the User Delete Confirmation page and takes you back to the User Management page. |

## Assign Roles to Multiple Users field descriptions

Use this page to assign roles to multiple users. The page has the following two sections:

- Selected Users
- Select Roles

### Selected Users

| Name              | Description   |
|-------------------|---|
| <b>Status</b>     | The current login status of the user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status. |
| <b>Name</b>       | Name of the user.   |
| <b>User Name</b>  | Unique name that gives access to the system .   |
| <b>Last login</b> | Time and date when the user has logged in to the system.  |

### Select Roles

| Name                    | Description                          |
|-------------------------|--------------------------------------|
| <b>Select Check box</b> | Use this check box to select a role. |
| <b>Name</b>             | Name of the role.                    |

| Name        | Description                         |
|-------------|-------------------------------------|
| Description | A brief description about the role. |

| Button | Description   |
|--------|---|
| Commit | Assigns roles to the selected users.  |
| Cancel | Cancels the role assignment operation and takes you back to the User Management page. |

---

## Assign Roles field descriptions

Use this page to assign a role to the user. The page has the following two sections:

- Selected Roles
- Available Roles

### Selected Roles

The table in this section displays roles that you have assigned to the user account.

| Name        | Description   |
|-------------|---|
| Name        | The roles that you have assigned to the user account. |
| Description | Displays a brief description about the roles.         |

### Available Roles

The table in this section displays roles that you can assign to the user account.

| Name             | Description  |
|------------------|--|
| Select Check box | Use this check box displayed at the header row to select all the roles in the table. |
| Name             | The roles that you can assign to the user account.                                   |
| Description      | Displays a brief description of the roles.   |

| Button | Description   |
|--------|---|
| Select | Assigns the selected roles to the user.                                 |
| Cancel | Cancels the role assignment operation and returns to the previous page. |

---

## Assign Groups field descriptions

Use this page to assign a group to the user account. The page has the following two sections:

- Selected Groups
- Available Groups

### Selected Groups section

The table in this section displays groups that you have assigned to the user account.

| Name               | Description                             |
|--------------------|---|
| <b>Name</b>        | Name of the group.                      |
| <b>Type</b>        | Group type based on the resources.      |
| <b>Hierarchy</b>   | Position of the group in the hierarchy. |
| <b>Description</b> | A brief description about the group.    |

### Available Groups section

The table in this section displays groups that you can assign to the user account.

| Name                    | Description                             |
|-------------------------|---|
| <b>Select Check box</b> | Select the group.                       |
| <b>Name</b>             | Name of the group.                      |
| <b>Type</b>             | Group type based on the resources.      |
| <b>Hierarchy</b>        | Position of the group in the hierarchy. |
| <b>Description</b>      | A brief description about the group.    |

| Button              | Description                             |
|---------------------|---|
| <b>Select</b>       | Assigns the selected groups to the user |
| <b>Cancel</b>       | Cancels the group assignment operation. |
| <b>Select: ALL</b>  | Selects all groups in the table         |
| <b>Select: None</b> | Clears the selection                    |

---

## Assign Groups to Multiple Users field descriptions

Use this page to add users to the selected groups. This page has the following two sections:

- Selected Users
- Select Groups

## Selected Users

| Name              | Description   |
|-------------------|---|
| <b>Status</b>     | The current login status of the user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status. |
| <b>Name</b>       | Name of the user.   |
| <b>User Name</b>  | Unique name that gives access to the system .   |
| <b>Last login</b> | Time and date when the user has last logged in to the system.   |

## Select Groups

| Name                    | Description                              |
|-------------------------|--|
| <b>Select Check box</b> | Use this check box to select a group.    |
| <b>Name</b>             | Name of the group.                       |
| <b>Type</b>             | Group type based on the resources.       |
| <b>Hierarchy</b>        | Position of the group within the groups. |
| <b>Description</b>      | A brief description about the group.     |

| Button              | Description   |
|---------------------|---|
| <b>Select: All</b>  | Selects all the groups displayed in the table.  |
| <b>Select: None</b> | Clears the selected check boxes.  |
| <b>Commit</b>       | Assigns groups to the selected users.   |
| <b>Cancel</b>       | Cancel the group assignment operation and takes you back to the User Management page. |

---

## Deleted Users field descriptions

You can view the users that you have deleted using the Delete feature. Use this page to view, permanently delete a user, and restore users that you have deleted.

| Name                    | Description   |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select a deleted user.  |
| <b>Status</b>           | The current login status of the deleted user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status. |

| Name              | Description   |
|-------------------|---|
| <b>Name</b>       | Name of the deleted user.   |
| <b>User Name</b>  | The unique name that identifies the user in the system.                   |
| <b>Last login</b> | Date and time when the user has last successfully logged into the system. |

| Button                    | Description  |
|---------------------------|--|
| <b>Delete</b>             | Deletes the user permanently from the database.        |
| <b>Restore</b>            | Restores the deleted user.                             |
| <b>Show Regular users</b> | Returns to the User page and display the active users. |

---

## User Restore Confirmation field descriptions

Use this page to restore a deleted user.

| Name              | Description   |
|-------------------|---|
| <b>Status</b>     | The status indicates whether the user is currently online or offline. |
| <b>Name</b>       | The name that identifies the group to which the user belongs.         |
| <b>User Name</b>  | The unique name of the user account.                                  |
| <b>Last login</b> | The date and time of last successful login into System Manager.       |

| Button         | Description   |
|----------------|---|
| <b>Restore</b> | Removes the user from the list of deleted users and restores the user as an active user.  |
| <b>Cancel</b>  | Closes the User Restore Confirmation page and returns you back to the Deleted Users page. |

---

## Change Password field descriptions

Use this page to change the password for your account.

| Name                | Description                            |
|---------------------|--|
| <b>Old Password</b> | The existing password.                 |
| <b>New Password</b> | The new password that you want to set. |

| Name                    | Description                            |
|-------------------------|--|
| <b>Confirm Password</b> | The new password that you want to set. |

| Button        | Description   |
|---------------|---|
| <b>Save</b>   | Changes the password.   |
| <b>Cancel</b> | Cancel the change password operation and closes the Change Password page. |

---

## Assign Users To Roles field descriptions

Use this page to assign one or more users to the selected roles. The page has two sections:

- Selected Roles
- Select Users

### Selected Roles section

The roles to which you can assign users.

| Name                 | Description  |
|----------------------|--|
| <b>Name</b>          | Name of the role.  |
| <b>Resource Type</b> | The resource type that the corresponding role is assigned. |
| <b>Description</b>   | A brief description about role.                            |

### Select Users section

The table displays the users to which you can assign the roles.

| Name                    | Description   |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select the user.  |
| <b>Status</b>           | Displays whether the user is currently online or offline. The online status indicates that the user is logged into the application and offline status indicates that the user is logged out of the application. |
| <b>User Name</b>        | The unique name that identifies the user  |
| <b>Last Login</b>       | Time and date when the user has last logged into the system.  |
| <b>User Type</b>        | The type that defines the role of the user.   |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Assigns user to the role.   |
| <b>Cancel</b> | Cancel the assign users operation and returns to the Manage Roles page. |

## UnAssign Roles field descriptions

Use this page to unassign a role from the selected users. The page has two sections:

- Selected Roles
- Select Users

### Selected Roles section

The role from which users are unassigned.

| Name                 | Description  |
|----------------------|--|
| <b>Name</b>          | Name of the role.  |
| <b>Resource Type</b> | The resource type that the corresponding role is assigned. |
| <b>Description</b>   | A brief description about the role.                        |

### Select Users section

The table displays the users for which you can remove the roles.

| Name                    | Description   |
|-------------------------|---|
| <b>Select check box</b> | Use this check box to select the user.  |
| <b>Status</b>           | Displays whether the user is currently online or offline. The online status indicates that the user is logged into the application and offline status indicates that the user is logged out of the application. |
| <b>User Name</b>        | The unique name that identifies the user  |
| <b>Last Login</b>       | Time and date when the user has last logged into the system.  |
| <b>User Type</b>        | The type that defines the role of the user.   |

| Button        | Description   |
|---------------|---|
| <b>Commit</b> | Unassigns the role from the users.                                      |
| <b>Cancel</b> | Cancel the assign users operation and returns to the Manage Roles page. |

---

## Managing public contacts

---

### Manage public contact list

An administrator defines public contacts for users in System Manager. System Manager provides a provision to share the public contacts by all the users in System Manager.

A user with administrator permission can only add, modify and delete a public contact. While creating a public contact, you need to specify the details of contact that also includes the postal address and communication address of the public contact.

The public contacts defined in the system are the default public contacts for the users and access control list.

---

### Adding a new public contact

1. On the System Manager console, click **Users > Public Contact Lists** in the left navigation pane .
  2. On the Public Contacts page, click **New**.
  3. On the New Public Contact page in the Contact Details section, enter the appropriate information in the respective fields.  
The fields marked with an asterisk are mandatory. You must enter a valid information in these fields to successfully create a new public contact.  
Localized display name must be a unique name. If you do not enter any information in the **Localized Display Name** field, the system automatically generates a localized display name for the public contact.
  4. In the Postal Address section, add the postal address of the contact using the **New** button.
  5. In the Contact Address section, add the contact address using the **New** button.  
The contact address can be a phone number or any communication address that is supported by the application.
  6. Click **Commit** to create a new public contact.
-

**Related topics:**

[New Public Contact field descriptions](#) on page 1665

---

## Modifying the details of a public contact

1. On the System Manager console, click **Users > Public Contact Lists** in the left navigation pane .
2. On the Public Contacts page, click **Edit**.
3. On the Edit Public Contact page, modify the contact's information.
4. Click **Commit**.



Ensure that you have entered valid information in the mandatory fields that are marked with an asterisk before you click **Commit**.

---

**Related topics:**

[Edit Public Contact field descriptions](#) on page 1663

---

## Deleting public contacts

1. On the System Manager console, click **Users > Public Contact Lists** in the left navigation pane .
2. On the Public Contacts page, select one or more contacts.
3. Click **Delete**.
4. On the Contact Delete Confirmation page, click **Delete**.  
When you delete a public contact, the system deletes the contact from the default contact list.

---

## Viewing the details of a public contact

- 
1. On the System Manager console, click **Users > Public Contact Lists** in the left navigation pane .
  2. On the Public Contacts page, select a public contact and click **View**.

---

### Result

The View Public Contact page displays the details of a public contact.

### Related topics:

[View Public Contact field descriptions](#) on page 1662

---

## Adding a postal address of a public contact

- 
1. On the System Manager console, click **Users > Public Contact Lists** in the left navigation pane .
  2. On the Public Contacts page, perform one of the following steps:
    - Click **New** if you are adding a postal address for a new public contact.
    - Select a public contact and click **Edit** if you are adding a postal address for an existing public contact.
  3. Click **New** in the Postal Address section.
  4. On the Add Address page, enter the appropriate information in the respective fields. The fields marked with an asterisk are mandatory. You must enter a valid information in these fields.
  5. Click **Add** to create a new postal address for the public contact.
  6. On the New Public Contact or Edit Public Contact page, click **Commit**.

---

### Related topics:

[Add Address field descriptions](#) on page 1402

---

## Modifying a postal address of a public contact

- 
1. On the System Manager console, click **Users > Public Contact Lists** in the left navigation pane .
  2. On the Public Contacts page, select a public contact and click **Edit**.  
If you are on the New Public Contact page, follow step 4.
  3. On the Edit Public Contact page, select an address from the Postal Address section.
  4. Click **Edit**.
  5. On the Edit Address page, modify the information in the respective fields.  
The fields marked with an asterisk are mandatory. You must enter valid information in these fields.
  6. Click **Add** to save the modified address.

---

### Related topics:

[Add Address field descriptions](#) on page 1402

---

## Deleting postal addresses of a public contact

- 
1. On the System Manager console, click **Users > Public Contact Lists** in the left navigation pane .
  2. On the Public Contacts page, select a public contact and click **Edit** for deleting the postal address of an existing public contact.  
If you are on the New Public Contact page, follow step 3.
  3. Select a address from the table in the Postal Address and click **Delete**.
  4. Click **Commit** to save the changes.
-

---

## Choosing a shared address for a public contact

- 
1. On the System Manager console, click **Users > Public Contact Lists** in the left navigation pane .
  2. On the Public Contacts page, perform one of the following steps:
    - Click **New** if you are adding a postal address for a new public contact.
    - Select a public contact and click **Edit** if you are adding a postal address for an existing public contact.
  3. Click **Choose Shared Address** in the Postal Address section.
  4. On the Choose Address page, select one or more shared addresses.
  5. Click **Select** to add the selected addresses for the public contact.
- 

---

## Adding a contact address of a public contact

- 
1. On the System Manager console, click **Users > Public Contact Lists** in the left navigation pane .
  2. On the Public Contacts page, perform one of the following steps:
    - Click **New** if you are adding a postal address for a new public contact.
    - Select a public contact and click **Edit** if you are adding a postal address for an existing public contact.
  3. Click **New** in the Contact Address section.
  4. On the Add Address page, enter the appropriate information in the respective fields. The fields marked with an asterisk are mandatory. You must enter a valid information in these fields.
  5. Click **Add** to create a new contact address for the public contact.
  6. On the New Public Contact page, click **Commit**.
- 

### Related topics:

[Add Address field descriptions](#) on page 1614

---

## Modifying the details of a public contact

You can use this feature to modify the contact details, postal and contact address of an existing public contact.

- 
1. On the System Manager console, click **Users > Public Contact Lists** in the left navigation pane .
  2. On the Public Contacts page, select a public contact and click **Edit**.
  3. On the Edit Public Contact page, modify the information in the Contact Details, Postal Address and, Contact Address section.  
In the Postal Address and Contact Address section you can add, modify and delete addresses in the respective sections.  
The fields marked with an asterisk are mandatory. You must enter a valid information in these fields.
  4. Click **Commit**.

---

### Related topics:

[Edit Address field descriptions](#) on page 1615

---

## Deleting contact addresses of a public contact

- 
1. On the System Manager console, click **Users > Public Contact Lists** in the left navigation pane .
  2. On the Public Contacts page, select a public contact and click **Edit** for deleting the contact address of an existing public contact.  
If you are on the New Public Contact page, follow step 3.
  3. Select one or more addresses from the table in the Contact Address section and click **Delete**.
  4. Click **Commit** to save the changes.
-

---

## Add Address field descriptions

Use this page to add the mailing address of the user.

| Name                 | Description  |
|----------------------|--|
| <b>Name</b>          | The unique label that identifies the address.  |
| <b>Address Type:</b> | The type that identifies whether mailing address is a home or office address.  |
| <b>Building</b>      | The name of the building.  |
| <b>Room</b>          | The number or name of the room.  |
| <b>Street</b>        | The name of the street.  |
| <b>Locality Name</b> | The name of the city or town.  |
| <b>Postal Code</b>   | The postal code or zip code used by postal services to route mail to a destination. In the United States this is the Zip code. |
| <b>Province</b>      | The full name of the province.   |
| <b>Country</b>       | The name of the country.   |

| Button        | Description                           |
|---------------|---------------------------------------|
| <b>Add</b>    | Adds the mailing address of the user. |
| <b>Cancel</b> | Cancel the add address operation.     |

### Related topics:

- [Adding a mailing address of the user](#) on page 1400
- [Adding a postal address of a private contact](#) on page 1605
- [Adding a shared address](#) on page 1671
- [Modifying a shared address](#) on page 1671

---

## Choose Address field descriptions

Use this page to choose a shared address for the user.

| Name                | Description                                   |
|---------------------|---|
| <b>Name</b>         | The unique label that identifies the address. |
| <b>Address Type</b> | The type of address. The values are:          |

| Name                 | Description  |
|----------------------|--|
|                      | <ul style="list-style-type: none"> <li>• Office</li> <li>• Home</li> </ul>                                 |
| <b>Street</b>        | The name of the street.  |
| <b>Locality Name</b> | The name of the city or town.  |
| <b>Postal Code</b>   | The postal code used by postal services to route mail to a destination. In United States this is Zip code. |
| <b>Province</b>      | The full name of the province.   |
| <b>Country</b>       | The name of the country.   |

| Button        | Description   |
|---------------|---|
| <b>Select</b> | Adds the selected mailing address as the shared contact for the user account. |
| <b>Cancel</b> | Cancel the choose address operation.  |

**Related topics:**

[Choosing a shared address](#) on page 1401

[Choosing a shared address for a private contact](#) on page 1606

## View Public Contact field descriptions

### Contact Details

| Name                          | Description  |
|-------------------------------|--|
| <b>Last Name</b>              | Last name of the contact.  |
| <b>First Name</b>             | First name of the contact.   |
| <b>Middle Name</b>            | Middle name of the contact.  |
| <b>Description</b>            | A brief description about the contact.   |
| <b>Company</b>                | Name of contact's company  |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.                 |
| <b>Endpoint Display Name</b>  | Endpoint display name of the contact.  |
| <b>Language Preference</b>    | A list of languages from which you set one language as the preferred language for the contact. |

## Postal Address

| Name                 | Description   |
|----------------------|---|
| <b>Name</b>          | The name of the contact.  |
| <b>Address Type</b>  | The type that identifies whether mailing address is a home or office address. |
| <b>Street</b>        | The name of the street.   |
| <b>Locality Name</b> | The name of the city or town.   |
| <b>Postal Code</b>   | Name of the contact's company.  |
| <b>Province</b>      | The full name of the contact's province.                                      |
| <b>Country</b>       | The name of the contact's country.  |

## Contact Address

| Name                     | Description  |
|--------------------------|--|
| <b>Address</b>           | An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.      |
| <b>Type</b>              | Type signifies the communication medium used to interact with the user.  |
| <b>Category</b>          | Categorization of the address based on the location.   |
| <b>Label</b>             | A text description for classifying this contact.   |
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language. |

### Related topics:

[Viewing the details of a public contact](#) on page 1657

---

## Edit Public Contact field descriptions

### Contact Details

| Name               | Description                            |
|--------------------|--|
| <b>Last Name</b>   | Last name of the contact.              |
| <b>First Name</b>  | First name of the contact.             |
| <b>Middle Name</b> | Middle name of the contact.            |
| <b>Description</b> | A brief description about the contact. |
| <b>Company</b>     | Name of contact's company              |

| Name                          | Description  |
|-------------------------------|--|
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.                 |
| <b>Endpoint Display Name</b>  | Endpoint display name of the contact.  |
| <b>Language Preference</b>    | A list of languages from which you set one language as the preferred language for the contact. |

### Postal Address

| Name                 | Description   |
|----------------------|---|
| <b>Name</b>          | The name of the contact.  |
| <b>Address Type</b>  | The type that identifies whether mailing address is a home or office address. |
| <b>Street</b>        | The name of the street.   |
| <b>Locality Name</b> | The name of the city or town.   |
| <b>Postal Code</b>   | Name of the contact's company.  |
| <b>Province</b>      | The full name of the contact's province.                                      |
| <b>Country</b>       | The name of the contact's country.  |

| Button                       | Description  |
|------------------------------|--|
| <b>Edit</b>                  | Opens the <b>Edit Address</b> page. Use this page to add a new postal address of the public contact.         |
| <b>New</b>                   | Opens the <b>Add Address</b> page. Use this page to modify an existing postal address of the public contact. |
| <b>Delete</b>                | Deletes the selected public contacts.  |
| <b>Choose Shared Address</b> | Opens the <b>Choose Address</b> page. Use this page to choose addresses of the public contact.               |

### Contact Address

| Name            | Description   |
|-----------------|---|
| <b>Address</b>  | An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact. |
| <b>Type</b>     | Type signifies the communication medium used to interact with the user.   |
| <b>Category</b> | Categorization of the address based on the location.  |
| <b>Label</b>    | A text description for classifying this contact.  |

| Name                     | Description  |
|--------------------------|--|
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language. |

| Button        | Description  |
|---------------|--|
| <b>Edit</b>   | Opens the <b>Edit Address</b> page. Use this page to edit a contact address of the public contact. |
| <b>New</b>    | Opens the <b>Add Address</b> page. Use this page to add a contact address of the public contact.   |
| <b>Delete</b> | Deletes the selected public contacts.  |

| Button     | Description                                     |
|------------|---|
| <b>Add</b> | Saves the modified information in the database. |

**Related topics:**

[Modifying the details of a public contact](#) on page 1656

---

## New Public Contact field descriptions

### Contact Details

| Name                          | Description  |
|-------------------------------|--|
| <b>Last Name</b>              | Last name of the contact.  |
| <b>First Name</b>             | First name of the contact.   |
| <b>Middle Name</b>            | Middle name of the contact.  |
| <b>Description</b>            | A brief description about the contact.   |
| <b>Company</b>                | Name of contact's company  |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.                 |
| <b>Endpoint Display Name</b>  | Endpoint display name of the contact.  |
| <b>Language Preference</b>    | A list of languages from which you set one language as the preferred language for the contact. |

### Postal Address

| Name        | Description              |
|-------------|--------------------------|
| <b>Name</b> | The name of the contact. |

| Name                 | Description   |
|----------------------|---|
| <b>Address Type</b>  | The type that identifies whether mailing address is a home or office address. |
| <b>Street</b>        | The name of the street.   |
| <b>Locality Name</b> | The name of the city or town.   |
| <b>Postal Code</b>   | Name of the contact's company.  |
| <b>Province</b>      | The full name of the contact's province.                                      |
| <b>Country</b>       | The name of the contact's country.  |

| Button                       | Description  |
|------------------------------|--|
| <b>Edit</b>                  | Opens the <b>Edit Address</b> page. Use this page to add a new postal address of the public contact.         |
| <b>New</b>                   | Opens the <b>Add Address</b> page. Use this page to modify an existing postal address of the public contact. |
| <b>Delete</b>                | Deletes the selected public contacts.  |
| <b>Choose Shared Address</b> | Opens the <b>Choose Address</b> page. Use this page to choose addresses of the public contact.               |

### Contact Address

| Name                     | Description  |
|--------------------------|--|
| <b>Address</b>           | An address that you can use to communicate with the contact. This can be a phone number, e-mail address or IM of the contact.      |
| <b>Type</b>              | Type signifies the communication medium used to interact with the user.  |
| <b>Category</b>          | Categorization of the address based on the location.   |
| <b>Label</b>             | A text description for classifying this contact.   |
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language. |

| Button        | Description  |
|---------------|--|
| <b>Edit</b>   | Opens the <b>Edit Address</b> page. Use this page to edit a contact address of the public contact. |
| <b>New</b>    | Opens the <b>Add Address</b> page. Use this page to add a contact address of the public contact.   |
| <b>Delete</b> | Deletes the selected public contacts.  |

| Button     | Description  |
|------------|--|
| <b>Add</b> | Creates a new contact.<br><br> <b>Note:</b><br>You must enter valid information in the mandatory fields to successfully create a new contact. |

**Related topics:**

[Adding a new public contact](#) on page 1655

---

## Public Contacts field descriptions

Use this page to add new public contacts, modify and delete existing contacts.

**Public Contacts**

| Name                   | Description                            |
|------------------------|--|
| <b>Last Name</b>       | Last name of the public contact.       |
| <b>First Name</b>      | First name of the public contact.      |
| <b>Display Name</b>    | Display name of the public contact.    |
| <b>Contact Address</b> | Address of the public contact.         |
| <b>Description</b>     | A brief description about the contact. |

| Button                         | Description  |
|--------------------------------|--|
| <b>View</b>                    | Open the <b>View Public Contact</b> page. Use this page to view the details of the selected public contact.  |
| <b>Edit</b>                    | Opens the <b>Edit Public Contact</b> page. Use this page to modify the information of the selected contact.  |
| <b>New</b>                     | Opens the <b>New public Contact</b> page. Use this page to add a new public contact.                         |
| <b>Delete</b>                  | Deletes the selected contacts.   |
| <b>Filter: Advanced Search</b> | Displays fields that you can use to specify the search criteria for searching a public contact.              |
| <b>Filter: Disable</b>         | Hides the column filter fields without resetting the filter criteria. This is a toggle button.               |
| <b>Filter: Enable</b>          | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>           | Filters contacts based on the filter criteria.   |

### Criteria section

The page displays the following fields when you click **Advanced Search** . You can find the **Advanced Search** link at the at the upper-right corner of the public contact table.

| Name            | Description  |
|-----------------|--|
| <b>Criteria</b> | <p>Displays the following three fields:</p> <ul style="list-style-type: none"> <li>• Drop-down 1 - The list of criteria that you can use to search public contacts. The options are:                             <ol style="list-style-type: none"> <li>a. Last Name: Searches public contacts by last name.</li> <li>b. First Name: Searches public contacts by first name.</li> <li>c. Displays Name: Searches public contacts by display name.</li> <li>d. Contact Address: Searches public contacts by contact address.</li> </ol> </li> <li>• Drop-down 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you have selected in the first drop-down field.</li> <li>• Field 3 – The search value for the search criterion selected in the Drop-down 1 field.</li> </ul> |

---

## Add Address field descriptions

Use this page to add communication address of the contact.

| Name            | Description   |
|-----------------|---|
| <b>Address</b>  | <p>An address that you can use to communicate with the contact. This can be a phone number, e-mail address, sip or IM of the contact. The format of the address must conform to the type of address that you selected in the <b>Type</b> field.</p>   |
| <b>Type</b>     | <p>Type of address. The following are the types of address:</p> <ul style="list-style-type: none"> <li>• phone: An address of this type supports phone numbers.</li> <li>• sip: An address of this type supports sip based communication.</li> <li>• msrtc An address of this type supports communication with a Microsoft RTC Server.</li> <li>• ibmsametime: An address of this type supports communication with IBM Sametime,</li> <li>• xmpp: An address of this type supports xmpp based communication.</li> <li>• smtp: An address of this type supports communication with the SMTP server.</li> </ul> |
| <b>Category</b> | <p>Categorization of the address based on the location.</p>   |

| Name                     | Description  |
|--------------------------|--|
| <b>Label</b>             | A text description for classifying this contact.   |
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language. |

| Button     | Description   |
|------------|---|
| <b>Add</b> | Adds the contact address of the public contact in the database. |

**Related topics:**

[Adding a contact address of a private contact](#) on page 1607

[Adding a contact address of a public contact](#) on page 1659

---

## Edit Address field descriptions

Use this page to edit the details of a contact's communication address.

| Name                     | Description  |
|--------------------------|--|
| <b>Address</b>           | An address that you can use to communicate with the contact. This can be a phone number, e-mail address, sip or IM of the contact. The format of the address must conform to the type of address that you selected in the <b>Type</b> field.   |
| <b>Type</b>              | Type of address. The following are the types of address: <ul style="list-style-type: none"> <li>• phone: An address of this type supports phone numbers.</li> <li>• sip: An address of this type supports sip based communication.</li> <li>• msrtc An address of this type supports communication with a Microsoft RTC Server.</li> <li>• ibmsametime: An address of this type supports communication with IBM Sametime,</li> <li>• xmpp: An address of this type supports xmpp based communication.</li> <li>• smtp: An address of this type supports communication with the SMTP server.</li> </ul> |
| <b>Category</b>          | Categorization of the address based on the location.   |
| <b>Label</b>             | A text description for classifying this contact.   |
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language.   |

| Button     | Description                                     |
|------------|---|
| <b>Add</b> | Saves the modified information in the database. |

**Related topics:**

[Modifying a contact address of a private contact](#) on page 1608

[Modifying the details of a public contact](#) on page 1660

---

## Managing shared addresses

---

### Manage shared address

Shared Address contains common addresses that can be specified for one or more users in the enterprise. The user who is an administrator can create a new shared address, modify and delete an existing shared address. For example, you can add the address of the company in the list of shared address and use the address as an alternative address for the users in the enterprise.

---

### Choosing a shared address

Use this feature to choose a shared address for the user from a set of common addresses. You can use the Shared Addresses feature to add, modify and delete a shared address.

- 
1. On the System Manager console, click **Users > Manage Users** in the left navigation pane.
  2. Perform one of the following steps:
    - On the User Management page, click **New**.
    - If you are in the editing a user account, on the User Management page, select a user and click **Edit**.
    - If you are viewing information of an user, on the User Management page, select a user and click **View > Edit**.
  3. On the New User Profile page or the User Profile Edit page, click **Identity > Address > Choose Shared Address**.
  4. On the Choose Address page, select one or more shared addresses.
  5. Click **Select**.
  6. Click **Commit**.

If you are choosing a shared address for a new user, ensure that you have entered valid information in all the mandatory fields on the New User Profile page before

you click **Commit**. If you fail to enter valid information in a mandatory field, the system displays an error message.

---

**Related topics:**

[Choose Address field descriptions](#) on page 1403

---

## Adding a shared address

- 
1. On the System Manager console, click **Users > Shared Addresses** in the left navigation pane.
  2. On the Shared Address page, click **New** in the **Shared Address** section.
  3. On the Add Address page, enter the appropriate information.
  4. Click **Commit**.

---

**Result**

The new address is available as shared address and you can specify this address when you create, modify a user account.

---

## Modifying a shared address

- 
1. On the System Manager console, click **Users > Shared Addresses** in the left navigation pane.
  2. On the Shared Address page, select the address and click **Edit**.
  3. On the Edit Address page, modify the information in the fields.
  4. Click **Commit**.

---

## Deleting a shared address

You can use this feature to delete a shared address. You cannot delete a shared address if the address is associated with one or more users.

- 
1. On the System Manager console, click **Users > Shared Addresses** in the left navigation pane.
  2. On the Shared Address page, select the address and click **Delete** in the **Shared Address** section.
- 

## Add Address field descriptions

Use this page to add the mailing address of the user.

| Name                 | Description  |
|----------------------|--|
| <b>Name</b>          | The unique label that identifies the address.  |
| <b>Address Type:</b> | The type that identifies whether mailing address is a home or office address.  |
| <b>Building</b>      | The name of the building.  |
| <b>Room</b>          | The number or name of the room.  |
| <b>Street</b>        | The name of the street.  |
| <b>Locality Name</b> | The name of the city or town.  |
| <b>Postal Code</b>   | The postal code or zip code used by postal services to route mail to a destination. In the United States this is the Zip code. |
| <b>Province</b>      | The full name of the province.   |
| <b>Country</b>       | The name of the country.   |

| Button        | Description                           |
|---------------|---------------------------------------|
| <b>Add</b>    | Adds the mailing address of the user. |
| <b>Cancel</b> | Cancel the add address operation.     |

### Related topics:

- [Adding a mailing address of the user](#) on page 1400
- [Adding a postal address of a private contact](#) on page 1605
- [Adding a shared address](#) on page 1671
- [Modifying a shared address](#) on page 1671

---

## Shared Address field descriptions

Use this page to create a new shared address, modify and delete an existing shared address.

### Shared Address

| Name                    | Description  |
|-------------------------|--|
| <b>Select check box</b> | Use this check box to select an address.   |
| <b>Name</b>             | The name of the person or entity associated with the address.  |
| <b>Address Type</b>     | The type of address indicates whether the address is an Office or home address.                                |
| <b>Street</b>           | The name of the street.  |
| <b>Locality Name</b>    | The name of the city or town.  |
| <b>Postal Code</b>      | The postal code used by postal services to route mail to a destination. In the United States this is Zip code. |
| <b>Province</b>         | The full name of the province.   |
| <b>Country</b>          | The name of the country.   |
| <b>Refresh</b>          | Refreshes the address information in the table.  |
| <b>All</b>              | Selects all the addresses in the table.  |
| <b>None</b>             | Clears the check box selections.   |

| Button        | Description   |
|---------------|---|
| <b>New</b>    | Opens the Add Address page . Use this page to add an address.                         |
| <b>Edit</b>   | Opens the Edit Address page. Use this page to modify the mailing address information. |
| <b>Delete</b> | Deletes a selected address.   |

---

## Managing presence access control lists

---

### Manage Presence access control lists

You can create the following rules

### **Enforced User ACL**

The Enforced User ACL rules can only be set by a user who is an administrator. These rules define the access of presence information between the individual presentities and watchers. You can set the Enforced User ACL rules with different priorities. The rules with higher priority take precedence over the rules with lower priority.

### **System ACL**

The System ACL rules are set at enterprise level that grant or deny a watcher permission to view the presence of all the users in the enterprise. The list that defines the System ACL rules may contain several entries and each entry corresponds to one watcher. System ACL provides critical system services with a privileged access to presence of all users.

### **System Rules**

The System Rules defines a certain level of presence access for everyone in the enterprise. You can define multiple System Rules that apply to all presentities and all watchers in the enterprise. System Rules allows you to enforce global policies.

### **System Default**

The System Default rules are global default rules that define access to presence information if none of the more specific rules apply. There must be one System Default rule defined in the System.

---

## **Viewing details of a high priority enforced ACL rule**

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, select a high priority ACL rule from the list of high priority ACL rules displayed in the High Priority Enforced User ACL section.
  3. Click **View**.
- 

### **Result**

The View Enforced User ACL page displays the details of the selected ACL rule.

### **Related topics:**

[View Enforced User ACL field descriptions](#) on page 1694

---

## Modifying a high priority enforced ACL rule

1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
2. On the Presence ACL page, select a high priority ACL rule from the list of high priority ACL rules in the High Priority Enforced User ACL section.
3. Perform one of the following steps:
  - Click **Edit**.
  - Click **View > Edit**.
4. On the Edit High Priority Enforced User ACL page, perform one of the following steps:
  - Click **New** and create a new access level.
  - Select an existing access level and click **Edit**.
5. Click **Commit** to save the changes.

---

### Related topics:

[Edit Enforced User ACL field descriptions](#) on page 1692

---

## Creating a new high priority enforced ACL rule

1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, click **New** in the High Priority Enforced User ACL section.
  3. On the New High Priority Enforced User ACL page, click **New**.
  4. Create an access level.
  5. Select presentities from the Select Presentity section.
  6. Select watchers from the Select Watcher section.
  7. Click **Commit**.
-

**Related topics:**

[New Enforced User ACL field descriptions](#) on page 1689

---

## Deleting high priority enforced ACL rules

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, select one or more high priority ACL rules from the list of high priority rules displayed in the High Priority Enforced User ACL section.
  3. Click **Delete**.
- 

---

## Viewing details of a low priority enforced ACL rule

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, select a low priority ACL rule from the list of low priority ACL rules displayed in the Low Priority Enforced User ACL section.
  3. Click **View**.
- 

**Result**

The View Enforced User ACL page displays the details of the selected ACL rule.

**Related topics:**

[View Enforced User ACL field descriptions](#) on page 1694

---

## Modifying a low priority enforced ACL rule

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, select a low priority ACL rule from the list of low priority enforced ACL rules displayed in the Low Priority Enforced User ACL section.

3. Perform one of the following steps:
  - Click **Edit**.
  - Click **View > Edit**.
4. On the Edit Low Priority Enforced User ACL page, perform one of the following steps:
  - Click **New** and create a new access level.
  - Select an existing access level and click **Edit**.
5. Click **Commit** to save the changes.

---

**Related topics:**

[Edit Enforced User ACL field descriptions](#) on page 1692

---

## Creating a low priority enforced ACL rule

1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
2. On the Presence ACL page, click **New** in the Low Priority Enforced User ACL section.
3. On the New Low Priority Enforced User ACL page, click **New**.
4. Create an access level.
5. Select presentities from the Select Presentity section.
6. Select watchers from the Select Watcher section.
7. Click **Commit**.

---

**Related topics:**

[New Enforced User ACL field descriptions](#) on page 1689

---

## Deleting low priority enforced ACL rules

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, select one or more low priority ACL rules from the list of low priority ACL rules displayed in the low Priority Enforced User ACL section.
  3. Click **Delete**.
- 

---

## Viewing details of a System ACL rule

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, select a system ACL rule from the list of System ACL rules displayed in the System ACL section.
  3. Click **View**.
- 

### Result

The View System ACL page displays the details of the selected ACL rule.

### Related topics:

[View System ACL field descriptions](#) on page 1700

---

## Modifying a System ACL rule

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, select a system ACL rule from the list of System ACL rules displayed in the System ACL section.
  3. Perform one of the following steps:
    - Click **Edit**.

- Click **View > Edit**.
4. On the Edit System ACL page, perform one of the following steps:
    - Click **New** and create a new access level.
    - Select an existing access level and click **Edit**.
  5. Click **Commit** to save the changes.
- 

**Related topics:**

[Edit System ACL field descriptions](#) on page 1698

[Edit System ACL field descriptions](#) on page 1698

---

## Creating a new System ACL rule

---

1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, click **New** in the System ACL section.
  3. On the New System ACL page, click **New**.
  4. Create an access level.
  5. Select watchers from the Select Watcher section.
  6. Click **Commit**.
- 

**Related topics:**

[New System ACL field descriptions](#) on page 1696

[New System ACL field descriptions](#) on page 1696

---

## Deleting System ACL rules

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, select one or more System ACL rules from list of System ACL rules in the System ACL section.
  3. Click **Delete**.
- 

---

## Defining a new policy for Enforced User ACL rules

You can use this feature to define a new policy for the high or low priority Enforced User ACL rules. An access level rule determines what permissions does a watcher has on the presence information of a presentity. Use this feature to add permissions over the presence information of a presentity for a watcher.

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, click **New** from the High or Low Priority Enforced User ACL section.  
If you want to add a new policy for an existing High or Low Enforced User ACL rule, select a rule and click **Edit**.
  3. On the New High Priority Enforced User ACL or Low Priority Enforced User ACL page, click **New** in the Define Policy .
  4. From the **Access Level** drop-down field, select an access level.
  5. From the **Action** drop-down field, select an action.
  6. Click **Save**.
- 

### Related topics:

[New Enforced User ACL field descriptions](#) on page 1689

[Edit Enforced User ACL field descriptions](#) on page 1692

---

## Modifying a policy for Enforced User ACL rules

You can use this feature to modify an existing policy for a high or low priority Enforced User ACL rule. An access level rule determines what permissions does a watcher has on the presence information of a presentity. Use this feature to modify the permissions over the presence information of a presentity for a watcher.

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, select a Enforced User ACL rule from the High or Low Priority Enforced User ACL section and click **Edit**.  
If you are creating a new High or Low Priority Enforced User ACL rule and are on the New High Priority Enforced User ACL or Low High Priority Enforced User ACL page, follow the next step.
  3. Select the access level rule that you want to modify.
  4. Click **Edit**.
  5. Modify the information in the respective fields.
  6. Click **Save**.

---

### Related topics:

[New Enforced User ACL field descriptions](#) on page 1689

[Edit Enforced User ACL field descriptions](#) on page 1692

---

## Deleting policies for Enforced User ACL rules

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, select a Enforced User ACL rule from the High or Low Priority Enforced User ACL section and click **Edit**.  
If you are creating a new High or Low Priority Enforced User ACL rule and are on the New High Priority Enforced User ACL or Low High Priority Enforced User ACL page, follow the next step.

3. Select one or more policies.
  4. Click **Delete**.
- 

---

## Creating a system rule

You can use this feature to define a certain level of presence access for everyone in the enterprise.

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, click **New** in the System Rule section.
  3. On the New System Rule page, click **New**.
  4. From the **Priority** drop-down field, select a priority.
  5. Create an access level.
  6. Click **Commit**.
- 

### Related topics:

[New System Rule field descriptions](#) on page 1701

---

## Modifying a System rule

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, select a system rule from the list of system rules displayed in the System Rule section.
  3. Click **Edit**.
  4. On the Edit System Rule page, perform one of the following steps:
    - Click **New** and create a new access level.
    - Select an existing access level and click **Edit** to modify the access level.
  5. Click **Commit** to save the changes.
-

**Related topics:**

[Edit System Rule field descriptions](#) on page 1702

---

## Deleting system rules

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, select a system rule from the list of system rules displayed in the System Rule section.
  3. Click **Delete**.
- 

---

## Filtering presentities

You can use this feature to filter and view selected presentities by using the following filter criteria:

- Status of the presentity.
- Name of the presentity
- Login Name of the presentity

You can filter presentities by applying one ore more filter criteria.

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, click **New** or **Edit** from the .High or Low Priority Enforced User ACL section.
  3. On the New High Priority Enforced User ACL page or Low High Priority Enforced User ACL page, click **Filter: Enable** from the Select Presentity section.
  4. Select or enter the filter criteria you want to apply to the selected presentity.
  5. Click **Filter:Apply**.
-

---

## Searching for presentities

1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
2. On the Presence ACL page, click **New**.
3. On the Create new ACL page, click **Advanced Search** in the Select Presentity section.
4. Select the search criteria and operator from the respective drop down fields.
5. Enter or select the search value in the third field.
6. Click the + button if you want to add another search condition.  
To delete a search condition, click the – button. You can delete a search condition only if you have more than one search condition specified.
7. Select the AND or OR operator from the drop-down field.  
This option appears when you add a search condition using the + button.
8. Click **Search** to find presentities for the given search conditions.

---

### Result

The page displays the presentities which meet the search criteria in the Select Presentity section.

---

## Filtering watchers

You can use this feature to filter and view only selected watchers by using the following filter criteria:

- Last name of the watcher
- First name of the watcher
- Contact type of the watcher. Contact types are User and Public contact.

- 
1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, perform one of the following steps: or **Edit** .
    - Click **New** in the .High Priority Enforced User ACL section.
    - Click **New** in the .Low Priority Enforced User ACL section.

- Click **New** in the System ACL section.
3. Click **Filter: Enable** from the Select Watcher section.
  4. Select or enter the filter criteria you want to apply to the selected watchers.
  5. Click **Filter:Apply**.
- 

## Searching for watchers

---

1. On the System Manager console, click **Users > System Presence ACLs** in the left navigation pane.
  2. On the Presence ACL page, click **New**.
  3. On the Create new ACL page, click **Advanced Search** in the Select Watcher section.
  4. Select the search criteria and operator from the respective drop down fields.
  5. Enter or select the search value in the third field.
  6. Click the + button if you want to add another search condition.  
To delete a search condition, click the – button. You can delete a search condition only if you have more than one search condition specified.
  7. Select the AND or OR operator from the drop-down field.  
This option appears when you add a search condition using the + button.
  8. Click **Search** to find watchers for the given search conditions.
- 

### Result

The page displays the watchers that meet the search criteria in the Select Watcher section.

## Presence ACL field descriptions

### High Priority Enforced User ACL (Access Control List)

This section displays the high priority enforced user access control list (ACL) rules for users. You can add a new rule, modify and delete an existing rule for users.

| Name                        | Description                 |
|-----------------------------|-----------------------------|
| <b>Presentity Last Name</b> | Last name of the presentity |

| Name                         | Description  |
|------------------------------|--|
| <b>Presentity First Name</b> | First name of the presentity.  |
| <b>Watcher Last Name</b>     | Last name of the watcher.  |
| <b>Watcher First Name</b>    | First name of the watcher.   |
| <b>Watcher Type</b>          | Categorization of the watcher based on whether the watcher is a public or private contact. |
| <b>Access Level</b>          | Presence information for which access control rules are set.                               |
| <b>Action</b>                | Defines the access control permission over the presence information.                       |

| Button        | Description  |
|---------------|--|
| <b>View</b>   | Opens the View Enforced User ACL page. Use this page to view the high priority enforced user ACL rules set for the watchers.   |
| <b>Edit</b>   | Opens the Edit High Priority Enforced User ACL page. Use this page to edit a high priority enforced user ACL rule set for a watcher.   |
| <b>New</b>    | Opens the New High Priority Enforced User ACL page. Use this page to create a rule by adding one or more access control rules and assigning these rules to one or more watchers. |
| <b>Delete</b> | Deletes the selected high priority enforced user ACL rules.  |

### Low Priority Enforced User ACL

This section displays the low priority enforced user ACL rules for users. You can add a new rule, modify and delete an existing rule for users.

| Name                         | Description  |
|------------------------------|--|
| <b>Presentity Last Name</b>  | Last name of the presentity  |
| <b>Presentity First Name</b> | First name of the presentity.  |
| <b>Watcher Last Name</b>     | Last name of the watcher.  |
| <b>Watcher First Name</b>    | First name of the watcher.   |
| <b>Watcher Type</b>          | Categorization of the watcher based on whether the watcher is a public or private contact. |
| <b>Access Level</b>          | Presence information for which access control rules are set.                               |
| <b>Action</b>                | Defines the access control permission over the presence information.                       |

| Button      | Description   |
|-------------|---|
| <b>View</b> | Opens the View Enforced User ACL page. Use this page to view the low priority enforced user ACL rules set for the watchers. |

| Button        | Description   |
|---------------|---|
| <b>Edit</b>   | Opens the Edit Low Priority Enforced User ACL page. Use this page to edit a low priority enforced user ACL rule set for a watcher.  |
| <b>New</b>    | Opens the New Low Priority Enforced User ACL page. Use this page to create a rule by adding one or more access control rules and assigning these rules to one or more watchers. |
| <b>Delete</b> | Deletes the selected low priority enforced user ACL rules.  |

## System ACL

This section displays the system ACL rules for watchers. You can add a new rule, modify and delete an existing rule for watchers.

| Name                             | Description  |
|----------------------------------|--|
| <b>Watcher Last Name</b>         | Last name of the watcher.  |
| <b>Watcher First Name</b>        | First name of the watcher.   |
| <b>Display Name / Login Name</b> | Display or login name of the watcher.  |
| <b>Watcher Type</b>              | Categorization of the watcher based on whether the watcher is a public or private contact. |
| <b>Access Level</b>              | Presence information for which access control rules are set.                               |
| <b>Action</b>                    | Defines the access control permission over the presence information.                       |

| Button        | Description   |
|---------------|---|
| <b>View</b>   | Opens the View System ACL page. Use this page to view the system ACL rules set for the watchers.  |
| <b>Edit</b>   | Opens the Edit System ACL page. Use this page to edit a system ACL rule set for a watcher.  |
| <b>New</b>    | Opens the New System ACL page. Use this page to create a rule by adding one or more access control rules and assigning these rules to one or more watchers. |
| <b>Delete</b> | Deletes the selected System ACL rules.  |

## System Rule

This section displays the system rules. You can add a new rule, modify and delete an existing system rule.

| Name                | Description  |
|---------------------|--|
| <b>Priority</b>     | Priority set for the rule.   |
| <b>Access Level</b> | Presence information for which access control rules are set.         |
| <b>Action</b>       | Defines the access control permission over the presence information. |

| Button        | Description   |
|---------------|---|
| <b>Edit</b>   | Opens the Edit System rule page. Use this page to edit a system rule.   |
| <b>New</b>    | Opens the New System rule page. Use this page to create a new system rule by adding one or more access control rules. |
| <b>Delete</b> | Deletes the selected system rules.  |

### Define Policy

You can use this section to define your personal rules for accessing your presence information by one or more watchers.

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use this check box to select a rule.                                 |
| <b>Access Level</b>     | Presence information for which access control rules are set.         |
| <b>Action</b>           | Defines the access control permission over the presence information. |

| Button        | Description  |
|---------------|--|
| <b>Edit</b>   | Use this button to modify an existing rule.                              |
| <b>New</b>    | Use this button to add a new rule for the watchers.                      |
| <b>Delete</b> | Deletes the selected rule from the list of rules added for the watchers. |

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

| Name                | Description   |
|---------------------|---|
| <b>Access Level</b> | Presence information for which access control rules are set.<br>The options are <ul style="list-style-type: none"> <li>• Telephony: Telephony related presence information for which you can set an access permission.</li> <li>• All: Contains all the presence information types for which you can set an access permission.</li> </ul>   |
| <b>Action</b>       | Defines the access control permission over the presence information.<br>The options are: <ul style="list-style-type: none"> <li>• Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher.</li> <li>• Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher.</li> </ul> |

| Name | Description   |
|------|---|
|      | <ul style="list-style-type: none"> <li>• Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information.</li> <li>• Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.</li> </ul> |

| Button      | Description   |
|-------------|---|
| <b>Save</b> | Saves the rules information in the database when you add or modify a rule for watchers. |

## New Enforced User ACL field descriptions

### Define Policy

You can use this section to add permissions on the presentity presence information for one or more watchers.

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use this check box to select a rule.                                 |
| <b>Access Level</b>     | Presence information for which access control rules are set.         |
| <b>Action</b>           | Defines the access control permission over the presence information. |

| Button        | Description  |
|---------------|--|
| <b>Edit</b>   | Use this button to modify an existing rule.                              |
| <b>New</b>    | Use this button to add a new rule for the watchers.                      |
| <b>Delete</b> | Deletes the selected rule from the list of rules added for the watchers. |

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

| Name                | Description   |
|---------------------|---|
| <b>Access Level</b> | Presence information for which access control rules are set.<br>The options are <ul style="list-style-type: none"> <li>• Telephony: Telephony related presence information for which you can set an access permission.</li> <li>• All: Contains all the presence information types for which you can set an access permission.</li> </ul> |
| <b>Action</b>       | Defines the access control permission over the presence information.  |

| Name | Description   |
|------|---|
|      | <p>The options are:</p> <ul style="list-style-type: none"> <li>• Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher.</li> <li>• Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher.</li> <li>• Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information.</li> <li>• Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.</li> </ul> |

| Button      | Description   |
|-------------|---|
| <b>Save</b> | Saves the rules information in the database when you add or modify a rule for watchers. |

### Select Presentity

| Name                   | Description   |
|------------------------|---|
| <b>Status</b>          | The current login status of the user. Online indicates that the user is currently logged into System Manager and offline indicates the user is logged out of the system. The column displays an image for the status. |
| <b>Name</b>            | Name of the user.   |
| <b>User Name</b>       | Unique name that gives access to the system.  |
| <b>Last Login</b>      | Date and time when the user has successfully logged into the system.  |
| <b>Advanced Search</b> | Displays fields that you can use to specify the search criteria to search for presentities.   |
| <b>Filter: Enable</b>  | Displays fields under select columns that you can use to set filter criteria. This is a toggle button.  |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.  |
| <b>Filter: Apply</b>   | Filters presentities based on the filter criteria.  |
| <b>Select: All</b>     | Selects all the presentities in the table.  |
| <b>Select: None</b>    | Clears the check box selections.  |
| <b>Refresh</b>         | Refreshes the presentity information in the table.  |

## Select Watcher

| Name                           | Description  |
|--------------------------------|--|
| <b>Last Name</b>               | Last name of the watcher.  |
| <b>First Name</b>              | First name of the watcher.   |
| <b>Display Name/Login Name</b> | Display or login name of the watcher   |
| <b>Contact Type</b>            | Identifies whether the watcher is a private or public contact.   |
| <b>Description</b>             | A brief description about the watcher.   |
| <b>Advanced Search</b>         | Displays fields that you can use to specify the search criteria to search for watchers.                |
| <b>Filter: Enable</b>          | Displays fields under select columns that you can use to set filter criteria. This is a toggle button. |
| <b>Filter: Disable</b>         | Hides the column filter fields without resetting the filter criteria. This is a toggle button.         |
| <b>Filter: Apply</b>           | Filters watchers based on the filter criteria.   |
| <b>Select: All</b>             | Selects all the watchers in the table.   |
| <b>Select: None</b>            | Clears the check box selections.   |
| <b>Refresh</b>                 | Refreshes the watcher information in the table.  |

The page displays the following field when you click the **Advanced Search** button above the presentity and watcher table at the upper-right corner.

| Name            | Description   |
|-----------------|---|
| <b>Criteria</b> | Use the fields to define the search criteria for searching the watchers and presentities in the database. Displays the following three fields: <ul style="list-style-type: none"> <li>• Drop-down 1 - Lists the search criteria.</li> <li>• Drop-down 2 – The operators for evaluating the expression. Based on the search criterion which you select in the first drop-down field, only those operators that are applicable for the selected criterion are displayed in the second drop-down field.</li> <li>• Field 3 – The value for the search criterion</li> </ul> |

| Name          | Description  |
|---------------|--|
| <b>Commit</b> | Creates the new enforced user ACL rule for the watchers. |

### Related topics:

[Creating a new high priority enforced ACL rule](#) on page 1675

[Creating a low priority enforced ACL rule](#) on page 1677

[Defining a new policy for Enforced User ACL rules](#) on page 1680

[Modifying a policy for Enforced User ACL rules](#) on page 1681

## Edit Enforced User ACL field descriptions

### Edit Access Level Along With Action

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use this check box to select a rule.                                 |
| <b>Access Level</b>     | Presence information for which access control rules are set.         |
| <b>Action</b>           | Defines the access control permission over the presence information. |

| Button        | Description  |
|---------------|--|
| <b>Edit</b>   | Use this button to modify an existing rule.                              |
| <b>New</b>    | Use this button to add a new rule for the watchers.                      |
| <b>Delete</b> | Deletes the selected rule from the list of rules added for the watchers. |

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

| Name                | Description  |
|---------------------|--|
| <b>Access Level</b> | <p>Presence information for which access control rules are set.<br/>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Telephony:</b> Telephony related presence information for which you can set an access permission.</li> <li>• <b>All:</b> Contains all the presence information types for which you can set an access permission.</li> </ul>   |
| <b>Action</b>       | <p>Defines the access control permission over the presence information.<br/>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Allow:</b> If you select this action for an access level, presence information associated with that access level is accessible to the watcher.</li> <li>• <b>Block:</b> If you select this action for an access level, presence information associated with this access level is not accessible to the watcher.</li> <li>• <b>Confirmed:</b> If you select this action, watcher needs confirmation from the presentities to access their presence information.</li> <li>• <b>Undefined:</b> If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.</li> </ul> |

| Button | Description   |
|--------|---|
| Save   | Saves the rules information in the database when you add or modify a rule for watchers. |

## Presentity

| Name                   | Description   |
|------------------------|---|
| Last Name              | Last name of the presentity.  |
| First Name             | First name of the presentity.   |
| Middle Name            | Middle name of the presentity   |
| Description            | Brief description about the presentity.   |
| Login Name             | A unique system login name for users that includes the users marked as deleted. It takes the form of username@domain. It is used to create the user's primary handle. |
| Localized Display Name | Localized display name of the presentity. It is the localized full name.  |
| Endpoint Display Name  | Display name that identifies the presentity for an endpoint.  |

## Contact Address

| Name        | Description   |
|-------------|---|
| Handle      | Unique contact address for communication with the presentity. |
| Handle Type | Qualifier that represents the type of handle.                 |
| Sub Type    | Sub type defines the format of the address for the handle     |
| Domain      | Domain to which the handle belongs.                           |

## Watcher

| Name                   | Description   |
|------------------------|---|
| Last Name              | Last name of the watcher.   |
| First Name             | First name of the watcher.  |
| Middle Name            | Middle name of the watcher.   |
| Description            | Brief description about the watcher.                                  |
| Company                | Company name of the watcher.  |
| Localized Display Name | Localized display name of the watcher. It is the localized full name. |
| Endpoint Display Name  | Display name that identifies the watcher for an endpoint.             |

## Contact Address

| Name                     | Description  |
|--------------------------|--|
| <b>Address</b>           | Contact address of the watcher.  |
| <b>Type</b>              | Qualifier that represents the type of address.   |
| <b>Category</b>          | Category defines whether the address is an official or residential address.  |
| <b>Label</b>             | A text description for classifying this contact.   |
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language. |

| Name          | Description                        |
|---------------|------------------------------------|
| <b>Commit</b> | Saves the changes to the database. |

### Related topics:

[Modifying a high priority enforced ACL rule](#) on page 1675

[Modifying a low priority enforced ACL rule](#) on page 1676

[Defining a new policy for Enforced User ACL rules](#) on page 1680

[Modifying a policy for Enforced User ACL rules](#) on page 1681

---

## View Enforced User ACL field descriptions

### View Access Level Along With Action

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use this check box to select a rule.                                 |
| <b>Access Level</b>     | Presence information for which access control rules are set.         |
| <b>Action</b>           | Defines the access control permission over the presence information. |

### Presentity

| Name               | Description                             |
|--------------------|---|
| <b>Last Name</b>   | Last name of the presentity.            |
| <b>First Name</b>  | First name of the presentity.           |
| <b>Middle Name</b> | Middle name of the presentity           |
| <b>Description</b> | Brief description about the presentity. |

| Name                          | Description   |
|-------------------------------|---|
| <b>Login Name</b>             | A unique system login name for users that includes the users marked as deleted. It takes the form of username@domain. It is used to create the user's primary handle. |
| <b>Localized Display Name</b> | Localized display name of the presentity. It is the localized full name.  |
| <b>Endpoint Display Name</b>  | Display name that identifies the presentity for an endpoint.  |

### Contact Address

| Name               | Description   |
|--------------------|---|
| <b>Handle</b>      | Unique contact address for communication with the presentity. |
| <b>Handle Type</b> | Qualifier that represents the type of handle.                 |
| <b>Sub Type</b>    | Sub type defines the format of the address for the handle     |
| <b>Domain</b>      | Domain to which the handle belongs.                           |

### Watcher

| Name                          | Description   |
|-------------------------------|---|
| <b>Last Name</b>              | Last name of the watcher.   |
| <b>First Name</b>             | First name of the watcher.  |
| <b>Middle Name</b>            | Middle name of the watcher.   |
| <b>Description</b>            | Brief description about the watcher.                                  |
| <b>Company</b>                | Company name of the watcher.  |
| <b>Localized Display Name</b> | Localized display name of the watcher. It is the localized full name. |
| <b>Endpoint Display Name</b>  | Display name that identifies the watcher for an endpoint.             |

### Contact Address

| Name            | Description   |
|-----------------|---|
| <b>Address</b>  | Contact address of the watcher.   |
| <b>Type</b>     | Qualifier that represents the type of address.                              |
| <b>Category</b> | Category defines whether the address is an official or residential address. |
| <b>Label</b>    | A text description for classifying this contact.                            |

| Name                     | Description  |
|--------------------------|--|
| <b>Alternative Label</b> | A text description for classifying this contact. This is similar to Label, but it is used to store label in an alternate language. |

| Name        | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Edit High Priority Enforced User ACL page. Use this page to edit the high priority ACL for a watcher. |

**Related topics:**

[Viewing details of a high priority enforced ACL rule](#) on page 1674

[Viewing details of a low priority enforced ACL rule](#) on page 1676

## New System ACL field descriptions

Use this page to add enterprise wide permissions on the presence information of presentities in an enterprise and associate these permissions with the watchers.

### Define Policy

You can use this section to add permissions on the presentity presence information for one or more watchers.

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use this check box to select a rule.                                 |
| <b>Access Level</b>     | Presence information for which access control rules are set.         |
| <b>Action</b>           | Defines the access control permission over the presence information. |

| Button        | Description  |
|---------------|--|
| <b>Edit</b>   | Use this button to modify an existing rule.                              |
| <b>New</b>    | Use this button to add a new rule for the watchers.                      |
| <b>Delete</b> | Deletes the selected rule from the list of rules added for the watchers. |

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

| Name                | Description   |
|---------------------|---|
| <b>Access Level</b> | <p>Presence information for which access control rules are set. The options are</p> <ul style="list-style-type: none"> <li>• <b>Telephony:</b> Telephony related presence information for which you can set an access permission.</li> <li>• <b>All:</b> Contains all the presence information types for which you can set an access permission.</li> </ul> |

| Name          | Description   |
|---------------|---|
| <b>Action</b> | Defines the access control permission over the presence information. The options are: <ul style="list-style-type: none"> <li>• Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher.</li> <li>• Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher.</li> <li>• Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information.</li> <li>• Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.</li> </ul> |

| Button      | Description   |
|-------------|---|
| <b>Save</b> | Saves the rules information in the database when you add or modify a rule for watchers. |

### Select Watcher

| Name                           | Description  |
|--------------------------------|--|
| <b>Last Name</b>               | Last name of the watcher.  |
| <b>First Name</b>              | First name of the watcher.   |
| <b>Display Name/Login Name</b> | Display or login name of the watcher.  |
| <b>Contact Type</b>            | Identifies whether the watcher is a private or public contact.   |
| <b>Description</b>             | A brief description about the watcher.   |
| <b>Advanced Search</b>         | Displays fields that you can use to specify the search criteria to search for watchers.                |
| <b>Filter: Enable</b>          | Displays fields under select columns that you can use to set filter criteria. This is a toggle button. |
| <b>Filter: Disable</b>         | Hides the column filter fields without resetting the filter criteria. This is a toggle button.         |
| <b>Filter: Apply</b>           | Filters watchers based on the filter criteria.   |
| <b>Select: All</b>             | Selects all the watchers in the table.   |
| <b>Select: None</b>            | Clears the check box selections.   |
| <b>Refresh</b>                 | Refreshes the watcher information in the table.  |

The page displays the following field when you click the **Advanced Search** button above the presentity and watcher table at the upper-right corner.

| Name            | Description   |
|-----------------|---|
| <b>Criteria</b> | Search criteria for searching the watchers or presentities. |

| Name          | Description                                       |
|---------------|---|
| <b>Commit</b> | Creates the new system ACL rule for the watchers. |

**Related topics:**

[Creating a new System ACL rule](#) on page 1679

[Creating a new System ACL rule](#) on page 1679

## Edit System ACL field descriptions

### Edit Access Level Along With Action

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use this check box to select a rule.                                 |
| <b>Access Level</b>     | Presence information for which access control rules are set.         |
| <b>Action</b>           | Defines the access control permission over the presence information. |

| Button        | Description  |
|---------------|--|
| <b>Edit</b>   | Use this button to modify an existing rule.                              |
| <b>New</b>    | Use this button to add a new rule for the watchers.                      |
| <b>Delete</b> | Deletes the selected rule from the list of rules added for the watchers. |

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

| Name                | Description   |
|---------------------|---|
| <b>Access Level</b> | Presence information for which access control rules are set.<br>The options are <ul style="list-style-type: none"> <li>• Telephony: Telephony related presence information for which you can set an access permission.</li> <li>• All: Contains all the presence information types for which you can set an access permission.</li> </ul> |
| <b>Action</b>       | Defines the access control permission over the presence information.  |

| Name | Description   |
|------|---|
|      | <p>The options are:</p> <ul style="list-style-type: none"> <li>• Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher.</li> <li>• Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher.</li> <li>• Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information.</li> <li>• Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.</li> </ul> |

| Button | Description   |
|--------|---|
| Save   | Saves the rules information in the database when you add or modify a rule for watchers. |

### Watcher

You can only view information in these fields.

| Name                   | Description   |
|------------------------|---|
| Last Name              | Last name of the watcher.                                 |
| First Name             | First name of the watcher.                                |
| Middle Name            | Middle name of the watcher.                               |
| Description            | Brief description about the watcher.                      |
| Company                | Company name of the watcher.                              |
| Localized Display Name | Brief description about the watcher.                      |
| Endpoint Display Name  | Display name that identifies the watcher for an endpoint. |

### Contact Address

You can only view information in these fields.

| Name              | Description   |
|-------------------|---|
| Address           | Contact address of the watcher.   |
| Type              | Qualifier that represents the type of address.                              |
| Category          | Category defines whether the address is an official or residential address. |
| Label             | Need Information  |
| Alternative Label | Need Information  |

| Name          | Description                        |
|---------------|------------------------------------|
| <b>Commit</b> | Saves the changes to the database. |

**Related topics:**

[Modifying a System ACL rule](#) on page 1678

[Modifying a System ACL rule](#) on page 1678

## View System ACL field descriptions

### View Access Level Along With Action

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use this check box to select a rule.                                 |
| <b>Access Level</b>     | Presence information for which access control rules are set.         |
| <b>Action</b>           | Defines the access control permission over the presence information. |

### Watcher

| Name                          | Description   |
|-------------------------------|---|
| <b>Last Name</b>              | Last name of the watcher.                                 |
| <b>First Name</b>             | First name of the watcher.                                |
| <b>Middle Name</b>            | Middle name of the watcher.                               |
| <b>Description</b>            | Brief description about the watcher.                      |
| <b>Company</b>                | Company name of the watcher.                              |
| <b>Localized Display Name</b> | Brief description about the watcher.                      |
| <b>Endpoint Display Name</b>  | Display name that identifies the watcher for an endpoint. |

### Contact Address

| Name                     | Description   |
|--------------------------|---|
| <b>Address</b>           | Contact address of the watcher.   |
| <b>Type</b>              | Qualifier that represents the type of address.                              |
| <b>Category</b>          | Category defines whether the address is an official or residential address. |
| <b>Label</b>             | Need Information  |
| <b>Alternative Label</b> | Need Information  |

| Name        | Description   |
|-------------|---|
| <b>Edit</b> | Opens the Edit High Priority Enforced User ACL page. Use this page to edit the high priority ACL for a watcher. |

**Related topics:**

[Viewing details of a System ACL rule](#) on page 1678

---

## New System Rule field descriptions

**New System Rule**

Use this section to set a priority for the new rule.

| Name            | Description  |
|-----------------|--|
| <b>Priority</b> | <p>Defines a priority for the new rule. The options are:</p> <ul style="list-style-type: none"> <li>• High</li> <li>• Low</li> </ul> <p>The rule with high priority has more weight than the rule with low priority.</p> |

**Define Policy**

You can use this section to add permissions on the presentity presence information for one or more watchers.

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use this check box to select a rule.                                 |
| <b>Access Level</b>     | Presence information for which access control rules are set.         |
| <b>Action</b>           | Defines the access control permission over the presence information. |

| Button        | Description  |
|---------------|--|
| <b>Edit</b>   | Use this button to modify an existing rule.                              |
| <b>New</b>    | Use this button to add a new rule for the watchers.                      |
| <b>Delete</b> | Deletes the selected rule from the list of rules added for the watchers. |

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

| Name                | Description  |
|---------------------|--|
| <b>Access Level</b> | Presence information for which access control rules are set. |

| Name          | Description   |
|---------------|---|
|               | The options are <ul style="list-style-type: none"> <li>• Telephony: Telephony related presence information for which you can set an access permission.</li> <li>• All: Contains all the presence information types for which you can set an access permission.</li> </ul>   |
| <b>Action</b> | Defines the access control permission over the presence information. The options are: <ul style="list-style-type: none"> <li>• Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher.</li> <li>• Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher.</li> <li>• Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information.</li> <li>• Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.</li> </ul> |

| Button      | Description   |
|-------------|---|
| <b>Save</b> | Saves the rules information in the database when you add or modify a rule for watchers. |

| Name          | Description                                |
|---------------|--|
| <b>Commit</b> | Creates the new system rule for the users. |

**Related topics:**

[Creating a system rule](#) on page 1682

## Edit System Rule field descriptions

Use this page to edit a system rule.

### Edit Access Level Along With Action

You can use this section to add permissions on the presentity presence information for one or more watchers.

| Name                    | Description  |
|-------------------------|--|
| <b>Select Check box</b> | Use this check box to select a rule.                                 |
| <b>Access Level</b>     | Presence information for which access control rules are set.         |
| <b>Action</b>           | Defines the access control permission over the presence information. |

| Button        | Description  |
|---------------|--|
| <b>Edit</b>   | Use this button to modify an existing rule.                              |
| <b>New</b>    | Use this button to add a new rule for the watchers.                      |
| <b>Delete</b> | Deletes the selected rule from the list of rules added for the watchers. |

The page displays the following fields when you click the **New** or **Edit** button in the Define policy section.

| Name                | Description  |
|---------------------|--|
| <b>Access Level</b> | <p>Presence information for which access control rules are set.<br/>The options are</p> <ul style="list-style-type: none"> <li>• Telephony: Telephony related presence information for which you can set an access permission.</li> <li>• All: Contains all the presence information types for which you can set an access permission.</li> </ul>  |
| <b>Action</b>       | <p>Defines the access control permission over the presence information.<br/>The options are:</p> <ul style="list-style-type: none"> <li>• Allow: If you select this action for an access level, presence information associated with that access level is accessible to the watcher.</li> <li>• Block: If you select this action for an access level, presence information associated with this access level is not accessible to the watcher.</li> <li>• Confirmed: If you select this action, watcher needs confirmation from the presentities to access their presence information.</li> <li>• Undefined: If you select this action for an access level , access to the presence information associated with this access level is not defined for the watcher.</li> </ul> |

| Button      | Description   |
|-------------|---|
| <b>Save</b> | Saves the rules information in the database when you add or modify a rule for watchers. |

| Name          | Description                        |
|---------------|------------------------------------|
| <b>Commit</b> | Saves the changes to the database. |

**Related topics:**

[Modifying a System rule](#) on page 1682



## Index

---

### Special Characters

|   |   |
|---|---|
| (Calls Warning) Port .....  | <a href="#">646</a>                       |
| (Starting) Port .....   | <a href="#">431</a> , <a href="#">833</a> |
| (Time Warning) Port .....   | <a href="#">652</a>                       |
| % of Gateways in Network Region with Hyperactive<br>Registration Alarms ..... | <a href="#">705</a>                       |

---

### Numerics

|   |                      |
|---|----------------------|
| 01 through XX<br>Call Vector .....                    | <a href="#">465</a>  |
| 01–1000 .....   | <a href="#">841</a>  |
| 1-number access .....                                 | <a href="#">389</a>  |
| 1-Step Clearing .....                                 | <a href="#">877</a>  |
| 1408/1416 Native Support .....                        | <a href="#">201</a>  |
| 1st/2nd/3rd Skill .....                               | <a href="#">1048</a> |
| 2-Party Loss Plan/Tone Loss Plan .....                | <a href="#">777</a>  |
| 440Hz PBX-dial Tone .....                             | <a href="#">975</a>  |
| 440Hz Secondary-dial Tone .....                       | <a href="#">975</a>  |
| 6400/8400/2420J LINE APPEARANCE LED SETTINGS<br>..... | <a href="#">628</a>  |
| 7103A Button List .....                               | <a href="#">428</a>  |
| 7405ND Numeric Terminal Display .....                 | <a href="#">591</a>  |
| 7434ND .....  | <a href="#">591</a>  |
| 802.1p .....  | <a href="#">713</a>  |
| 802.1P/Q Parameters .....                             | <a href="#">693</a>  |

---

### A

|  |  |
|--|--|
| A/D Grp/Sys List Dialing Start at 01 .....                                 | <a href="#">942</a>                        |
| AAR and ARS Digit Analysis Table .....                                     | <a href="#">418</a>                        |
| AAR and ARS Digit Conversion Table .....                                   | <a href="#">421</a>                        |
| AAR/ARS Access .....   | <a href="#">591</a>                        |
| AAR/ARS Access Code .....  | <a href="#">498</a> , <a href="#">529</a>  |
| AAR/ARS Dial Tone Required .....   | <a href="#">573</a>                        |
| AAR/ARS Internal Call Prefix .....   | <a href="#">533</a>                        |
| AAR/ARS Internal Call Total Length .....                                   | <a href="#">533</a>                        |
| AAR/ARS Partitioning .....   | <a href="#">484</a>                        |
| AAS .....  | <a href="#">435</a> , <a href="#">653</a>  |
| Abandoned Call Search .....  | <a href="#">738</a> , <a href="#">1009</a> |
| Abbreviated Dial .....   | <a href="#">559</a>                        |
| Abbreviated Dial Programming by Assigned Lists ....<br><a href="#">574</a> |  |
| abbreviated dialing .....  | <a href="#">501</a>                        |
| Abbreviated dialing  |  |

|   |   |
|---|---|
| Adding group lists .....  | <a href="#">226</a>   |
| station access to new group list .....  | <a href="#">225</a>   |
| Abbreviated Dialing .....   | <a href="#">579</a>   |
| ABBREVIATED DIALING .....   | <a href="#">455</a>   |
| Abbreviated Dialing Enhanced List ....  | <a href="#">74</a> , <a href="#">423</a> , <a href="#">942</a> , <a href="#">1086</a> |
| Abbreviated Dialing List 1, List 2, List 3 ....                                       | <a href="#">74</a> , <a href="#">877</a> , <a href="#">1085</a>                       |
| Abbreviated Dialing List1 Access Code .....   | <a href="#">558</a>   |
| Abbreviated Dialing List2 Access Code .....   | <a href="#">558</a>   |
| Abbreviated Dialing List3 Access Code .....   | <a href="#">559</a>   |
| abbreviated dialing lists .....   | <a href="#">74</a> , <a href="#">501</a> , <a href="#">1085</a>                       |
| Abbreviated Dialing Lists .....   | <a href="#">225</a> , <a href="#">226</a> , <a href="#">228</a>                       |
| Troubleshooting .....   | <a href="#">226</a>   |
| Abort Conference Upon Hang-Up .....   | <a href="#">596</a>   |
| Abort Transfer .....  | <a href="#">596</a>   |
| aborting a global user settings import job on first error ...<br><a href="#">1419</a> |   |
| aborting a role importing job .....   | <a href="#">1205</a>  |
| aborting a user import job .....  | <a href="#">1413</a>  |
| about Adaptations .....   | <a href="#">1242</a>  |
| about dial patterns .....   | <a href="#">1281</a>  |
| about Domains .....   | <a href="#">1233</a>  |
| about entity links .....  | <a href="#">1266</a>  |
| about locations .....   | <a href="#">1237</a>  |
| About regular expressions .....   | <a href="#">1288</a>  |
| about routing policies .....  | <a href="#">1274</a>  |
| about Service Profile Management .....  | <a href="#">1336</a>  |
| about SIP entities .....  | <a href="#">1255</a>  |
| about SIP entity references .....   | <a href="#">1265</a>  |
| About the time ranges .....   | <a href="#">1270</a>  |
| about Trust Management .....  | <a href="#">38</a>  |
| Absorption Treatment Assignment .....   | <a href="#">536</a>   |
| Absorption Treatment Information .....  | <a href="#">536</a>   |
| AC .....  | <a href="#">460</a>   |
| Authorization Code — COR Mapping .....  | <a href="#">460</a>   |
| ACA Assignment .....  | <a href="#">738</a> , <a href="#">1009</a>  |
| ACA Long Holding Time Originating Extension .....                                     | <a href="#">574</a>   |
| ACA Referral Calls .....  | <a href="#">574</a>   |
| ACA Referral Destination .....  | <a href="#">574</a>   |
| ACA Remote PBX Identification .....   | <a href="#">575</a>   |
| ACA Short Holding Time Originating Extension .....                                    | <a href="#">575</a>   |
| Acceptable Service Level (sec) .....  | <a href="#">1048</a>  |
| Access Code .....   | <a href="#">877</a>   |
| Access Code 2 .....   | <a href="#">559</a>   |
| Access Endpoint .....   | <a href="#">429</a>   |
| Access Security Gateway .....   | <a href="#">137</a>   |
| Access Security Gateway (ASG) .....   | <a href="#">942</a>   |
| Access to MCT .....   | <a href="#">479</a>   |

|   |   |  |   |
|---|---|--|---|
| Accessing .....   | <a href="#">135</a>   | adding a postal address of a public contact .....            | <a href="#">1657</a>                      |
| Accessing Avaya S8XXX Server remotely .....                                 | <a href="#">135</a>   | adding a private contact .....                               | <a href="#">1602</a>                      |
| accessing log harvest .....   | <a href="#">1115</a>  | adding a public contact .....                                | <a href="#">1655</a>                      |
| accessing resources .....   | <a href="#">1186</a>  | adding a shared address .....                                | <a href="#">1671</a>                      |
| accessing scheduler .....   | <a href="#">1318</a>  | adding a station profile .....                               | <a href="#">1568</a>                      |
| accessing the Data Retention Rules service ....                             | <a href="#">1300</a> ,  | adding a subnet .....  | <a href="#">120</a>                       |
|   | <a href="#">1310</a>  | Adding Abbreviated Dialing Lists .....                       | <a href="#">226</a>                       |
| accessing the Log Settings service .....                                    | <a href="#">1108</a>  | adding an announcement .....                                 | <a href="#">87</a>                        |
| accessing WebLM .....   | <a href="#">1131</a>  | adding an audio group .....                                  | <a href="#">96</a>                        |
| ACD .....   | <a href="#">318</a> , <a href="#">645</a> , <a href="#">950</a>   | adding an SNMP Access profile .....                          | <a href="#">117</a>                       |
| enhancing .....   | <a href="#">318</a>   | adding announcements .....                                   | <a href="#">87</a>                        |
| ACD Login Identification Length .....                                       | <a href="#">618</a>   | adding attributes to a permission .....                      | <a href="#">1209</a>                      |
| Act Time .....  | <a href="#">755</a> , <a href="#">970</a> , <a href="#">971</a>   | adding audio groups .....                                    | <a href="#">96</a>                        |
| Activate Answer Detection (Preserves SBA) On Final<br>CCRON Cvg Point ..... | <a href="#">932</a>   | Adding data sharing to a video conference .....              | <a href="#">397</a>                       |
| Activation .....  | <a href="#">238</a>   | adding endpoints   |   |
| Active Station Ringing .....  | <a href="#">60</a> , <a href="#">878</a> , <a href="#">1072</a>   | add endpoints .....  | <a href="#">52</a>                        |
| Actual % .....  | <a href="#">828</a>   | Adding fax modem .....                                       | <a href="#">184</a>                       |
| ACW Agent Considered Idle .....   | <a href="#">436</a>   | Adding feature buttons .....                                 | <a href="#">204</a>                       |
| ACW Agents Considered Idle .....  | <a href="#">615</a>   | adding groups and resources to a permission .....            | <a href="#">1208</a>                      |
| ACW Forced Logout Reason Code .....   | <a href="#">623</a>   | Adding IP Softphones .....                                   | <a href="#">187</a>                       |
| Ad hoc Video Conferencing .....   | <a href="#">493</a>   | Adding multiple call center agents .....                     | <a href="#">174</a>                       |
| adaptation deletion .....   | <a href="#">1249</a>  | Adding Remote Office to Avaya Communication<br>Manager ..... | <a href="#">194</a>                       |
| adaptation details .....  | <a href="#">1252</a>  | adding resources to a selected group .....                   | <a href="#">1188</a>                      |
| adaptation example .....  | <a href="#">1243</a>  | Adding Road Warrior .....                                    | <a href="#">188</a>                       |
| adaptation Module administration .....                                      | <a href="#">1244</a>  | adding subnets .....   | <a href="#">120</a>                       |
| adaptations .....   | <a href="#">1252</a>  | adding subscriber templates .....                            | <a href="#">1088</a>                      |
| adapters  |   | adding subscriber templates MM .....                         | <a href="#">1090</a>                      |
| AT&T Adapter (AttAdapter) .....   | <a href="#">1251</a>  | adding subscribers CMM; field description                    |   |
| Cisco Adapter (CiscoAdapter) .....  | <a href="#">1249</a>  | CMM field description  |   |
| Verizon Adapter (VerizonAdapter) .....                                      | <a href="#">1251</a>  | editing subscribers CMM field description ....               | <a href="#">105</a>                       |
| add .....   | <a href="#">52</a> , <a href="#">87</a> , <a href="#">96</a> , <a href="#">117</a> , <a href="#">120</a> , <a href="#">122</a>          | viewing subscribers CMM; field description ....              | <a href="#">105</a>                       |
| Add Address page ....   | <a href="#">1402</a> , <a href="#">1403</a> , <a href="#">1614</a> , <a href="#">1661</a> , <a href="#">1668</a> , <a href="#">1672</a> | adding subscribers MM; field description                     |   |
| Add Agent Skill Access Code .....   | <a href="#">569</a>   | MM field description   |   |
| add endpoints .....   | <a href="#">58</a> , <a href="#">1069</a>   | editing subscribers MM; field description ....               | <a href="#">107</a>                       |
| Add Local WebLM page .....  | <a href="#">1149</a>  | Viewing Subscribers MM; field description ....               | <a href="#">107</a>                       |
| Add New Phones .....  | <a href="#">167</a> , <a href="#">168</a>   | Adding telecommuter .....                                    | <a href="#">189</a>                       |
| add SNMP Access profile .....   | <a href="#">117</a>   | Adding telephones to Remote Office .....                     | <a href="#">197</a>                       |
| Add Station Template .....  | <a href="#">59</a> , <a href="#">1070</a>   | adding templates; subscriber                                 |   |
| Add Trusted Certificate page .....  | <a href="#">44</a>  | adding subscriber templates                                  |   |
| Add/Remove Agent Skills .....   | <a href="#">479</a>   | new subscriber templates .....                               | <a href="#">1065</a>                      |
| Adding a Communication Manager access profile ....                          | <a href="#">122</a>   | adding trusted certificates .....                            | <a href="#">39</a>                        |
| adding a contact address of a private contact .....                         | <a href="#">1607</a>  | AddingIPTelephone .....                                      | <a href="#">190</a>                       |
| adding a contact address of a public contact .....                          | <a href="#">1659</a>  | Address Digits Include End-of-Digits Signal .....            | <a href="#">797</a>                       |
| adding a contact in a contact list .....                                    | <a href="#">1595</a>  | Adjunct CTI Link .....                                       | <a href="#">653</a>                       |
| adding a local WebLM server .....   | <a href="#">1138</a>  | Adjunct Supervision .....                                    | <a href="#">878</a>                       |
| adding a mailing address .....  | <a href="#">1400</a>  | Adjunct Switch Applications Interface .....                  | <a href="#">395</a>                       |
| adding a messaging profile .....  | <a href="#">1565</a>  | Administer location per station .....                        | <a href="#">202</a> , <a href="#">203</a> |
| Adding a new area code or prefix .....                                      | <a href="#">331</a>   |  |   |
| adding a postal address of a private contact .....                          | <a href="#">1605</a>  |  |   |

|   |   |   |   |
|---|---|---|---|
| preparing administration steps .....                  | <a href="#">203</a>   | Alarm List page .....                               | <a href="#">1096</a>  |
| prerequisites .....                                   | <a href="#">203</a>   | Alarm Management .....                              | <a href="#">1383</a>  |
| setting up location number on Station screen .....    | <a href="#">203</a>   | Alarm Threshold .....                               | <a href="#">434</a>   |
| Administer secondary ip server interface board .....  | <a href="#">711</a>   | Alarm Type .....                                    | <a href="#">434</a>   |
| Administer Timers .....                               | <a href="#">733</a> , <a href="#">993</a>   | Alarm When PRI Endpoint Detached .....              | <a href="#">551</a>   |
| Administered Connection .....                         | <a href="#">432</a>   | Alarming .....                                      | <a href="#">1095</a>  |
| Administered Connection;                              |   | alarms  |   |
| Connection Number                                     |   | hyperactive registration .....                      | <a href="#">705</a>   |
| Destination   |   | alarms and detection .....                          | <a href="#">705</a>   |
| Data Line Circuit Pack                                |   | Alert Pager .....                                   | <a href="#">511</a>   |
| Authorized Time of Day                                |   | ALERT PAGER .....                                   | <a href="#">511</a>   |
| Miscellaneous Parameters                              |   | ALERT STATION .....                                 | <a href="#">511</a>   |
| Alarm Types   |   | Alerting (sec) .....                                | <a href="#">502</a>   |
| Auto Restoration Priority ...                         |   | Alerting Tone for Outgoing Trunk Calls .....        | <a href="#">340</a>   |
| <a href="#">395</a>                                   |   | setting the outgoing trunk alerting timer .....     | <a href="#">340</a>   |
| Administered Members (min/max) .....                  | <a href="#">667</a> , <a href="#">758</a> , <a href="#">1039</a>  | setting the trunk alerting tone interval .....      | <a href="#">340</a>   |
| administering   |   | Alias Set Type .....                                | <a href="#">443</a>   |
| initial setup of the Session Manager .....            | <a href="#">1229</a>  | Alias Station .....                                 | <a href="#">442</a>   |
| Administering .....                                   | <a href="#">140</a> , <a href="#">256</a>   | all .....   | <a href="#">91</a>  |
| Unicode Display .....                                 | <a href="#">256</a>   | all announcements .....                             | <a href="#">89</a>  |
| Administering Ad-hoc Video Conferencing .....         | <a href="#">374</a>   | Allocation Plan Number .....                        | <a href="#">756</a>   |
| Administering Call Type Digit Analysis .....          | <a href="#">327</a>   | Allocations by Feature Page .....                   | <a href="#">1155</a>  |
| Administering Circuit Packn .....                     | <a href="#">349</a>   | Allocations by Local WebLM page .....               | <a href="#">1156</a>  |
| Administering Dial Plan Transparency .....            | <a href="#">151</a>   | Allow ANI Restriction on AAR/ARS .....              | <a href="#">591</a>   |
| Administering Features .....                          | <a href="#">355</a>   | Allow ATMS Busyout, Error Logging and Alarming .... | <a href="#">1036</a>  |
| Administering MASI .....                              | <a href="#">348</a> , <a href="#">349</a> , <a href="#">351–356</a> , <a href="#">362</a> , <a href="#">365</a> | Allow Conference via Flash .....                    | <a href="#">606</a>   |
| Administering MASI Trunk Groups .....                 | <a href="#">352</a>   | Allow Direct-IP Multimedia .....                    | <a href="#">679</a>   |
| Administering Road Warrior .....                      | <a href="#">188</a>   | Allow H.248 Gateways .....                          | <a href="#">682</a>   |
| Administering the Avaya Video Telephony Solution .... | <a href="#">365</a>   | Allow H.323 Endpoints .....                         | <a href="#">682</a>   |
| Administering the ESM T.120 Server .....              | <a href="#">387</a>   | Allow Ringer-off with Auto-Answer .....             | <a href="#">619</a>   |
| Administering the Signaling Group .....               | <a href="#">349</a>   | Allow SIP URI Conversion .....                      | <a href="#">696</a>   |
| Administering User Profiles and Logins .....          | <a href="#">140</a>   | Allow Two Observers in Same Call .....              | <a href="#">613</a>   |
| Administrable Timers .....                            | <a href="#">752</a> , <a href="#">1024</a>  | Allow VDN Override .....                            | <a href="#">1048</a>  |
| Administration .....                                  | <a href="#">348</a>   | Alpha-name .....                                    | <a href="#">443</a>   |
| advanced call coverage                                |   | Alphanumeric Dialing Table .....                    | <a href="#">443</a>   |
| calls redirected to external numbers .....            | <a href="#">267</a>   | Alternate FRL Station .....                         | <a href="#">498</a>   |
| calls redirected to off-site location .....           | <a href="#">267</a>   | Alternate Route Timer .....                         | <a href="#">854</a>   |
| coverage answer groups .....                          | <a href="#">270</a>   | Always Use .....                                    | <a href="#">68</a> , <a href="#">452</a> , <a href="#">879</a> , <a href="#">1079</a> |
| time-of-day coverage .....                            | <a href="#">269</a>   | Always Use re-INVITE for Display Updates .....      | <a href="#">1042</a>  |
| advanced search .....                                 | <a href="#">57</a> , <a href="#">127</a>  | AMD Treatment .....                                 | <a href="#">875</a>   |
| searching endpoints .....                             | <a href="#">57</a>  | Analog Busy Auto Callback .....                     | <a href="#">598</a>   |
| AE Services Server .....                              | <a href="#">719</a>   | Analog Digital .....                                | <a href="#">789</a>   |
| After Call Work Access Code .....                     | <a href="#">569</a>   | Analog Gain .....                                   | <a href="#">978</a>   |
| AGENT AND CALL SELECTION .....                        | <a href="#">615</a>   | Analog Line Transmission .....                      | <a href="#">773</a>   |
| Agent Login ID .....                                  | <a href="#">435</a>   | Analog Loss Group .....                             | <a href="#">820</a> , <a href="#">993</a>   |
| Agent Login ID page 1 .....                           | <a href="#">435</a>   | Analog Ringing Cadence .....                        | <a href="#">773</a>   |
| Agent Login ID page 2 .....                           | <a href="#">440</a>   | Analog Trunk Incoming Call ID .....                 | <a href="#">942</a>   |
| Agent Management page .....                           | <a href="#">1381</a>  | ANI Available .....                                 | <a href="#">799</a>   |
| Agent States .....                                    | <a href="#">953</a>   | ANI Calling Party Information                       |   |
| AGL .....   | <a href="#">697</a>   | Displaying .....                                    | <a href="#">254</a>   |

|   |   |  |   |
|---|---|--|---|
| ANI Not Available .....                             | <a href="#">799</a>   | As-needed Inactivity Time-out (min) .....  | <a href="#">872</a> , <a href="#">873</a>   |
| ANI Prefix .....                                    | <a href="#">790</a>   | ASAI .....                                 | <a href="#">634</a> , <a href="#">754</a>   |
| ANI Req'd   |   | ASAI Call Classification .....             | <a href="#">616</a>                         |
| AAR and ARS Digit Analysis Table .....              | <a href="#">418</a>   | ASAI Link Core Capabilities .....          | <a href="#">943</a>                         |
| AAR and ARS Digit Conversion Table .....            | <a href="#">421</a>   | ASAI Link Plus Capabilities .....          | <a href="#">943</a>                         |
| ANI Source for Forwarded & Covered Calls .....      | <a href="#">797</a>   | ASAI Routing .....                         | <a href="#">466</a>                         |
| ANI/II-Digits .....                                 | <a href="#">466</a>   | ASAI Uses Station Lock .....               | <a href="#">485</a>                         |
| Annc Name .....                                     | <a href="#">444</a>   | ASCII mode .....                           | <a href="#">638</a>                         |
| Annc Type .....                                     | <a href="#">444</a>   | ASG .....                                  | <a href="#">138</a>                         |
| announcement .....                                  | <a href="#">87</a>  | assign applications .....                  | <a href="#">34</a>                          |
| Announcement .....                                  | <a href="#">961</a>   | assign groups .....                        | <a href="#">1650</a>                        |
| Announcement Access Code .....                      | <a href="#">559</a>   | Assign Groups .....                        | <a href="#">1651</a>                        |
| Announcement Extension .....                        | <a href="#">850</a>   | Assign Role page .....                     | <a href="#">1649</a>                        |
| Announcement Ports .....                            | <a href="#">639</a>   | Assign Roles page .....                    | <a href="#">1648</a>                        |
| Announcement Server IP Address .....                | <a href="#">704</a>   | Assign Users .....                         | <a href="#">1220</a> , <a href="#">1653</a> |
| Announcement Storage Path Name .....                | <a href="#">704</a>   | Assigned Member — Ext .....                | <a href="#">879</a>                         |
| Announcement Type .....                             | <a href="#">640</a>   | Assigned Member — Name .....               | <a href="#">879</a>                         |
| announcements .....                                 | <a href="#">87–93</a>   | Assigned Members .....                     | <a href="#">674</a>                         |
| Announcements .....                                 | <a href="#">598</a> , <a href="#">808</a>                       | Assigned VDN .....                         | <a href="#">556</a>                         |
| announcements field description .....               | <a href="#">93</a>  | assigning an appender to a logger .....    | <a href="#">1110</a> , <a href="#">1300</a> |
| announcements list .....                            | <a href="#">85</a>  | assigning applications .....               | <a href="#">24</a>                          |
| Announcements/Audio Sources .....                   | <a href="#">444</a>   | assigning groups                           |   |
| Ans Delay .....                                     | <a href="#">1040</a>  | multiple users .....                       | <a href="#">1397</a>                        |
| Answer Back Access Code .....                       | <a href="#">559</a>   | single user                                |   |
| answer groups .....                                 | <a href="#">507</a>   | multiple users .....                       | <a href="#">1396</a>                        |
| Answer Send (msec) .....                            | <a href="#">1024</a>  | Assigning Multimedia Buttons .....         | <a href="#">385</a>                         |
| Answer Supervision by Call Classifier .....         | <a href="#">942</a>   | assigning permission to a role .....       | <a href="#">1207</a>                        |
| Answer Supervision Timeout .....                    | <a href="#">733</a> , <a href="#">821</a> , <a href="#">993</a> | assigning resources .....                  | <a href="#">1168</a> , <a href="#">1186</a> |
| Answer Supervision Timeout (sec) .....              | <a href="#">785</a>   | assigning roles to                         |   |
| Answer Text .....                                   | <a href="#">522</a>   | multiple users .....                       | <a href="#">1395</a>                        |
| Answering multimedia calls .....                    | <a href="#">408</a>   | assigning roles to multiple users          |   |
| APLT .....  | <a href="#">479</a>   | single user .....                          | <a href="#">1394</a>                        |
| Appl .....  | <a href="#">834</a> , <a href="#">923</a>                       | assigning users to roles .....             | <a href="#">1200</a> , <a href="#">1399</a> |
| Appl. ....  | <a href="#">872</a> , <a href="#">873</a>                       | Assignment .....                           | <a href="#">1046</a> , <a href="#">1056</a> |
| application .....                                   | <a href="#">916</a>   | Assist Access Code .....                   | <a href="#">569</a>                         |
| Application   |   | Assistance Call .....                      | <a href="#">504</a>                         |
| Stations With Off-PBX Telephone Integration .....   | <a href="#">916</a>   | Associated Signaling .....                 | <a href="#">854</a>                         |
| Application Management page .....                   | <a href="#">27</a>  | Asynch. Transfer Mode (ATM) PNC .....      | <a href="#">943</a>                         |
| Apply Intercept Locally .....                       | <a href="#">609</a>   | Asynch. Transfer Mode (ATM) Trunking ..... | <a href="#">943</a>                         |
| Apply Local Ringback .....                          | <a href="#">738</a>   | At End of Member List .....                | <a href="#">667</a>                         |
| Apply MCT Warning Tone .....                        | <a href="#">589</a>   | AT&T Adapter (AttAdapter) .....            | <a href="#">1251</a>                        |
| Apply Ready Indication Tone To Which Parties In The |   | ATM WAN Spare Processor .....              | <a href="#">944</a>                         |
| Call .....  | <a href="#">599</a>   | ATMS .....                                 | <a href="#">944</a>                         |
| ARS .....   | <a href="#">560</a> , <a href="#">942</a>                       | ATMS Thresholds .....                      | <a href="#">1035</a>                        |
| ARS Analysis .....                                  | <a href="#">322</a>   | Att. Call Waiting Indication .....         | <a href="#">879</a>                         |
| ARS Analysis Information .....                      | <a href="#">321</a>   | Attach Appender page .....                 | <a href="#">1114</a> , <a href="#">1309</a> |
| ARS FAC .....                                       | <a href="#">320</a> , <a href="#">771</a>                       | Attach Contacts page .....                 | <a href="#">1598</a>                        |
| ARS Prefix 1 Required for 10-Digit NANP Calls ..... | <a href="#">771</a>   | Attd FAC .....                             | <a href="#">771</a>                         |
| ARS Toll Table .....                                | <a href="#">448</a>   | Attendant Access Code .....                | <a href="#">559</a>                         |
| ARS/AAR Dialing without FAC .....                   | <a href="#">943</a>   | Attendant console                          |   |
| ARS/AAR Partitioning .....                          | <a href="#">943</a>   | Adding .....                               | <a href="#">244</a>                         |

|  |  |   |   |
|--|--|---|---|
| Feature buttons .....                                      | <a href="#">245</a>  | Authorization Code .....                                  | <a href="#">460</a>   |
| providing backup .....                                     | <a href="#">253</a>  | Authorization Code — PIN Checking for Private Calls ...   | <a href="#">460</a>   |
| Attendant Console ....                                     | <a href="#">241–243</a> , <a href="#">252</a> , <a href="#">448</a> , <a href="#">452</a> , <a href="#">454</a> , <a href="#">456</a> ,<br><a href="#">459</a> | Authorization Code Cancellation Symbol .....              | <a href="#">586</a>   |
| 302A/B Console .....                                       | <a href="#">241–243</a>  | Authorization Code Length .....                           | <a href="#">586</a>   |
| display module button assignment .....                     | <a href="#">459</a>  | AUTHORIZATION CODE PARAMETERS .....                       | <a href="#">586</a>   |
| feature button assignment .....                            | <a href="#">456</a>  | Authorization Code Required .....                         | <a href="#">838</a>   |
| removing .....   | <a href="#">252</a>  | Authorization Codes .....                                 | <a href="#">944</a>   |
| Softconsole IP Attendant .....                             | <a href="#">452</a>  | Authorization Codes Enabled .....                         | <a href="#">587</a>   |
| VIS feature options .....                                  | <a href="#">454</a>  | Auto .....  | <a href="#">713</a>   |
| attendant console group parameters .....                   | <a href="#">498</a>  | Auto Abbreviated/Delayed Transition Interval (rings) .... | <a href="#">575</a>   |
| Attendant Console X .....                                  | <a href="#">448</a>  | Auto Alternate Routing .....                              | <a href="#">559</a>   |
| Attendant Consoles .....                                   | <a href="#">239</a>  | Auto Answer .....   | <a href="#">61</a> , <a href="#">436</a> , <a href="#">448</a> , <a href="#">489</a> , <a href="#">880</a> , <a href="#">1072</a> |
| Attendant Diversion Timing (sec) .....                     | <a href="#">808</a>  | Auto Guard .....  | <a href="#">993</a>   |
| Attendant Group .....                                      | <a href="#">962</a>  | Auto Hold .....   | <a href="#">591</a>   |
| Attendant Group Name .....                                 | <a href="#">498</a>  | Auto Inspect on Send All Calls .....                      | <a href="#">590</a>   |
| Attendant Lockout .....                                    | <a href="#">498</a>  | Auto Reserve Agents .....                                 | <a href="#">615</a>   |
| Attendant Originated Calls .....                           | <a href="#">595</a> , <a href="#">964</a>  | Auto Restoration .....                                    | <a href="#">435</a>   |
| Attendant Time Out Flag .....                              | <a href="#">586</a>  | Auto Return .....   | <a href="#">960</a>   |
| Attendant Tone .....                                       | <a href="#">591</a>  | Auto Route Selection (ARS) Access Code 1 .....            | <a href="#">560</a>   |
| Attendant Vectoring .....                                  | <a href="#">466</a> , <a href="#">944</a> , <a href="#">1049</a>   | Auto Select Any Idle Appearance .....                     | <a href="#">68</a> , <a href="#">881</a> , <a href="#">1079</a>   |
| Attendant Vectoring VDN .....                              | <a href="#">498</a> , <a href="#">962</a>  | Auto Start .....  | <a href="#">454</a> , <a href="#">591</a>   |
| attribute details defined in the Delete user XSD ....      | <a href="#">1513</a>   | Auto-A/D .....  | <a href="#">880</a>   |
| attribute details defined in the Endpoint profile XSD .... | <a href="#">1514</a>   | Auto-answer IP Failure AUX Reason Code .....              | <a href="#">622</a>   |
| attribute details defined in the Import User XSD ....      | <a href="#">1503</a>   | Auto-In Access Code .....                                 | <a href="#">569</a>   |
| attribute details defined in the Messaging communication   |  | auto-refresh log list page .....                          | <a href="#">1107</a>  |
| profile XSD .....  | <a href="#">1541</a>   | Auto?   |   |
| attribute details defined in the Session Manager           |  | IP Interfaces .....                                       | <a href="#">686</a>   |
| communication profile XSD .....                            | <a href="#">1550</a>   | Automatic Callback .....                                  | <a href="#">491</a>   |
| Audible Message Waiting .....                              | <a href="#">68</a> , <a href="#">880</a> , <a href="#">944</a> , <a href="#">1079</a>  | Automatic Callback — No Answer Timeout Interval           |   |
| Audible Notification .....                                 | <a href="#">631</a>  | (rings) .....   | <a href="#">575</a>   |
| Audio 802.1p Priority .....                                | <a href="#">693</a>  | Automatic Callback Activation .....                       | <a href="#">560</a>   |
| Audio Codec .....  | <a href="#">676</a>  | Automatic callback if an extension is busy .....          | <a href="#">162</a>   |
| Audio Group .....  | <a href="#">459</a>  | Automatic Charge Display .....                            | <a href="#">479</a>   |
| audio groups .....   | <a href="#">96–98</a>  | Automatic Circuit Assurance .....                         | <a href="#">575</a>   |
| audio groups field description .....                       | <a href="#">99</a>   | Automatic Customer Telephone Rearrangement ...            | <a href="#">177</a>   |
| Audio PHB Value .....                                      | <a href="#">692</a>  | Automatic Exclusion .....                                 | <a href="#">491</a>   |
| Audio Resource Reservation Parameters .....                | <a href="#">693</a>  | Automatic Exclusion by COS .....                          | <a href="#">625</a>   |
| Audio Source Location .....                                | <a href="#">459</a>  | Automatic Exclusion Coverage/Hold .....                   | <a href="#">625</a>   |
| Audio WAN-BW limits .....                                  | <a href="#">697</a>  | Automatic Exclusion with Whisper Page .....               | <a href="#">625</a>   |
| Audix .....  | <a href="#">436</a>  | Automatic hold .....                                      | <a href="#">162</a>   |
| Audix Name .....   | <a href="#">67</a> , <a href="#">880</a> , <a href="#">1078</a>  | Automatic Moves .....                                     | <a href="#">881</a>   |
| AUDIX Name .....   | <a href="#">662</a> , <a href="#">968</a> , <a href="#">1051</a>   | Automatic Selection of DID Numbers .....                  | <a href="#">640</a> , <a href="#">881</a>   |
| Audix Name for Messaging .....                             | <a href="#">436</a>  | Automatic Wakeup .....                                    | <a href="#">765</a>   |
| Audix Names .....  | <a href="#">459</a>  | Automatic Wakeup Call Access Code .....                   | <a href="#">571</a>   |
| Audix-MSA Node Names .....                                 | <a href="#">459</a>  | AutoRefresh Alarm List page .....                         | <a href="#">1095</a>  |
| Auth Code .....  | <a href="#">721</a> , <a href="#">978</a>  | Aux Work .....  | <a href="#">837</a>   |
| Authoritative Domain .....                                 | <a href="#">689</a>  | Aux Work Access Code .....                                | <a href="#">569</a>   |
| Authorization .....  | <a href="#">394</a>  | Aux Work Reason Code Type .....                           | <a href="#">436</a> , <a href="#">621</a>   |
| Authorization and Barrier Codes .....                      | <a href="#">395</a>  | Auxiliary Board for Announcement .....                    | <a href="#">641</a>   |

|   |   |   |  |
|---|---|---|--|
| Available Agent Adjustments for BSR .....       | <a href="#">610</a>   | Block Enhanced Conference/Transfer Display .....          | <a href="#">486</a>  |
| Avaya S8XXX Server .....                        | <a href="#">134</a> , <a href="#">135</a>                       | Block Progress Indicator .....                            | <a href="#">551</a>  |
| Avaya S8XXX servers directly .....              | <a href="#">134</a> , <a href="#">135</a>                       | Block Transfer Displays .....                             | <a href="#">486</a>  |
| Avaya Site Administration .....                 | <a href="#">135</a> – <a href="#">137</a>                       | Blocked Precedence Level .....                            | <a href="#">808</a>  |
| <hr/>   |   |   |  |
| <b>B</b>  |   |   |  |
| backing up all announcements .....              | <a href="#">89</a>  | Board .....   | <a href="#">709</a>  |
| backing up audio groups .....                   | <a href="#">98</a> , <a href="#">99</a>                         | Board Location .....                                      | <a href="#">671</a>  |
| backup .....                                    | <a href="#">89</a>  | Brazil Collect Call Blocking .....                        | <a href="#">486</a>  |
| Backup Alerting .....                           | <a href="#">498</a>   | Break (msec) .....  | <a href="#">1033</a>   |
| backup and restore .....                        | <a href="#">1297</a>  | BRI LINK/MAINTENANCE PARAMETERS .....                     | <a href="#">524</a>  |
| Backup And Restore page .....                   | <a href="#">1303</a>  | Bridge ID .....   | <a href="#">1057</a>   |
| backup of announcements .....                   | <a href="#">89</a>  | Bridged Appearance Origination Restriction .....          | <a href="#">73</a> , <a href="#">882</a> ,<br><a href="#">1084</a> |
| Backup page .....                               | <a href="#">1303</a>  | Bridged Appearances .....                                 | <a href="#">395</a>  |
| Backup Servers in Priority Order .....          | <a href="#">696</a>   | Bridged Call Alerting .....                               | <a href="#">68</a> , <a href="#">882</a> , <a href="#">1080</a>    |
| Backward Cycle Timer (sec) .....                | <a href="#">790</a>   | Bridged Call Appearances .....                            | <a href="#">228</a>  |
| Band .....                                      | <a href="#">843</a>   | Bridged Calls .....                                       | <a href="#">917</a>  |
| Barge-In Tone .....                             | <a href="#">494</a>   | Bridged Idle Line Preference .....                        | <a href="#">69</a> , <a href="#">882</a> , <a href="#">1080</a>    |
| Barrier Code .....                              | <a href="#">838</a>   | Bridging Tone .....                                       | <a href="#">592</a>  |
| Barrier Code Length .....                       | <a href="#">839</a>   | broadcast .....   | <a href="#">91</a>   |
| Base Parameter Set .....                        | <a href="#">965</a>   | broadcasting an announcement .....                        | <a href="#">91</a>   |
| Base Tone Generator Set .....                   | <a href="#">975</a>   | broadcasting announcements .....                          | <a href="#">91</a>   |
| Basic   |   | BSR .....   | <a href="#">466</a>  |
| Call Vector .....                               | <a href="#">466</a>   | BSR Application .....                                     | <a href="#">1051</a>   |
| basic call coverage                             |   | BSR Available Agent Strategy .....                        | <a href="#">1052</a>   |
| creating coverage paths .....                   | <a href="#">264</a>   | BSR Local Treatment .....                                 | <a href="#">1052</a>   |
| system-side call coverage .....                 | <a href="#">264</a>   | BSR Reply-best DISC Cause Value .....                     | <a href="#">739</a>  |
| Basic Call Setup .....                          | <a href="#">954</a>   | BSR Tie Strategy .....                                    | <a href="#">610</a> , <a href="#">1053</a>                         |
| Basic Mode Activation .....                     | <a href="#">571</a>   | Building  |  |
| Basic Mode Operation .....                      | <a href="#">377</a>   | Station .....   | <a href="#">73</a> , <a href="#">883</a> , <a href="#">1084</a>    |
| Basic Supplementary Services .....              | <a href="#">954</a>   | bulk add endpoint; field description                      |  |
| basic vectoring .....                           | <a href="#">952</a>   | bulk add endpoints  |  |
| Bcc   |   | add endpoints .....                                       | <a href="#">78</a>   |
| Attendant Console .....                         | <a href="#">454</a>   | bulk edit endpoints; field description                    |  |
| BCC .....                                       | <a href="#">516</a> , <a href="#">881</a> , <a href="#">978</a> | editing endpoints; field description .....                | <a href="#">79</a>   |
| BCC Value .....                                 | <a href="#">843</a>   | bulk exporting global settings .....                      | <a href="#">1416</a>   |
| BCIE .....                                      | <a href="#">844</a>   | bulk exporting roles .....                                | <a href="#">1202</a>   |
| BCMS (Basic) .....                              | <a href="#">950</a>   | bulk exporting users .....                                | <a href="#">1407</a>   |
| BCMS/VuStats Abandon Call Timer (seconds) ..... | <a href="#">618</a>   | bulk exporting users partially .....                      | <a href="#">1409</a>   |
| BCMS/VuStats LoginIDs .....                     | <a href="#">618</a>   | Bulk Import example for Adaptations .....                 | <a href="#">1254</a>   |
| BCMS/VuStats Measurement Interval .....         | <a href="#">618</a>   | Bulk Import example for Dial Patterns .....               | <a href="#">1287</a>   |
| BCMS/VuStats Service Level .....                | <a href="#">950</a>   | Bulk Import example for Domains .....                     | <a href="#">1236</a>   |
| Bearer .....                                    | <a href="#">882</a>   | Bulk Import example for Entity Links .....                | <a href="#">1269</a>   |
| Bearer Capability Class .....                   | <a href="#">516</a>   | Bulk Import example for Locations .....                   | <a href="#">1241</a>   |
| Bearer Capability Information Element .....     | <a href="#">844</a>   | Bulk Import example for Regular Expressions .....         | <a href="#">1293</a>   |
| Begin Time .....                                | <a href="#">972</a>   | Bulk Import example for Routing Policies .....            | <a href="#">1280</a>   |
| Beginning Station .....                         | <a href="#">632</a>   | Bulk Import example for SIP Entities .....                | <a href="#">1263</a>   |
| Best Service Routing .....                      | <a href="#">461</a> , <a href="#">952</a>                       | Bulk Import example for Time Ranges .....                 | <a href="#">1273</a>   |
| Bit Rate .....                                  | <a href="#">538</a> , <a href="#">994</a>                       | bulk importing and exporting .....                        | <a href="#">1404</a>   |
| Trunk Group .....                               | <a href="#">994</a>   | bulk importing global user settings .....                 | <a href="#">1415</a>   |
| Block CMS Move Agent Events .....               | <a href="#">515</a>   | bulk importing roles .....                                | <a href="#">1201</a>   |
|   |   | bulk importing user attributes partially for a user ..... | <a href="#">1408</a>   |

|  |   |  |   |
|--|---|--|---|
| bulk importing users .....   | <a href="#">1405</a>                      | Call Forwarding Enhanced .....                             | <a href="#">493</a>   |
| Bulletin Board .....   | <a href="#">462</a>                       | Call Forwarding Enhanced Activation/Deactivation ....      | <a href="#">560</a>   |
| Bulletin Board text lines .....  | <a href="#">463</a>                       | Call Forwarding Enhanced Status .....                      | <a href="#">560</a>   |
| Business Advocate .....  | <a href="#">951</a>                       | Call Handling Preference .....                             | <a href="#">440</a>   |
| Busy Auto Callback without Flash .....                                   | <a href="#">883</a>                       | call identifiers .....                                     | <a href="#">767</a>   |
| Busy Indicator for Call Parked on Analog Station Without Hardware? ..... | <a href="#">502</a>                       | Call Limit .....   | <a href="#">918</a>   |
| Busy Indicator lamp .....  | <a href="#">502</a>                       | CALL MANAGEMENT SYSTEMS .....                              | <a href="#">617</a>   |
| Busy Out .....   | <a href="#">521</a>                       | Call Park .....  | <a href="#">399</a>   |
| Busy Threshold .....   | <a href="#">722</a> , <a href="#">979</a> | Call Park Access Code .....                                | <a href="#">560</a>   |
| Busy Tone Disconnect .....   | <a href="#">1025</a>                      | Call Park Timeout .....                                    | <a href="#">575</a> , <a href="#">585</a>   |
| Busy Tone Disconnect for Analog Loop-start Trunks ....                   | <a href="#">938</a>                       | Call Park Timeout Interval (minutes) .....                 | <a href="#">576</a>   |
| Busy, Not Equipped .....   | <a href="#">808</a>                       | Call Pickup .....  | <a href="#">287</a> , <a href="#">289–295</a> , <a href="#">301</a> , <a href="#">631</a> |
| Button Assignment .....  | <a href="#">76</a> , <a href="#">1087</a> | Assigning button   |   |
| BUTTON ASSIGNMENTS .....   | <a href="#">883</a>                       | user telephone .....                                       | <a href="#">291</a>   |
| button label   |   | assigning feature access code .....                        | <a href="#">291</a>   |
| customization .....  | <a href="#">463</a>                       | deleting pickup groups .....                               | <a href="#">292</a> , <a href="#">293</a>   |
| button labels .....  | <a href="#">766</a>                       | removing user .....  | <a href="#">292</a>   |
| Button Type Customization Restriction .....                              | <a href="#">463</a>                       | adding pickup groups .....                                 | <a href="#">290</a>   |
| Buttons  |   | alerting .....   | <a href="#">287</a>   |
| Telephone feature buttons table .....                                    | <a href="#">206</a>                       | changing call pickup button .....                          | <a href="#">294</a>   |
| Bypass If IP Threshold Exceeded .....                                    | <a href="#">855</a>                       | enabling alerting .....                                    | <a href="#">290</a>   |
|  |   | flexible to simple .....                                   | <a href="#">301</a>   |
|  |   | removing call pickup button .....                          | <a href="#">295</a>   |
|  |   | setting .....  | <a href="#">289</a>   |
|  |   | Call Pickup Access Code .....                              | <a href="#">560</a>   |
|  |   | Call Pickup Alerting .....                                 | <a href="#">583</a> , <a href="#">631</a>   |
|  |   | Call Pickup on Intercom Calls .....                        | <a href="#">583</a> , <a href="#">631</a>   |
|  |   | Call Processing .....                                      | <a href="#">178</a>   |
|  |   | CALL PROCESSING OVERLOAD MITIGATION .....                  | <a href="#">583</a>   |
|  |   | Call Rate .....  | <a href="#">1057</a>  |
|  |   | Call Redirection .....                                     | <a href="#">395</a>   |
|  |   | Call routing modification .....                            | <a href="#">331</a>   |
|  |   | Call Selection Measurement .....                           | <a href="#">615</a>   |
|  |   | Call Still Held .....                                      | <a href="#">821</a> , <a href="#">994</a>   |
|  |   | Call Type .....  | <a href="#">530</a> , <a href="#">919</a>   |
|  |   | Survivable ARS Analysis Table .....                        | <a href="#">919</a>   |
|  |   | Call Type (AAR only) .....                                 | <a href="#">418</a>   |
|  |   | Call Type (ARS only) .....                                 | <a href="#">419</a>   |
|  |   | Call Type Digit Analysis .....                             | <a href="#">327</a>   |
|  |   | Call Type Digit Analysis Table .....                       | <a href="#">463</a>   |
|  |   | Call Vector .....  | <a href="#">464</a>   |
|  |   | Call Waiting Indication .....                              | <a href="#">885</a>   |
|  |   | Call Work Codes .....                                      | <a href="#">951</a>   |
|  |   | Call-Type Ordering Within Priority Levels? .....           | <a href="#">504</a>   |
|  |   | Called Len .....   | <a href="#">669</a>   |
|  |   | Called Number .....  | <a href="#">669</a>   |
|  |   | Called Party Restriction .....                             | <a href="#">480</a>   |
|  |   | Caller ID calls .....                                      | <a href="#">576</a>   |
|  |   | caller ID format for Extension to Cellular telephones .... | <a href="#">495</a>   |

## C

|   |   |
|---|---|
| CA-TSC Request .....                            | <a href="#">844</a>   |
| Cable .....                                     | <a href="#">73</a> , <a href="#">883</a> , <a href="#">1084</a> |
| Cadence Classification After Answer .....       | <a href="#">958</a>   |
| Cadence Step .....                              | <a href="#">958</a> , <a href="#">975</a>                       |
| call appearance buttons .....                   | <a href="#">766</a>   |
| Call Appearance Display Format .....            | <a href="#">67</a> , <a href="#">883</a> , <a href="#">1078</a> |
| Call Appearance Selection for Origination ..... | <a href="#">494</a>   |
| Call Category for Vector ii-digits .....        | <a href="#">797</a>   |
| Call Center Release .....                       | <a href="#">951</a>   |
| Call Control 802.1p Priority .....              | <a href="#">693</a>   |
| Call Control PHB Value .....                    | <a href="#">692</a>   |
| Call Counts .....                               | <a href="#">828</a>   |
| Call Coverage/Call Forwarding .....             | <a href="#">928</a>   |
| Call Detail Recording .....                     | <a href="#">396</a>   |
| Call Forward Override .....                     | <a href="#">932</a>   |
| call forwarding                                 |   |
| change coverage remotely .....                  | <a href="#">273</a>   |
| changing forwarding destination remotely .....  | <a href="#">272</a>   |
| determining extensions .....                    | <a href="#">271</a>   |
| enhanced call forwarding .....                  | <a href="#">274</a>   |
| forwarding destination .....                    | <a href="#">272</a>   |
| setting call forwarding .....                   | <a href="#">271</a>   |
| Call Forwarding .....                           | <a href="#">75</a> , <a href="#">1086</a>                       |
| Call Forwarding Activation Busy/DA .....        | <a href="#">560</a>   |
| Call Forwarding All Calls .....                 | <a href="#">491</a>   |
| Call Forwarding Busy/DA .....                   | <a href="#">491</a>   |

|  |   |  |  |
|--|---|--|--|
| Caller ID Message Waiting Indication .....             | <a href="#">884</a>                       | CDR FEAC .....   | <a href="#">973</a>  |
| Caller ID on Call Waiting Delay Timer (msec) .....     | <a href="#">606</a>                       | CDR for Calls to EC500 Destination .....               | <a href="#">495</a>  |
| Caller ID on Call Waiting Parameters .....             | <a href="#">606</a>                       | CDR for Origination .....                              | <a href="#">496</a>  |
| Caller's Emergency Service Identification (CESID) .... |   | CDR Privacy .....                                      | <a href="#">69</a> , <a href="#">885</a> , <a href="#">1080</a>  |
| <a href="#">469</a>                                    |   | CDR Reports .....                                      | <a href="#">722</a> , <a href="#">817</a> , <a href="#">979</a>  |
| Calling Number Style .....                             | <a href="#">495</a>                       | CDR system parameters .....                            | <a href="#">469</a>  |
| Calling Number Verification .....                      | <a href="#">495</a>                       | Cell Phone Number .....                                | <a href="#">885</a>  |
| Calling Party Number (CPN) .....                       | <a href="#">565</a>                       | Cellular Voice Mail Detection .....                    | <a href="#">496</a>  |
| Calling Party Number Conversion for Tandem Calls ....  |   | Centralized Attendant .....                            | <a href="#">954</a>  |
| <a href="#">719</a>                                    |   | Centralized Attendant Service (CAS) .....              | <a href="#">498</a> , <a href="#">499</a>                        |
| Calling Party Number to INTUITY AUDIX .....            | <a href="#">662</a>                       | Centralized Automatic Message Accounting (CAMA) ....   |  |
| Calling Party Restriction .....                        | <a href="#">480</a>                       | <a href="#">469</a>                                    |  |
| CALLING PERMISSION .....                               | <a href="#">490</a>                       | CESID .....  | <a href="#">469</a>  |
| Calling permissions .....                              | <a href="#">964</a>                       | CESID I Digits Sent .....                              | <a href="#">980</a>  |
| Calling Privileges Management .....                    | <a href="#">319</a>                       | CF-CB Common .....                                     | <a href="#">785</a>  |
| Callr-info Display Timer (sec) .....                   | <a href="#">619</a>                       | Chained Call Forwarding .....                          | <a href="#">624</a>  |
| Calls Allowed .....                                    | <a href="#">884</a> , <a href="#">918</a> | Chan Port .....  | <a href="#">871</a>  |
| Calls In Queue Warning .....                           | <a href="#">499</a>                       | Change all board location translations from board .... |  |
| Calls Share IP Signaling Connection .....              | <a href="#">855</a>                       | <a href="#">672</a>                                    |  |
| Calls to Hunt Group — Record .....                     | <a href="#">470</a>                       | Change Allocations page .....                          | <a href="#">1157</a>   |
| Calls Used .....                                       | <a href="#">839</a>                       | Change COR by FAC .....                                | <a href="#">944</a>  |
| Calls Warning Extension .....                          | <a href="#">646</a>                       | Change CORs .....                                      | <a href="#">163</a>  |
| Calls Warning Threshold .....                          | <a href="#">646</a>                       | Change Coverage Access Code .....                      | <a href="#">561</a>  |
| CAMA Numbering Format .....                            | <a href="#">469</a>                       | Change Day (Start) .....                               | <a href="#">527</a>  |
| Cama Outgoing Dial Guard (msec) .....                  | <a href="#">1025</a>                      | Change Day (Stop) .....                                | <a href="#">528</a>  |
| Cama Wink Start Time (msec) .....                      | <a href="#">1025</a>                      | Change Password page .....                             | <a href="#">1652</a>   |
| Can Be a Service Observer .....                        | <a href="#">481</a>                       | Change Station Extension .....                         | <a href="#">477</a>  |
| Can Be Picked Up By Directed Call Pickup .....         | <a href="#">481</a>                       | Changing a station .....                               | <a href="#">172</a>  |
| Can Be Service Observed .....                          | <a href="#">481</a>                       | changing alarm status .....                            | <a href="#">1099</a>   |
| Can Change Coverage .....                              | <a href="#">481</a>                       | changing allocations of a licensed feature .....       | <a href="#">1142</a>   |
| Can Use Directed Call Pickup .....                     | <a href="#">481</a>                       | Changing from dual-connect to single-connect IP        |  |
| canceling a global user settingsimporting job .....    | <a href="#">1420</a>                      | telephones .....                                       | <a href="#">191</a>  |
| canceling a user importing job .....                   | <a href="#">1413</a>                      | Changing Station .....                                 | <a href="#">320</a>  |
| canceling an import job .....                          | <a href="#">1205</a>                      | Channel Numbering .....                                | <a href="#">538</a>  |
| Carrier Medium .....                                   | <a href="#">722</a>                       | Character Set for QSIG Name .....                      | <a href="#">749</a>  |
| CAS .....  | <a href="#">499</a>                       | Charge Advice .....                                    | <a href="#">723</a> , <a href="#">733</a>                        |
| CAS Back-Up Extension .....                            | <a href="#">499</a>                       | Charge Conversion .....                                | <a href="#">739</a> , <a href="#">821</a> , <a href="#">1009</a> |
| CAS Branch .....                                       | <a href="#">944</a>                       | Charge Display Update Frequency (seconds) .....        | <a href="#">606</a>  |
| CAS Main .....   | <a href="#">944</a>                       | Charge Type .....                                      | <a href="#">821</a> , <a href="#">1010</a>                       |
| CAS Remote Hold/Answer Hold-Unhold Access Code ..      |   | Check-In status function .....                         | <a href="#">491</a>  |
| <a href="#">560</a>                                    |   | Check-Out status function .....                        | <a href="#">491</a>  |
| CBC Service Trunk Group Allocation Plan Assignment     |   | Checking bandwidth usage .....                         | <a href="#">374</a>  |
| Schedule .....   | <a href="#">755</a>                       | Checksum ID .....                                      | <a href="#">671</a>  |
| CBC Trunk Group Usage Allocation .....                 | <a href="#">756</a>                       | chime code extensions .....                            | <a href="#">494</a>  |
| CC .....   | <a href="#">916</a>                       | chime codes .....                                      | <a href="#">494</a>  |
| Stations With Off-PBX Telephone Integration ....       | <a href="#">916</a>                       | Choose Address page .....                              | <a href="#">1404</a> , <a href="#">1661</a>                      |
| CCSA .....   | <a href="#">479</a>                       | Choose Group page .....                                | <a href="#">1194</a>   |
| CDR .....  | <a href="#">780</a>                       | Choose Parent Group .....                              | <a href="#">1194</a>   |
| CDR Account Code .....                                 | <a href="#">561</a>                       | choosing a shared address .....                        | <a href="#">1401</a> , <a href="#">1670</a>                      |
| CDR Account Code Length .....                          | <a href="#">470</a>                       | choosing a shared address for a private contact ....   | <a href="#">1659</a>   |
| CDR Date Format .....                                  | <a href="#">470</a>                       |  |  |

|  |  |
|--|--|
| Choosing a shared address for a private contact ....<br><a href="#">1606</a> | Code-Pattern Choice Assignments ..... <a href="#">842</a>  |
| CINFO ..... <a href="#">466</a> , <a href="#">952</a>                        | Code/Sfx ..... <a href="#">682</a>   |
| Circuit Pack Assignments ..... <a href="#">788</a>                           | Codec Set ..... <a href="#">677</a> , <a href="#">690</a>  |
| Circuit Pack Location ..... <a href="#">788</a>                              | codec-set ..... <a href="#">698</a>  |
| Circuit Packs ..... <a href="#">479</a>                                      | CODES ..... <a href="#">842</a>  |
| Circuit Type   | Codeset to Send Display ..... <a href="#">734</a>  |
| Signaling Group ..... <a href="#">855</a>                                    | Codeset to Send National IEs ..... <a href="#">734</a>   |
| Cisco Adapter (CiscoAdapter) ..... <a href="#">1249</a>                      | Collect All Digits Before Seizure ..... <a href="#">790</a>  |
| class of restriction   | Collected Digits ..... <a href="#">754</a>   |
| Service Observing Permission ..... <a href="#">490</a>                       | Comm Type ..... <a href="#">980</a>  |
| calling permission ..... <a href="#">490</a>                                 | command parameters ..... <a href="#">916</a>   |
| Class of Restriction ..... <a href="#">303</a> , <a href="#">479</a>         | Common Error Conditions ..... <a href="#">362</a>  |
| assigning ..... <a href="#">303</a>  | Communication Interface Processor Channels ..... <a href="#">834</a>                                   |
| class of service ..... <a href="#">100</a> , <a href="#">110</a>             | Communication Manager Access list ..... <a href="#">121</a>  |
| messaging; class of service  | Communication Manager access profile ..... <a href="#">122</a>   |
| COS ..... <a href="#">100</a>  | Communication Manager Access profile ..... <a href="#">122</a>   |
| Class of service ..... <a href="#">490</a>                                   | Communication Manager access profile field description<br><a href="#">123</a>                          |
| Class of Service   | Communication Manager features ..... <a href="#">356</a>   |
| COS List ..... <a href="#">101</a>   | Communication Manager objects ..... <a href="#">81</a>   |
| class of service data ..... <a href="#">111</a>                              | Communication Manager objects; add   |
| class of service field description ..... <a href="#">112</a>                 | adding Communication Manager objects ..... <a href="#">82</a>  |
| class of service list ..... <a href="#">112</a>                              | Communication Manager objects; delete  |
| class of service page 2  | deleting Communication Manager objects ..... <a href="#">84</a>  |
| Ad hoc Video Conferencing ..... <a href="#">493</a>                          | Communication Manager objects; edit  |
| Call Forwarding Enhanced ..... <a href="#">493</a>                           | Communication Manager objects; edit ..... <a href="#">83</a>   |
| Masking CPN/Name Override ..... <a href="#">493</a>                          | communication profiles for a user ..... <a href="#">1564</a>   |
| Priority Ip Video ..... <a href="#">493</a>                                  | Communication Type ..... <a href="#">429</a>   |
| Class of service:page 1  | Community ..... <a href="#">921</a> , <a href="#">959</a>  |
| Automatic Callback ..... <a href="#">491</a>                                 | Community Size ..... <a href="#">921</a>   |
| Automatic Exclusion ..... <a href="#">491</a>                                | Community String ..... <a href="#">707</a>   |
| Call Forwarding Busy/D Client Room ..... <a href="#">491</a>                 | Companding Mode ..... <a href="#">774</a>  |
| Console Permissions ..... <a href="#">491</a>                                | Completed Jobs Page ..... <a href="#">1327</a>   |
| Clear Callr-info ..... <a href="#">619</a>                                   | Computer Telephony Adjunct Links ..... <a href="#">944</a>   |
| Clear VuStats Shift Data ..... <a href="#">619</a>                           | Condition Code 'T' for Redirected Calls ..... <a href="#">470</a>                                      |
| Clear-channel ..... <a href="#">679</a>                                      | Conf/Trans On Primary Appearance ..... <a href="#">69</a> , <a href="#">886</a> , <a href="#">1080</a> |
| Client Room ..... <a href="#">491</a>  | Conference Access Code ..... <a href="#">1055</a>  |
| Client Room Coverage Path Configuration ..... <a href="#">636</a>            | Conference Controller ..... <a href="#">1055</a>   |
| Clock Time Forced Logout Reason Code ..... <a href="#">623</a>               | Conference Parties ..... <a href="#">592</a>   |
| Cluster ID ..... <a href="#">921</a>   | Conference Tone ..... <a href="#">592</a>  |
| CM access ..... <a href="#">121</a>  | Conference Type ..... <a href="#">1055</a>   |
| CM access field description ..... <a href="#">123</a>                        | Conference/Transfer ..... <a href="#">596</a>  |
| CMS (appl mis) ..... <a href="#">617</a>                                     | Conferencing ..... <a href="#">395</a>   |
| Cntry/Peer Protocol ..... <a href="#">759</a> , <a href="#">762</a>          | Configuration ..... <a href="#">521</a>  |
| CO Type ..... <a href="#">981</a>  | configuration set ..... <a href="#">916</a>  |
| Code ..... <a href="#">758</a> , <a href="#">1040</a>                        | Configuration Set ..... <a href="#">494</a> , <a href="#">885</a> , <a href="#">916</a>                |
| Code Calling IDs ..... <a href="#">494</a>                                   | Configuration Set Description ..... <a href="#">497</a>  |
| Code Calling Playing Cycles ..... <a href="#">781</a>                        | Configurations ..... <a href="#">343</a>   |
| Code Calling, COR ..... <a href="#">781</a>                                  | Configure options ..... <a href="#">1060</a>   |
| Code Calling, TAC ..... <a href="#">781</a>                                  | Configuring ..... <a href="#">137</a>  |
| Code Calling, TN ..... <a href="#">781</a>                                   | Configuring Avaya Site Administration ..... <a href="#">137</a>  |

|   |   |   |   |
|---|---|---|---|
| configuring enterprise licensing .....  | <a href="#">1137</a>                      | Controlled Toll Restriction Replaces .....          | <a href="#">587</a>   |
| Configuring Polycom PathNavigator Gatekeepers ....  | <a href="#">370</a>                       | Controlling Adjunct .....                           | <a href="#">654</a>   |
| Configuring the Maximum Bandwidth for Inter-Network<br>Regions .....                          | <a href="#">373</a>                       | Controlling Calls Users Can Make and Receive .....  | <a href="#">163</a>   |
| Configuring the Polycom VSX Video Conferencing<br>Systems and V500 Video Calling Systems .... | <a href="#">367</a>                       | Conv .....  | <a href="#">422</a> , <a href="#">831</a> , <a href="#">1044</a>  |
| Configuring video trunks between two Avaya<br>Communication Manager systems .....             | <a href="#">371</a>                       | Converse Data Return Code .....                     | <a href="#">570</a>   |
| Configuring Video-Enabled Avaya IP Softphone<br>Endpoints .....                               | <a href="#">366</a>                       | Converse First Data Relay .....                     | <a href="#">611</a>   |
| Configuring your system .....   | <a href="#">237</a>                       | Converse Second Data Relay .....                    | <a href="#">611</a>   |
| Confirmed Answer .....  | <a href="#">497</a>                       | Converse Signaling Pause .....                      | <a href="#">611</a>   |
| Connect .....   | <a href="#">538</a> , <a href="#">856</a> | Converse Signaling Tone .....                       | <a href="#">612</a>   |
| Signaling Group .....   | <a href="#">856</a>                       | Conversion to Full Public Number - Delete .....     | <a href="#">695</a>   |
| CONNECT Reliable When Call Leaves ISDN .....  | <a href="#">734</a>                       | Conversion to Full Public Number - Insert .....     | <a href="#">695</a>   |
| Connected Indication .....  | <a href="#">522</a>                       | Convert 180 to 183 for Early Media .....            | <a href="#">1042</a>  |
| Connected to .....  | <a href="#">516</a>                       | Convert First Digit End-of-Dial To .....            | <a href="#">791</a>   |
| Connected to CO .....   | <a href="#">1010</a>                      | Copy ASAI UUI During Conference/Transfer .....      | <a href="#">615</a>   |
| connected to customer network .....   | <a href="#">135</a>                       | COR ..  | <a href="#">59</a> , <a href="#">429</a> , <a href="#">437</a> , <a href="#">445</a> , <a href="#">449</a> , <a href="#">454</a> , <a href="#">500</a> , <a href="#">514</a> , <a href="#">516</a> , <a href="#">634</a> , <a href="#">647</a> ,<br><a href="#">723</a> , <a href="#">832</a> , <a href="#">839</a> , <a href="#">886</a> , <a href="#">968</a> , <a href="#">981</a> , <a href="#">1049</a> , <a href="#">1070</a> |
| connected to services port .....  | <a href="#">134</a>                       | Access Endpoint .....                               | <a href="#">429</a>   |
| Connecting the Telephone physically .....   | <a href="#">170</a>                       | Agent Login ID .....                                | <a href="#">437</a>   |
| Connection Number .....   | <a href="#">432</a>                       | Announcements/Audio Sources .....                   | <a href="#">445</a>   |
| Connectivity Time .....   | <a href="#">926</a>                       | Attendant Console .....                             | <a href="#">449</a> , <a href="#">454</a>   |
| Connectivity Timer .....  | <a href="#">718</a>                       | console parameters .....                            | <a href="#">500</a>   |
| Console parameters .....  | <a href="#">498</a> , <a href="#">504</a> | Data Module .....                                   | <a href="#">516</a>   |
| page 3 .....  | <a href="#">504</a>                       | Group Paging Using Speakerphone .....               | <a href="#">634</a>   |
| Console Parameters  |   | Hunt Group .....                                    | <a href="#">647</a>   |
| abbreviated dialing .....   | <a href="#">501</a>                       | Terminating Extension Group .....                   | <a href="#">968</a>   |
| common shared extensions .....  | <a href="#">502</a>                       | COR Description .....                               | <a href="#">481</a>   |
| incoming call reminders .....   | <a href="#">502</a>                       | COR Number .....                                    | <a href="#">482</a>   |
| setting .....   | <a href="#">251</a>                       | COR to Use for DPT .....                            | <a href="#">588</a>   |
| timing .....  | <a href="#">503</a>                       | COR/COS .....                                       | <a href="#">400</a>   |
| Console Permissions .....   | <a href="#">491</a>                       | COR/FRL check for Covered and Forwarded Calls ....  | <a href="#">928</a>   |
| Console Type .....  | <a href="#">449</a>                       | Cord Length .....                                   | <a href="#">74</a> , <a href="#">886</a> , <a href="#">1085</a>   |
| Constraints .....   | <a href="#">359</a>                       | COS .....   | <a href="#">59</a> , <a href="#">430</a> , <a href="#">449</a> , <a href="#">454</a> , <a href="#">500</a> , <a href="#">516</a> , <a href="#">832</a> , <a href="#">839</a> , <a href="#">886</a> , <a href="#">1070</a>   |
| Consult .....   | <a href="#">400</a>                       | Access Endpoint .....                               | <a href="#">430</a>   |
| Contact Closure Activation .....  | <a href="#">492</a>                       | Attendant Console .....                             | <a href="#">449</a> , <a href="#">454</a>   |
| Contact Closure Close Code .....  | <a href="#">561</a>                       | console parameters .....                            | <a href="#">500</a>   |
| Contact Closure Open Code .....   | <a href="#">561</a>                       | Station .....                                       | <a href="#">59</a> , <a href="#">886</a> , <a href="#">1070</a>   |
| Contact Closure Pulse Code .....  | <a href="#">562</a>                       | COS Group .....                                     | <a href="#">492</a> , <a href="#">963</a>   |
| Contiguous .....  | <a href="#">757</a> , <a href="#">833</a> | COS Name .....                                      | <a href="#">492</a>   |
| Continue Daily Until Completed .....  | <a href="#">632</a>                       | Count .....   | <a href="#">502</a>   |
| Continuous .....  | <a href="#">433</a>                       | Country .....                                       | <a href="#">822</a> , <a href="#">981</a>   |
| Controlled Outward Restriction Intercept Treatment ....                                       | <a href="#">583</a>                       | Country code for CDR .....                          | <a href="#">774</a>   |
| Controlled Restrictions Configuration .....   | <a href="#">636</a>                       | country options table .....                         | <a href="#">935</a>   |
| Controlled Station to Station Restriction .....   | <a href="#">584</a>                       | Country Protocol .....                              | <a href="#">539</a> , <a href="#">856</a> , <a href="#">886</a>   |
| Controlled Termination Restriction .....  | <a href="#">584</a>                       | Coverage .....                                      | <a href="#">396</a>   |
| Controlled Toll Restriction Intercept Treatment .....   | <a href="#">587</a>                       | Coverage - Caller Response Interval (seconds) ..... | <a href="#">928</a>   |
|   |   | Coverage After Forwarding .....                     | <a href="#">61</a> , <a href="#">886</a> , <a href="#">932</a> , <a href="#">1073</a>   |
|   |   | Coverage Answer Group .....                         | <a href="#">507</a>   |
|   |   | COVERAGE CRITERIA .....                             | <a href="#">509</a>   |
|   |   | Coverage Module .....                               | <a href="#">887</a>   |
|   |   | Coverage Msg Retrieval .....                        | <a href="#">69</a> , <a href="#">887</a> , <a href="#">1080</a>   |

|  |   |   |  |
|--|---|---|--|
| Coverage Of Calls Redirected Off-Net Enabled .....       | <a href="#">933</a>   | creating user roles .....                         | <a href="#">1197</a>   |
| coverage path .....                                      | <a href="#">561</a>   | Crisis Alert Code .....                           | <a href="#">512</a>  |
| Coverage Path .....                                      | <a href="#">437</a> , <a href="#">508</a> , <a href="#">647</a> , <a href="#">817</a> , <a href="#">968</a> | Crisis Alert System Parameters .....              | <a href="#">511</a>  |
| Terminating Extension Group .....                        | <a href="#">968</a>   | Crisis Alert to a Digital Pager .....             | <a href="#">511</a>  |
| Coverage Path 1 or Coverage Path 2 .....                 | <a href="#">59</a> , <a href="#">887</a> , <a href="#">1070</a>   | Criteria for Logged Off/PSA/TTI Stations .....    | <a href="#">930</a>  |
| Coverage Path Number .....                               | <a href="#">508</a>   | Critical Reliable Bearer .....                    | <a href="#">683</a>  |
| COVERAGE POINTS .....                                    | <a href="#">510</a>   | CRV Length .....                                  | <a href="#">515</a> , <a href="#">887</a>  |
| CPE LOOPBACK JACK OPTIONS .....                          | <a href="#">554</a>   | CTI Link .....                                    | <a href="#">514</a>  |
| CPN .....  | <a href="#">565</a>   | CTI Stations .....                                | <a href="#">954</a>  |
| CPN Len .....  | <a href="#">720</a>   | Currency Symbol .....                             | <a href="#">739</a> , <a href="#">822</a> , <a href="#">1010</a>   |
| CPN Prefix .....   | <a href="#">720</a> , <a href="#">815</a>   | Custom Selection of VIP DID Numbers .....         | <a href="#">641</a> , <a href="#">887</a>  |
| CPN, ANI for Dissociated Sets .....                      | <a href="#">580</a>   | Customer Telephone Activation (CTA) Enabled ..... | <a href="#">581</a>  |
| CPN/ANI/ICLID Parameters .....                           | <a href="#">604</a>   | Customizable Labels .....                         | <a href="#">887</a>  |
| CPN/ANI/ICLID Replacement for Restricted Calls ....      | <a href="#">604</a>   | Customize .....                                   | <a href="#">778</a>  |
| CPN/ANI/ICLID Replacement for Unavailable Calls ....     | <a href="#">604</a>   | Customize Parameters .....                        | <a href="#">965</a>  |
| CRC .....  | <a href="#">539</a>   | Customize the phone .....                         | <a href="#">175</a>  |
| Create New Profile page .....                            | <a href="#">1123</a>  | Cut-Through .....                                 | <a href="#">994</a>  |
| Create Universal Call ID (UCID) .....                    | <a href="#">590</a>   | Cvg Of Calls Redirected Off-net .....             | <a href="#">944</a>  |
| creating a low priority enforced ACL rule .....          | <a href="#">1677</a>  | CVG Path .....                                    | <a href="#">971</a>  |
| Creating a multi-party video conference ....             | <a href="#">395</a> , <a href="#">410</a> , <a href="#">411</a>   | Cyclical Hunt .....                               | <a href="#">995</a>  |
| creating a new communication address for a profile ....  | <a href="#">1561</a>  |   |  |
| creating a new communication profile .....               | <a href="#">1560</a>  | <b>D</b>  |  |
| creating a new high priority enforced ACL rule .....     | <a href="#">1675</a>  | D Channel .....                                   | <a href="#">856</a>  |
| creating a new instance .....                            | <a href="#">21</a>  | D-Channel .....                                   | <a href="#">539</a>  |
| creating a new log harvesting profile .....              | <a href="#">1115</a>  | dadmin login .....                                | <a href="#">945</a>  |
| creating a new port .....                                | <a href="#">25</a>  | Daily Wakeup .....                                | <a href="#">641</a>  |
| creating a new System ACL rule .....                     | <a href="#">1679</a>  | Data Call Setup .....                             | <a href="#">400</a>  |
| Creating a New Time of Day Routing Plan .....            | <a href="#">337</a>   | Data Collaboration .....                          | <a href="#">397</a>  |
| creating a new user profile .....                        | <a href="#">1391</a>  | Data Extension .....                              | <a href="#">454</a> , <a href="#">517</a> , <a href="#">888</a>  |
| creating a system data backup on a local computer ....   | <a href="#">1298</a>  | Data Item .....                                   | <a href="#">476</a>  |
| creating a system rule .....                             | <a href="#">1682</a>  | Data Module .....                                 | <a href="#">449</a> , <a href="#">516</a> , <a href="#">888</a>  |
| creating a user on communication management system ..... | <a href="#">1392</a>  | Attendant Console .....                           | <a href="#">449</a>  |
| creating Adaptations .....                               | <a href="#">1245</a>  | Station .....                                     | <a href="#">888</a>  |
| creating an access point .....                           | <a href="#">26</a>  | Data Option .....                                 | <a href="#">888</a>  |
| creating dial patterns .....                             | <a href="#">1282</a>  | Data Origination Access Code .....                | <a href="#">562</a>  |
| creating domains .....                                   | <a href="#">1234</a>  | Data Privacy .....                                | <a href="#">492</a>  |
| creating duplicate groups .....                          | <a href="#">1164</a>  | Data Privacy Access Code .....                    | <a href="#">562</a>  |
| creating duplicate roles .....                           | <a href="#">1198</a>  | Data Replication page .....                       | <a href="#">1317</a>   |
| creating duplicate users .....                           | <a href="#">1392</a>  | data replication service .....                    | <a href="#">1312</a>   |
| creating Entity Links .....                              | <a href="#">1267</a>  | Data Restriction .....                            | <a href="#">69</a> , <a href="#">739</a> , <a href="#">817</a> , <a href="#">888</a> , <a href="#">1010</a> , <a href="#">1081</a> |
| creating groups .....                                    | <a href="#">1162</a>  | Data Retention page .....                         | <a href="#">1306</a> , <a href="#">1311</a>  |
| creating locations .....                                 | <a href="#">1238</a>  | data retention rules .....                        | <a href="#">1310</a>   |
| creating regular expressions .....                       | <a href="#">1289</a>  | Data Transport Static Config page .....           | <a href="#">1388</a>   |
| creating routing policies .....                          | <a href="#">1275</a>  | Data Trunk Groups .....                           | <a href="#">400</a>  |
| creating SIP entities .....                              | <a href="#">1257</a>  | DataHotline .....                                 | <a href="#">400</a>  |
| creating time ranges .....                               | <a href="#">1270</a>  | Date  |  |
|  |   | Bulletin Board .....                              | <a href="#">463</a>  |
|  |   | Date (Start) .....                                | <a href="#">528</a>  |
|  |   | Date (Stop) .....                                 | <a href="#">528</a>  |
|  |   | Date and Time .....                               | <a href="#">526</a>  |
|  |   | Date Format on 607/2400/4600/6400 Terminals ..... | <a href="#">606</a>  |

|   |  |   |   |
|---|--|---|---|
| Date Format on Terminals .....                          | <a href="#">606</a>  | Delete .....  | <a href="#">464</a> , <a href="#">720</a>   |
| Day   |  | Call Type Digit Analysis Table .....                  | <a href="#">464</a>                         |
| system parameters port networks .....                   | <a href="#">960</a>  | delete a mailing address .....                        | <a href="#">1401</a>                        |
| Day of the Month .....                                  | <a href="#">526</a>  | Delete Application Confirmation page .....            | <a href="#">34</a>                          |
| Day of the Week .....                                   | <a href="#">526</a>  | Delete Confirmation Page .....                        | <a href="#">1335</a>                        |
| Daylight Savings Rule .....                             | <a href="#">526</a> , <a href="#">1056</a>   | Delete Group Confirmation page .....                  | <a href="#">1181</a>                        |
| daylight savings rules .....                            | <a href="#">141</a>  | Delete Local WebLM page .....                         | <a href="#">1151</a>                        |
| Daylight Savings Rules .....                            | <a href="#">140</a> , <a href="#">141</a> , <a href="#">527</a>  | Deleted Trusted Certificate Confirmation page .....   | <a href="#">46</a>                          |
| DC .....  | <a href="#">672</a>  | Deleted Users page .....                              | <a href="#">1651</a>                        |
| DCP Terminal-parameters Plan .....                      | <a href="#">774</a>  | deleting  |   |
| DCP/Analog Bearer Capability .....                      | <a href="#">760</a> , <a href="#">762</a> , <a href="#">857</a>  | pending jobs  |   |
| DCP/ANALOG Bearer Capability .....                      | <a href="#">540</a>  | completed jobs .....                                  | <a href="#">1323</a>                        |
| DCS (Basic) .....                                       | <a href="#">944</a>  | deleting a communication address .....                | <a href="#">1563</a>                        |
| DCS Call Coverage .....                                 | <a href="#">945</a>  | deleting a Communication Manager Access profile ....  | <a href="#">122</a>                         |
| DCS Signaling .....                                     | <a href="#">740</a>  | deleting a communication profile .....                | <a href="#">1561</a>                        |
| DCS to QSIG TSC Gateway .....                           | <a href="#">529</a>  | deleting a global user settings importing Job .....   | <a href="#">1420</a>                        |
| DCS with Rerouting .....                                | <a href="#">945</a>  | deleting a port .....                                 | <a href="#">26</a>                          |
| DCS/QSIG Intw .....                                     | <a href="#">844</a>  | deleting a profile .....                              | <a href="#">1116</a>                        |
| Deactivation .....                                      | <a href="#">239</a>  | deleting a role importing job .....                   | <a href="#">1206</a>                        |
| Debug Filter Values .....                               | <a href="#">716</a>  | deleting a shared address .....                       | <a href="#">1671</a>                        |
| Decimal Point .....                                     | <a href="#">740</a> , <a href="#">823</a> , <a href="#">1011</a>   | deleting a station profile .....                      | <a href="#">1567</a> , <a href="#">1570</a> |
| Default ANI .....                                       | <a href="#">791</a>  | deleting a subnet .....                               | <a href="#">120</a>                         |
| Default Announcement Extension .....                    | <a href="#">641</a>  | deleting a user .....                                 | <a href="#">1399</a>                        |
| Default Call Appearance Display Format .....            | <a href="#">536</a>  | deleting Adaptations .....                            | <a href="#">1249</a>                        |
| Default COR .....                                       | <a href="#">581</a>  | deleting an access point .....                        | <a href="#">27</a>                          |
| Default Coverage Path for Client Rooms .....            | <a href="#">637</a>  | deleting an announcement .....                        | <a href="#">88</a>                          |
| DEFAULT DIALING .....                                   | <a href="#">456</a>  | deleting an application instance .....                | <a href="#">23</a>                          |
| Default Dialing Abbreviated Dialing Dial Code .....     | <a href="#">888</a>  | deleting an audio group .....                         | <a href="#">98</a>                          |
| Default Multimedia Outgoing Trunk Parameter Selection   |  | deleting an Import Job .....                          | <a href="#">1414</a>                        |
| <a href="#">579</a>                                     |  | deleting announcements .....                          | <a href="#">88</a>                          |
| Default Reason Code .....                               | <a href="#">837</a>  | deleting audio groups .....                           | <a href="#">98</a>                          |
| Default Route Digit .....                               | <a href="#">809</a>  | deleting Communication Manager Access profile ....    | <a href="#">122</a>                         |
| Default RTCP Report Period (secs) .....                 | <a href="#">704</a>  | deleting contact addresses of a private contact ..... | <a href="#">1608</a>                        |
| Default Server IP Address .....                         | <a href="#">704</a>  | deleting contact addresses of a public contact .....  | <a href="#">1660</a>                        |
| Default Server Port .....                               | <a href="#">704</a>  | deleting contacts from the contact list .....         | <a href="#">1597</a>                        |
| Default Service Domain .....                            | <a href="#">809</a>  | deleting dial patterns .....                          | <a href="#">1283</a>                        |
| default settings .....                                  | <a href="#">1295</a>   | deleting domains .....                                | <a href="#">1235</a>                        |
| defining a new policy for Enforced User ACL rules ....  |  | deleting endpoints                                    |   |
| <a href="#">1680</a>                                    |  | removing endpoints .....                              | <a href="#">54</a>                          |
| Defining options for calling party identification ..... | <a href="#">238</a>  | deleting Entity Links .....                           | <a href="#">1268</a>                        |
| Definition for Rooms in State 1 through 6 .....         | <a href="#">644</a>  | deleting groups .....                                 | <a href="#">1164</a>                        |
| Definitions .....                                       | <a href="#">375</a>  | deleting high priority enforced ACL rules .....       | <a href="#">1676</a>                        |
| Del .....   | <a href="#">422</a> , <a href="#">669</a> , <a href="#">831</a> , <a href="#">1044</a>   | deleting Locations .....                              | <a href="#">1239</a>                        |
| Incoming Call Handling Treatment .....                  | <a href="#">669</a>  | deleting low priority enforced ACL rules .....        | <a href="#">1678</a>                        |
| Delay   |  | Deleting messages .....                               | <a href="#">143</a>                         |
| feature related system parameters .....                 | <a href="#">609</a>  | deleting policies .....                               | <a href="#">1681</a>                        |
| Delay Call Setup When Accessed Via IGAR .....           | <a href="#">995</a>  | deleting postal addresses of a private contact .....  | <a href="#">1606</a>                        |
| Delay for USNI Calling Name for Analog Caller ID        |  | deleting postal addresses of a public contact .....   | <a href="#">1658</a>                        |
| Phones (seconds) .....                                  | <a href="#">599</a>  | deleting private contact of a user .....              | <a href="#">1604</a>                        |
| Delay Sending Release .....                             | <a href="#">589</a>  | deleting public contact of a user .....               | <a href="#">1656</a>                        |
| delete .....  | <a href="#">54</a> , <a href="#">88</a> , <a href="#">98</a> , <a href="#">117</a> , <a href="#">120</a> , <a href="#">122</a> |   |   |

|  |   |   |  |
|--|---|---|--|
| deleting regular expressions .....                     | <a href="#">1290</a>  | Digit Absorption .....                                  | <a href="#">536</a>  |
| deleting routing policies .....                        | <a href="#">1277</a>  | Digit Absorption List .....                             | <a href="#">982</a>  |
| deleting SIP entities .....                            | <a href="#">1260</a>  | Digit Handling (in/out) .....                           | <a href="#">735</a>  |
| deleting SNMP Access profile .....                     | <a href="#">117</a>   | Digit to Insert/Delete .....                            | <a href="#">642</a>  |
| deleting subnets .....                                 | <a href="#">120</a>   | Digit Treatment .....                                   | <a href="#">996</a>  |
| deleting System ACL rules .....                        | <a href="#">1680</a>  | Digital Loss Group .....                                | <a href="#">735</a> , <a href="#">823</a> , <a href="#">995</a>  |
| deleting system rules .....                            | <a href="#">1683</a>  | Digital Loss Plan Modification .....                    | <a href="#">945</a>  |
| deleting time ranges .....                             | <a href="#">1271</a>  | digital PPM per country protocol .....                  | <a href="#">549</a>  |
| deleting user roles .....                              | <a href="#">1198</a>  | Digits .....  | <a href="#">995</a>  |
| Deluxe Paging and Call Park Timeout to Originator .... | <a href="#">585</a>   | Digits to Record for Outgoing Calls .....               | <a href="#">470</a>  |
| denied locations for dial patterns .....               | <a href="#">1241</a>  | Direct Agent Announcement Extension .....               | <a href="#">610</a>  |
| Deny   |   | Direct Agent Calling .....                              | <a href="#">482</a>  |
| Survivable ARS Analysis Table .....                    | <a href="#">920</a>   | Direct Agent Skill .....                                | <a href="#">441</a>  |
| Description .....                                      | <a href="#">635</a> , <a href="#">811</a> , <a href="#">853</a> , <a href="#">1046</a> , <a href="#">1056</a> | Direct Agents Calls First .....                         | <a href="#">437</a>  |
| Holiday Table .....                                    | <a href="#">635</a>   | Direct Dial Access-Trunk .....                          | <a href="#">783</a>  |
| Service Hours Table .....                              | <a href="#">853</a>   | Direct Inside Access .....                              | <a href="#">783</a>  |
| Dest # 1, 2, or 3 IP Address .....                     | <a href="#">715</a>   | Direct IP-IP Audio Connections ...                      | <a href="#">70</a> , <a href="#">452</a> , <a href="#">627</a> , <a href="#">631</a> , <a href="#">857</a> ,<br><a href="#">889</a> , <a href="#">1081</a> |
| Dest # IP address .....                                | <a href="#">707</a>   | Direct Trunk Group Select Button Assignments .....      | <a href="#">451</a>  |
| Dest. Digits .....                                     | <a href="#">872</a> , <a href="#">873</a>   | direct-WAN .....  | <a href="#">698</a>  |
| Destination .....                                      | <a href="#">432</a> , <a href="#">1049</a>  | Directed Call Pickup .....                              | <a href="#">301</a> , <a href="#">303</a> , <a href="#">304</a> , <a href="#">481</a> , <a href="#">631</a>  |
| Destination Node .....                                 | <a href="#">710</a> , <a href="#">835</a> , <a href="#">923</a>   | assigning button .....                                  | <a href="#">303</a>  |
| Destination Port .....                                 | <a href="#">835</a> , <a href="#">923</a>   | assigning feature access code .....                     | <a href="#">303</a>  |
| Detect Slips .....                                     | <a href="#">760</a>   | removing .....  | <a href="#">304</a>  |
| detection and alarms .....                             | <a href="#">705</a>   | Directed Call Pickup                                    |  |
| device discovery .....                                 | <a href="#">115</a> , <a href="#">123</a> , <a href="#">124</a>   | creating classes of restriction .....                   | <a href="#">302</a>  |
| DHCP .....   | <a href="#">711</a> , <a href="#">714</a>   | ensuring availability .....                             | <a href="#">301</a>  |
| Dial Access .....                                      | <a href="#">724</a> , <a href="#">982</a>   | Directed Call Pickup Access Code .....                  | <a href="#">562</a>  |
| Dial Access to Attendant .....                         | <a href="#">400</a>   | Directed Group Call Pickup Access Code .....            | <a href="#">562</a>  |
| DIAL CODE .....  | <a href="#">424</a> , <a href="#">426</a> , <a href="#">427</a>   | Direction .....   | <a href="#">724</a> , <a href="#">786</a> , <a href="#">982</a>  |
| Dial Detection .....                                   | <a href="#">995</a>   | Directory Buttons                                       |  |
| Dial Echoing .....                                     | <a href="#">523</a>   | Setting .....   | <a href="#">263</a>  |
| dial pattern deletion .....                            | <a href="#">1284</a>  | Directory Number .....                                  | <a href="#">764</a>  |
| dial pattern details .....                             | <a href="#">1285</a>  | Directory Search Sort Order .....                       | <a href="#">938</a>  |
| dial patterns .....                                    | <a href="#">1284</a>  | Disable call classifier for CCRON over ISDN trunks .... | <a href="#">933</a>  |
| Dial Plan Analysis Table .....                         | <a href="#">530</a>   | Disable call classifier for CCRON over SIP Enablement   |  |
| Dial Plan Parameters .....                             | <a href="#">533</a>   | Services (SES) trunks .....                             | <a href="#">933</a>  |
| Dial Plan Transparency in Survivable Mode .....        | <a href="#">695</a>   | Disable Confirmation page .....                         | <a href="#">1333</a>   |
| dial prefix .....                                      | <a href="#">916</a>   | Disable Following a Security Violation .....            | <a href="#">839</a>  |
| Dial Prefix .....                                      | <a href="#">888</a> , <a href="#">917</a>   | Disable Restarts .....                                  | <a href="#">540</a>  |
| Dial Tone Validation Timer (sec) .....                 | <a href="#">937</a>   | Disabling   |  |
| Dialed String .....                                    | <a href="#">420</a> , <a href="#">531</a> , <a href="#">830</a> , <a href="#">920</a> , <a href="#">973</a>   | pending jobs  |  |
| Dialed String length (Min, Max) .....                  | <a href="#">464</a>   | completed jobs .....                                    | <a href="#">1324</a>   |
| Dialed String Match .....                              | <a href="#">464</a>   | Disabling firmware downloads .....                      | <a href="#">201</a>  |
| DID Busy Treatment .....                               | <a href="#">592</a>   | Disconnect Information in Place of FRL .....            | <a href="#">470</a>  |
| DID to Attendant .....                                 | <a href="#">505</a>   | Disconnect on No Answer by Call Type .....              | <a href="#">938</a>  |
| DID-LDN Only to LDN Night Ext .....                    | <a href="#">500</a>   | Disconnect Sequence .....                               | <a href="#">523</a>  |
| DID/Tie/ISDN/SIP Intercept Treatment .....             | <a href="#">576</a>   | Disconnect Signal Error (sec) .....                     | <a href="#">1025</a>   |
| DID/Tie/ISDN/SIP Treatment .....                       | <a href="#">575</a>   | Disconnect Supervision-In .....                         | <a href="#">823</a> , <a href="#">996</a>  |
| DiffServ .....   | <a href="#">713</a>   | Disconnect Supervision-Out .....                        | <a href="#">735</a> , <a href="#">997</a>  |
| Diffserv/TOS Parameters .....                          | <a href="#">691</a> , <a href="#">692</a>   |   |  |

|  |   |  |   |
|--|---|--|---|
| Disconnect Timing (msec) .....   | <a href="#">776</a> , <a href="#">997</a>   | Distinctive Audible Alerting .....   | <a href="#">595</a> , <a href="#">596</a> , <a href="#">964</a>   |
| Disconnect Type .....  | <a href="#">997</a>   | Distinctive ringing .....  | <a href="#">162</a>   |
| discovered device inventory list .....   | <a href="#">128</a>   | Diversion by Reroute .....   | <a href="#">749</a>   |
| discovered inventory .....   | <a href="#">126</a> , <a href="#">127</a>   | DLI Voltage Level .....  | <a href="#">966</a>   |
| discovered inventory list .....  | <a href="#">127</a>   | DMI-BOS .....  | <a href="#">540</a>   |
| discovering devices .....  | <a href="#">115</a> , <a href="#">124</a>   | Do Not Disturb Restriction .....   | <a href="#">584</a>   |
| discovery .....  | <a href="#">123</a>   | Do Not Send Group B Signals to CO .....                                    | <a href="#">797</a>   |
| discovery management .....   | <a href="#">115</a>   | domain deletion confirmation .....   | <a href="#">1235</a>  |
| discovering devices field description .....                                      | <a href="#">125</a>   | domains .....  | <a href="#">1235</a>  |
| Disp Client Redir .....  | <a href="#">449</a>   | download .....   | <a href="#">90</a>  |
| Disp Parm .....  | <a href="#">771</a>   | Download Flag .....  | <a href="#">706</a> , <a href="#">707</a>   |
| Display administration .....   | <a href="#">254</a>   | Download Set Type .....  | <a href="#">633</a>   |
| Display Authorization Code .....   | <a href="#">587</a>   | downloading an announcement .....  | <a href="#">90</a>  |
| Display Caller ID .....  | <a href="#">889</a>   | downloading announcements .....  | <a href="#">90</a>  |
| Display Calling Number for Room to Room Caller ID<br>Calls .....                 | <a href="#">576</a>   | downloading audio groups .....   | <a href="#">98</a>  |
| Display Cartridge .....  | <a href="#">889</a>   | Downloading firmware to a 2420, 2410, 1408, or 1416<br>DCP telephone ..... | <a href="#">197</a>   |
| Display Character Set .....  | <a href="#">938</a>   | Downloading firmware to a single station .....                             | <a href="#">199</a>   |
| Display Client Redirection .....   | <a href="#">70</a> , <a href="#">889</a> , <a href="#">1081</a>                       | Downloading firmware to multiple stations .....                            | <a href="#">200</a>   |
| Display Connected Name/Number for ISDN DCS Calls<br>.....                        | <a href="#">600</a>   | downloading harvested log files .....                                      | <a href="#">1119</a>  |
| Display Forwarding Party Name .....  | <a href="#">749</a>   | Downloading the error records for an unsuccessful role<br>import .....     | <a href="#">1206</a>  |
| Display Information With Bridged Call .....                                      | <a href="#">629</a>   | Downloading the firmware file to Communication<br>Manager .....            | <a href="#">198</a>   |
| Display labels .....   | <a href="#">170</a>   | Drop Treatment .....   | <a href="#">998</a>   |
| Display Language .....   | <a href="#">62</a> , <a href="#">450</a> , <a href="#">889</a> , <a href="#">1073</a> | DS1 circuit pack<br>page 2 .....   | <a href="#">553</a>   |
| Display Language Changes .....   | <a href="#">256</a>   | DS1 Circuit Pack .....   | <a href="#">538</a>   |
| Display Mode .....   | <a href="#">965</a>   | DS1 Echo Cancellation .....  | <a href="#">740</a> , <a href="#">824</a> , <a href="#">945</a> , <a href="#">1011</a>                      |
| Display Module Button Assignments .....  | <a href="#">459</a>   | DS1 MSP .....  | <a href="#">945</a>   |
| Display Notification for a locked Station .....                                  | <a href="#">624</a>   | DSN Term .....   | <a href="#">741</a> , <a href="#">1011</a>  |
| Display Notification for Call Forward .....                                      | <a href="#">624</a>   | dst rgn .....  | <a href="#">698</a>   |
| Display Notification for Do Not Disturb .....                                    | <a href="#">624</a>   | DTMF Duration - Tone (msec) .....  | <a href="#">512</a>   |
| Display Notification for Enhanced Call Forward .....                             | <a href="#">624</a>   | DTMF Duration On .....   | <a href="#">784</a>   |
| Display Notification for Limit Number of Concurrent Calls<br><a href="#">624</a> | <a href="#">624</a>   | DTMF Feedback Signals For VRU .....  | <a href="#">951</a>   |
| Display Notification for Posted Messages .....                                   | <a href="#">624</a>   | DTMF Over IP .....   | <a href="#">857</a>   |
| Display Notification for Send All Calls .....                                    | <a href="#">624</a>   | DTMF Tone Feedback .....   | <a href="#">596</a>   |
| Display Parameters .....   | <a href="#">536</a>   | Dual Wakeup .....  | <a href="#">642</a>   |
| Display PBX data on telephone .....  | <a href="#">565</a>   | Duplex .....   | <a href="#">687</a> , <a href="#">713</a> , <a href="#">736</a> , <a href="#">786</a> , <a href="#">998</a> |
| Display Room Information in Call Display .....                                   | <a href="#">642</a>   | IP Interfaces .....  | <a href="#">687</a>   |
| Display Text .....   | <a href="#">604</a>   | ISDN Trunk Group .....   | <a href="#">736</a>   |
| Display VDN for Route-To DAC .....   | <a href="#">1053</a>  | Trunk Group .....  | <a href="#">998</a>   |
| Displaying   |   | Duplicate Group page .....   | <a href="#">1182</a>  |
| ANI calling party .....  | <a href="#">254</a>   | Duplicate role page .....  | <a href="#">1218</a>  |
| ICLID Information .....  | <a href="#">255</a>   | Duplicate Station .....  | <a href="#">555</a>   |
| Displaying daylight savings time rules .....                                     | <a href="#">141</a>   | Duplicate telephones .....   | <a href="#">172</a>   |
| Displaying firmware download status .....  | <a href="#">201</a>   | Duplicate Vector .....   | <a href="#">556</a>   |
| Displaying messages .....  | <a href="#">143</a>   | Duplicating MASI Terminals .....   | <a href="#">354</a>   |
| displaying SIP entity references .....   | <a href="#">1265</a>  | duplicating routing entity data .....                                      | <a href="#">1233</a>  |
| Displays   |   | Duration .....   | <a href="#">433</a>   |
| Troubleshooting .....  | <a href="#">262</a>   | Duration (msec) .....  | <a href="#">976</a>   |
| Distinctive Audible Alert .....  | <a href="#">890</a>   |  |   |

|  |   |   |   |
|--|---|---|---|
| Duration Maximum .....                               | <a href="#">958</a>   | completed jobs .....                                  | <a href="#">1322</a>  |
| Duration Minimum .....                               | <a href="#">959</a>   | editing a Communication Manager Access profile ....   | <a href="#">122</a>   |
| Duration of Call Timer Display .....                 | <a href="#">626</a>   | editing a logger in a log file .....                  | <a href="#">1110</a> , <a href="#">1301</a>   |
| Dynamic Advocate .....                               | <a href="#">951</a>   | editing a subnet .....                                | <a href="#">120</a>   |
| Dynamic CAC Gateway .....                            | <a href="#">698</a>   | editing an announcement .....                         | <a href="#">87</a>  |
| Dynamic Percentage Adjustment .....                  | <a href="#">654</a>   | editing an audio group .....                          | <a href="#">97</a>  |
| Dynamic Queue Position .....                         | <a href="#">654</a>   | editing announcements .....                           | <a href="#">87</a>  |
| Dynamic Threshold Adjustment .....                   | <a href="#">655</a> , <a href="#">951</a>   | editing audio groups .....                            | <a href="#">97</a>  |
| <hr/>  |   |   |   |
| <b>E</b>   |   |   |   |
| Early Answer .....                                   | <a href="#">394</a>   | editing class of service data .....                   | <a href="#">111</a>   |
| EAS .....  | <a href="#">467</a>   | editing Communication Manager profiles .....          | <a href="#">122</a>   |
| EAS-PHD .....  | <a href="#">951</a>   | editing endpoint extension; field description         |   |
| EC Configuration .....                               | <a href="#">551</a>   | endpoint extension .....                              | <a href="#">77</a>  |
| EC Direction .....                                   | <a href="#">552</a>   | editing SNMP Access profile .....                     | <a href="#">117</a>   |
| EC500 Self Administration Access Code .....          | <a href="#">562</a>   | editing subnets .....                                 | <a href="#">120</a>   |
| Echo Cancellation .....                              | <a href="#">552</a>   | editing subscriber templates CMM .....                | <a href="#">1088</a>  |
| Echo Digits Dialed .....                             | <a href="#">454</a>   | editing subscriber templates MM .....                 | <a href="#">1090</a>  |
| echo direction .....                                 | <a href="#">552</a>   | ednpoint templates; delete                            |   |
| edit .....   | <a href="#">87</a> , <a href="#">97</a> , <a href="#">111</a> , <a href="#">117</a> , <a href="#">120</a> , <a href="#">122</a> | deleting endpoint templates .....                     | <a href="#">1063</a>  |
| Edit Address page .....                              | <a href="#">1615</a> , <a href="#">1669</a>   | deleting templates .....                              | <a href="#">1063</a>  |
| Edit Appender page .....                             | <a href="#">1113</a> , <a href="#">1308</a>   | element links   |   |
| Edit Application Instance page .....                 | <a href="#">28</a>  | modifying .....                                       | <a href="#">1267</a>  |
| Edit Common Console Profile page .....               | <a href="#">1371</a>  | Emergency Access .....                                | <a href="#">505</a>   |
| Edit Contact List Member page .....                  | <a href="#">1599</a>  | Emergency Access Redirection Extension .....          | <a href="#">585</a> , <a href="#">588</a>   |
| Edit Dialing on 96xx H.323 Terminals .....           | <a href="#">606</a>   | Emergency Access to Attendant .....                   | <a href="#">945</a>   |
| edit endpoint .....                                  | <a href="#">58</a> , <a href="#">1069</a>   | Emergency Access To Attendant Access Code .....       | <a href="#">562</a>   |
| edit global feature profiles .....                   | <a href="#">1338</a>  | Emergency Location Ext .....                          | <a href="#">59</a> , <a href="#">452</a> , <a href="#">890</a> , <a href="#">1071</a> |
| Edit Group page .....                                | <a href="#">1179</a>  | emergency location extension .....                    | <a href="#">477</a>   |
| Edit High Priority Enforced User ACL page .....      | <a href="#">1692</a>  | Emergency Location Extension .....                    | <a href="#">478</a> , <a href="#">674</a>   |
| Edit Logger page .....                               | <a href="#">1112</a> , <a href="#">1307</a>   | EMU .....   | <a href="#">236</a> – <a href="#">239</a>   |
| Edit Private Contact List page .....                 | <a href="#">1611</a>  | EMU Inactivity Interval for Deactivation .....        | <a href="#">583</a>   |
| Edit Profile   |   | EMU Login Allowed .....                               | <a href="#">72</a> , <a href="#">890</a> , <a href="#">1084</a>                       |
| Alarming UI page .....                               | <a href="#">1341</a>  | Enable .....  | <a href="#">432</a> , <a href="#">835</a> , <a href="#">924</a>                       |
| Communication System Management Configuration        |   | Survivable Processor .....                            | <a href="#">924</a>   |
| page .....   | <a href="#">1372</a>  | Enable 'dadmin' Login .....                           | <a href="#">945</a>   |
| IAM page .....                                       | <a href="#">1355</a>  | Enable Busy Tone Disconnect for Analog Loop-start     |   |
| Licenses page .....                                  | <a href="#">1340</a>  | Trunks .....  | <a href="#">938</a>   |
| Logging page .....                                   | <a href="#">1365</a>  | Enable CDR Storage on Disk .....                      | <a href="#">471</a>   |
| Logging Service page .....                           | <a href="#">1367</a>  | Enable Command Logging .....                          | <a href="#">779</a>   |
| Role Bulk Import Profile page .....                  | <a href="#">1374</a>  | Enable Detection and Alarms .....                     | <a href="#">705</a>   |
| Edit Profile System Manager page .....               | <a href="#">1337</a>  | Enable Dial Plan Transparency in Survivable Mode .... | <a href="#">589</a>   |
| Edit Public Contact List page .....                  | <a href="#">1663</a>  | Enable Enbloc Dialing without ARS FAC .....           | <a href="#">605</a>   |
| Edit Role page .....                                 | <a href="#">1215</a>  | Enable Ethernet Interface .....                       | <a href="#">683</a> , <a href="#">687</a>   |
| Edit Scheduler Profile page .....                    | <a href="#">1369</a>  | Enable File Transfer .....                            | <a href="#">556</a>   |
| Edit System ACL page .....                           | <a href="#">1698</a>  | Enable Inter-Gateway Alternate Routing .....          | <a href="#">589</a>   |
| Edit System Manager Element Manager Profile page ... | <a href="#">1363</a>  | Enable Layer 3 Test .....                             | <a href="#">858</a>   |
| Edit System Rule page .....                          | <a href="#">1702</a>  | Enable on Survivable Processors (ESS and LSP) ....    | <a href="#">871</a>   |
| Editing  |   | Enable on the Main Processor(s)? .....                | <a href="#">871</a>   |
| pending jobs   |   | Enable Operation of IPSI Duplication .....            | <a href="#">956</a>   |

|   |   |  |   |
|---|---|--|---|
| Enable Operation of PNC Duplication .....               | <a href="#">956</a>   | editing templates .....                              | <a href="#">1062</a>  |
| Enable PE for H.248 Gateways .....                      | <a href="#">921</a>   | endpoint templates; field description                |   |
| Enable PE for H.323 Endpoints .....                     | <a href="#">921</a>   | edit endpoint templates; field description ....      | <a href="#">58</a> ,  |
| Enable Q-SIP .....                                      | <a href="#">1042</a>  | <a href="#">1069</a>                                 |   |
| Enable QoS .....  | <a href="#">711</a>   | view endpoint template field description ....        | <a href="#">58</a> , <a href="#">1069</a>                       |
| Enable Session .....                                    | <a href="#">557</a>   | endpoint templates; view                             |   |
| Enable Syslog .....                                     | <a href="#">715</a>   | viewing endpoint templates .....                     | <a href="#">1063</a>  |
| Enable Voice/Network Stats .....                        | <a href="#">703</a>   | viewing templates .....                              | <a href="#">1063</a>  |
| Enable VoIP/Network Thresholds .....                    | <a href="#">688</a>   | endpoint, adding templates                           |   |
| Enabled .....   | <a href="#">716</a> , <a href="#">719</a> , <a href="#">872</a> , <a href="#">873</a> , <a href="#">925</a> | adding endpoint templates .....                      | <a href="#">1062</a>  |
| Signaling Group .....                                   | <a href="#">872</a> , <a href="#">873</a>   | endpoints .....                                      | <a href="#">52</a> , <a href="#">54</a>                         |
| Survivable Processor .....                              | <a href="#">925</a>   | endpoints; bulk add                                  |   |
| Enabling  |   | bulk add endpoints .....                             | <a href="#">55</a>  |
| pending jobs  |   | endpoints; bulk edit                                 |   |
| completed jobs .....                                    | <a href="#">1324</a>  | bulk editing endpoints                               |   |
| Enabling extended text fields for feature buttons ....  | <a href="#">205</a>   | bulk edit .....                                      | <a href="#">55</a>  |
| Enabling transmission over IP .....                     | <a href="#">185</a>   | endpoints; edit                                      |   |
| Enbloc Dialing Parameters .....                         | <a href="#">605</a>   | editing endpoints .....                              | <a href="#">53</a>  |
| encrypting passwords .....                              | <a href="#">1410</a> , <a href="#">1411</a>   | endpoints; view                                      |   |
| Encryption .....  | <a href="#">711</a>   | viewing endpoints .....                              | <a href="#">53</a>  |
| End Day .....   | <a href="#">635</a>   | Endpt ID .....                                       | <a href="#">764</a> , <a href="#">890</a>                       |
| End Hour .....  | <a href="#">635</a>   | Endpt Init .....                                     | <a href="#">524</a> , <a href="#">764</a> , <a href="#">890</a> |
| End Min .....   | <a href="#">635</a>   | Enforce PNT-to-PNT Restrictions .....                | <a href="#">609</a>   |
| End Month .....   | <a href="#">635</a>   | Enforce SIPS URI for SRTP .....                      | <a href="#">858</a>   |
| End OCM After Answer (msec) .....                       | <a href="#">774</a>   | Enhanced Abbreviated Dial Length .....               | <a href="#">579</a>   |
| End of OCM Intercept Extension .....                    | <a href="#">775</a>   | Enhanced Abbreviated Dialing .....                   | <a href="#">766</a>   |
| End Time .....  | <a href="#">972</a>   | Enhanced Attendant Notification .....                | <a href="#">502</a>   |
| End to end signaling .....                              | <a href="#">753</a> , <a href="#">1032</a>  | enhanced call forwarding                             |   |
| End-to-End Signaling .....                              | <a href="#">998</a>   | activating from an off-network phone .....           | <a href="#">278</a>   |
| End-to-End total loss (dB) in a n-party conference .... | <a href="#">778</a>   | activating from phone with console parameters ....   | <a href="#">279</a>   |
| Ending Station .....                                    | <a href="#">633</a>   | activating using feature access code .....           | <a href="#">275</a>   |
| Endpoint .....  | <a href="#">588</a>   | activating using feature button .....                | <a href="#">275</a>   |
| endpoint administration                                 |   | deactivating from an off-network phone .....         | <a href="#">279</a>   |
| endpoint management                                     |   | deactivating from phone with console parameters ...  | <a href="#">280</a>   |
| endpoints .....   | <a href="#">51</a>  | deactivating using feature access code .....         | <a href="#">276</a>   |
| endpoint extension                                      |   | deactivating using feature button .....              | <a href="#">276</a>   |
| editing endpoint extension                              |   | displaying status using feature access code ....     | <a href="#">278</a>   |
| changing endpoint extension .....                       | <a href="#">54</a>  | displaying status using feature button .....         | <a href="#">278</a>   |
| endpoint list .....                                     | <a href="#">56</a>  | reactivating using feature access code .....         | <a href="#">277</a>   |
| endpoint template list .....                            | <a href="#">1067</a>  | reactivating using feature button .....              | <a href="#">277</a>   |
| endpoint template versions .....                        | <a href="#">1061</a>  | Enhanced Call Fwd .....                              | <a href="#">75</a> , <a href="#">1086</a>                       |
| endpoint template; distribute                           |   | Enhanced Call Pickup Alerting .....                  | <a href="#">631</a>   |
| distribution of templates .....                         | <a href="#">1064</a>  | Enhanced Call Pickup Delay Timer (sec.) .....        | <a href="#">631</a>   |
| endpoint templates .....                                | <a href="#">1062</a>  | Enhanced Call Pickup Delay Timer (sec.) Display .... | <a href="#">631</a>   |
| endpoint templates; duplicate                           |   | Enhanced Conferencing .....                          | <a href="#">945</a>   |
| copying templates .....                                 | <a href="#">1063</a>  | Enhanced EC500 .....                                 | <a href="#">945</a>   |
| duplicating endpoint templates .....                    | <a href="#">1063</a>  | Enhanced EC500 Activation .....                      | <a href="#">562</a>   |
| duplicating templates .....                             | <a href="#">1063</a>  | Enhanced EC500 Deactivation .....                    | <a href="#">562</a>   |
| endpoint templates; edit                                |   |  |   |
| editing endpoint templates .....                        | <a href="#">1062</a>  |  |   |

|   |   |   |   |
|---|---|---|---|
| Enhanced Mode Activation .....                        | <a href="#">571</a>   | Attendant Console .....                               | <a href="#">456</a>   |
| Enhanced Mode MM Complex .....                        | <a href="#">403</a>   | Coverage Answer Group .....                           | <a href="#">507</a>   |
| Enhanced Mode Operation .....                         | <a href="#">378</a> , <a href="#">403</a>   | Group Paging Using Speakerphone .....                 | <a href="#">634</a>   |
| Enhanced PSA Location/Display Information Enabled ... |   | Hunt Group .....                                      | <a href="#">668</a>   |
| <a href="#">581</a>                                   |   | Intercom Group .....                                  | <a href="#">673</a>   |
| Enrollment Password page .....                        | <a href="#">42</a>  | Listed Directory Numbers .....                        | <a href="#">770</a>   |
| Enterprise Configuration page .....                   | <a href="#">1146</a>  | Terminating Extension Group .....                     | <a href="#">969</a>   |
| Enterprise Mobility .....                             | <a href="#">235</a>   | Ext Alert (TAAS) Extension .....                      | <a href="#">500</a> , <a href="#">963</a>   |
| Enterprise Mobility User Activation .....             | <a href="#">563</a>   | Ext Alert Port (TAAS) .....                           | <a href="#">500</a> , <a href="#">963</a>   |
| Enterprise Mobility User Deactivation .....           | <a href="#">563</a>   | Ext and Name .....                                    | <a href="#">521</a>   |
| Enterprise Survivable Server .....                    | <a href="#">945</a>   | Ext Code .....  | <a href="#">469</a> , <a href="#">813</a> , <a href="#">815</a>   |
| Enterprise Usage page .....                           | <a href="#">1153</a>  | CAMA Numbering Format .....                           | <a href="#">469</a>   |
| Enterprise Wide Licensing .....                       | <a href="#">946</a>   | Ext Len .....   | <a href="#">469</a> , <a href="#">814</a> , <a href="#">816</a>   |
| entity links .....                                    | <a href="#">1268</a>  | CAMA Numbering Format .....                           | <a href="#">469</a>   |
| EPN .....   | <a href="#">852</a>   | Extended Call Fwd Activate All .....                  | <a href="#">563</a>   |
| EPSCS .....   | <a href="#">479</a>   | Extended Call Fwd Activate Busy D/A .....             | <a href="#">563</a>   |
| Erase 24xx User Data Upon:                            |   | Extended Cvg/Fwd Admin .....                          | <a href="#">946</a>   |
| Dissociate or unmerge this phone .....                | <a href="#">486</a>   | Extended Forwarding All .....                         | <a href="#">492</a>   |
| EMU login or logoff at this phone .....               | <a href="#">486</a>   | Extended Forwarding B/DA .....                        | <a href="#">492</a>   |
| ESF DATA LINK OPTIONS .....                           | <a href="#">554</a>   | Extended Group Call Pickup .....                      | <a href="#">585</a> , <a href="#">632</a>   |
| ESS Administration .....                              | <a href="#">946</a>   | Extended Group Call Pickup Access Code .....          | <a href="#">563</a>   |
| Established .....                                     | <a href="#">872</a> , <a href="#">873</a>   | Extended Group Number .....                           | <a href="#">557</a> , <a href="#">828</a>   |
| Establishing Customer Options .....                   | <a href="#">348</a>   | Extended Loop Range .....                             | <a href="#">999</a>   |
| Establishing Daylight Savings Rules .....             | <a href="#">140</a> , <a href="#">141</a>   | Extended Pick-Up Group .....                          | <a href="#">557</a>   |
| Establishing maintenance parameters and alarming      |   | Extended pickup group                                 |   |
| options .....   | <a href="#">348</a>   | assigning pickup groups .....                         | <a href="#">296</a>   |
| Establishing the physical connection .....            | <a href="#">348</a>   | associating individual pickup groups .....            | <a href="#">298</a>   |
| ETA Node Number .....                                 | <a href="#">533</a>   | creating .....  | <a href="#">296</a>   |
| ETA Routing Pattern .....                             | <a href="#">534</a>   | creating flexible groups .....                        | <a href="#">298</a>   |
| Ethernet Link .....                                   | <a href="#">683</a> , <a href="#">687</a>   | Extended Pickup Group                                 |   |
| Ethernet Options .....                                | <a href="#">682</a>   | changing groups .....                                 | <a href="#">300</a>   |
| ETSI CCBS .....                                       | <a href="#">760</a>   | Extension ...   | <a href="#">58</a> , <a href="#">430</a> , <a href="#">445</a> , <a href="#">450</a> , <a href="#">514</a> , <a href="#">558</a> , <a href="#">674</a> , <a href="#">832</a> , <a href="#">891</a> ,<br><a href="#">1049</a> , <a href="#">1069</a> |
| ETSI CCBS Support .....                               | <a href="#">858</a>   | Access Endpoint .....                                 | <a href="#">430</a>   |
| Event Minimization .....                              | <a href="#">515</a>   | Announcements/Audio Sources .....                     | <a href="#">445</a>   |
| Event processor page .....                            | <a href="#">1384</a>  | Attendant Console .....                               | <a href="#">450</a>   |
| Every User Responds .....                             | <a href="#">511</a>   | CTI Link .....  | <a href="#">514</a>   |
| Examples Of Digit Conversion .....                    | <a href="#">322</a>   | Intra-Switch CDR .....                                | <a href="#">674</a>   |
| Expansion Module .....                                | <a href="#">891</a>   | Station .....   | <a href="#">58</a> , <a href="#">891</a> , <a href="#">1069</a>   |
| Expected Call Handling Time (sec) .....               | <a href="#">655</a>   | EXTENSION DISPLAY FORMATS .....                       | <a href="#">534</a> , <a href="#">536</a>   |
| Expected Digits .....                                 | <a href="#">999</a>   | Extension only label for Team button on 96xx H.323    |   |
| Expert Agent Selection (EAS) .....                    | <a href="#">951</a>   | terminals .....                                       | <a href="#">604</a>   |
| Expert Agent Selection (EAS) Enabled .....            | <a href="#">610</a>   | Extension to Cellular .....                           | <a href="#">230</a>   |
| Expiration Date .....                                 | <a href="#">839</a>   | Extension to Cellular call security .....             | <a href="#">494</a>   |
| exporting   |   | Extension to Cellular Setup Table .....               | <a href="#">230</a>   |
| routing element data .....                            | <a href="#">1232</a>  | Extension to Receive Failed Wakeup LWC Messages ...   | <a href="#">642</a>   |
| exporting alarms .....                                | <a href="#">1099</a>  | Extensions Administered to have an MCT-Control Button |   |
| exporting global settings .....                       | <a href="#">1416</a>  | .....   | <a href="#">558</a>   |
| exporting roles in bulk .....                         | <a href="#">1202</a>  | extensions for chime codes .....                      | <a href="#">494</a>   |
| exporting users .....                                 | <a href="#">1407</a>  |   |   |
| exporting users in bulk .....                         | <a href="#">1407</a>  |   |   |
| Ext .....   | <a href="#">456</a> , <a href="#">494</a> , <a href="#">507</a> , <a href="#">634</a> , <a href="#">668</a> , <a href="#">673</a> , <a href="#">770</a> , <a href="#">827</a> , <a href="#">828</a> , <a href="#">969</a> |   |   |

|  |  |
|--|--|
| Extensions to Call Which Activate Features by Name ...<br><a href="#">558</a>  | filtering Communication Manager objects<br>using filters; Communication Manager objects .... <a href="#">84</a>  |
| External Coverage ..... <a href="#">783</a>  | filtering groups ..... <a href="#">1171</a>  |
| External Coverage Treatment for Transferred Incoming<br>Trunk Calls ..... <a href="#">930</a>  | filtering inventory list ..... <a href="#">127</a>   |
| External Device Alarm Admin ..... <a href="#">946</a>  | filtering log harvesting profiles ..... <a href="#">1120</a>   |
| External Ringing for Calls with Trunks ..... <a href="#">597</a>   | Filtering log harvesting requests ..... <a href="#">1121</a>   |
| <hr/>  | filtering logs ..... <a href="#">1103</a>  |
| <b>F</b>   | filtering network subnets ..... <a href="#">124</a>  |
| Facilities Restriction Level ..... <a href="#">482</a>   | filtering presentities ..... <a href="#">1683</a>  |
| Facility Access Trunk Test ..... <a href="#">482</a>   | filtering resources ..... <a href="#">1171</a> , <a href="#">1189</a>  |
| Facility Busy Indicators ..... <a href="#">567</a>   | filtering roles ..... <a href="#">1199</a>   |
| Facility Coding ..... <a href="#">812</a>  | filtering subnets ..... <a href="#">121</a>  |
| Facility Test Calls Access Code ..... <a href="#">563</a>  | filtering subscribers<br>using filters; subscribers ..... <a href="#">104</a>  |
| Facility Type ..... <a href="#">812</a>  | filtering templates<br>filtering endpoint templates ..... <a href="#">1068</a><br>filtering subscriber templates ..... <a href="#">1068</a><br>using filters; templates ..... <a href="#">1068</a> |
| Far End Resource Info ..... <a href="#">1057</a>   | filtering users ..... <a href="#">1393</a>   |
| Far End Test Line No. .... <a href="#">724</a>   | filtering watchers ..... <a href="#">1684</a>  |
| Far-end CSU Address ..... <a href="#">554</a>  | Firmware Station Download ..... <a href="#">632</a>  |
| Far-end Domain ..... <a href="#">859</a>   | First Announcement Delay (sec) ..... <a href="#">663</a>   |
| Far-end Listen Port ..... <a href="#">859</a>  | First Announcement Extension ..... <a href="#">663</a>   |
| Far-end Network Region ..... <a href="#">859</a>   | Five Port Networks Max Per MCC ..... <a href="#">946</a>   |
| Far-end Node Name ..... <a href="#">860</a>  | Fixed ..... <a href="#">756</a>  |
| Far-End Test No ..... <a href="#">1035</a>   | Fixed TEI ..... <a href="#">515</a> , <a href="#">525</a> , <a href="#">891</a>  |
| Fast Connect on Origination ..... <a href="#">497</a>  | Fixing Problems in Terminal Self-Administration ..... <a href="#">234</a>  |
| Fax  | Flash ..... <a href="#">506</a> , <a href="#">809</a>  |
| Adding ..... <a href="#">184</a>   | Flash Access Code ..... <a href="#">564</a> , <a href="#">573</a>  |
| Enabling transmission over IP networks ..... <a href="#">185</a>   | Flash Length (msec) ..... <a href="#">1026</a>   |
| FAX Mode ..... <a href="#">680</a>   | Flash Override ..... <a href="#">507</a> , <a href="#">809</a>   |
| FEAC ..... <a href="#">482</a>   | Flash Override Access Code ..... <a href="#">573</a>   |
| Feature Access Code ..... <a href="#">558</a>  | Flashhook Interval ..... <a href="#">776</a>   |
| Feature Access Code (FAC)<br>Refresh Terminal Parameters Access Code ..... <a href="#">567</a>   | Flexible Billing ..... <a href="#">946</a>   |
| FEATURE BUTTON ASSIGNMENTS ..... <a href="#">456</a>   | Flexible Extended Pickup Group<br>assigning pickup groups ..... <a href="#">299</a>  |
| Feature buttons table ..... <a href="#">206</a>  | Flexible Extended Pickup Groups ..... <a href="#">297</a>  |
| Feature Module ..... <a href="#">891</a>   | Floor  |
| Feature Options ..... <a href="#">60</a> , <a href="#">1071</a>  | Station ..... <a href="#">73</a> , <a href="#">891</a> , <a href="#">1084</a>  |
| Feature Plus Ext ..... <a href="#">600</a>   | Force Entry of Acct Code for Calls Marked on Toll<br>Analysis Form ..... <a href="#">471</a>   |
| Feature-related system parameters ..... <a href="#">573</a>  | Force Phones and Gateways to Active LSPs ..... <a href="#">705</a>   |
| field description .... <a href="#">58</a> , <a href="#">99</a> , <a href="#">112</a> , <a href="#">118</a> , <a href="#">128</a> , <a href="#">1069</a> , <a href="#">1088</a> ,<br><a href="#">1090</a> | Forced Agent Logout Time ..... <a href="#">437</a>   |
| File Size ..... <a href="#">969</a>  | Forced Entry of Account Codes ..... <a href="#">482</a> , <a href="#">946</a>  |
| File Status ..... <a href="#">969</a>  | Forced Entry of Stroke Counts or Call Work Codes ....<br><a href="#">661</a>   |
| File to Retrieve ..... <a href="#">970</a>   | Format ..... <a href="#">999</a> , <a href="#">1011</a>  |
| file transfer settings ..... <a href="#">92</a>  | Forward Cycle Timer (sec) ..... <a href="#">791</a>  |
| Filename in Memory ..... <a href="#">969</a>   | Forward Disconnect Timer (msec) ..... <a href="#">776</a>  |
| filter ..... <a href="#">93</a> , <a href="#">112</a> , <a href="#">124</a> , <a href="#">127</a>  | Forward PMS Message to INTUITY Lodging ..... <a href="#">637</a>   |
| filtering ..... <a href="#">1321</a>   | Forwarded Destination ..... <a href="#">75</a> , <a href="#">891</a> , <a href="#">1086</a>  |
| filtering alarms ..... <a href="#">1100</a>  |  |
| filtering announcements ..... <a href="#">93</a>   |  |
| filtering class of service list ..... <a href="#">112</a>  |  |
| filtering CM access list ..... <a href="#">121</a>   |  |

|  |   |
|--|---|
| Forwarding of voice and multimedia calls ..... | <a href="#">413</a>                       |
| Forwarding voice/multimedia calls .....        | <a href="#">398</a>                       |
| Frames Per Pkt .....                           | <a href="#">677</a>                       |
| Framing Mode .....                             | <a href="#">541</a>                       |
| Frequency .....                                | <a href="#">1033</a>                      |
| FRL .....                                      | <a href="#">482</a> , <a href="#">844</a> |
| FROM / TO .....                                | <a href="#">779</a>                       |
| From IP Address .....                          | <a href="#">675</a>                       |
| Fully Restricted Service .....                 | <a href="#">483</a>                       |

## G

|  |   |
|--|---|
| G3 Version .....                                     | <a href="#">939</a>   |
| G3V4 Adv Route .....                                 | <a href="#">467</a>   |
| G3V4 Enhanced .....                                  | <a href="#">467</a>   |
| Gatekeeper Priority .....                            | <a href="#">683</a>   |
| Gateway .....  | <a href="#">710</a> , <a href="#">712</a> , <a href="#">714</a>   |
| Gateway Node Name .....                              | <a href="#">683</a> , <a href="#">687</a>   |
| General Options .....                                | <a href="#">59</a> , <a href="#">1070</a>   |
| Glare .....  | <a href="#">1026</a>  |
| Glare Handling .....                                 | <a href="#">1012</a>  |
| Global Call Classification .....                     | <a href="#">946</a>   |
| Global Classifier Adjustment (dB) .....              | <a href="#">958</a>   |
| global feature profiles .....                        | <a href="#">1336</a> , <a href="#">1337</a>   |
| Group  |   |
| Attendant Console .....                              | <a href="#">450</a>   |
| Group Control Restrict Activation/Deactivation ..... | <a href="#">564</a>   |
| Group Controlled Restriction .....                   | <a href="#">483</a>   |
| Group Extension .....                                | <a href="#">634</a> , <a href="#">647</a> , <a href="#">667</a> , <a href="#">968</a>   |
| Hunt Group .....                                     | <a href="#">667</a>   |
| Group II Called Party Category .....                 | <a href="#">792</a>   |
| Group II Category For MFC .....                      | <a href="#">483</a>   |
| Group List .....                                     | <a href="#">75</a> , <a href="#">424</a> , <a href="#">425</a> , <a href="#">1086</a>   |
| Group Management .....                               | <a href="#">1161</a>  |
| Group Management page .....                          | <a href="#">1173</a>  |
| Group Member Assignments .....                       | <a href="#">758</a> , <a href="#">828</a> , <a href="#">1039</a>  |
| Group Membership .....                               | <a href="#">76</a> , <a href="#">1087</a>   |
| Group Name .....                                     | <a href="#">459</a> , <a href="#">508</a> , <a href="#">634</a> , <a href="#">647</a> , <a href="#">724</a> , <a href="#">818</a> , <a href="#">983</a>   |
| Coverage Answer Group .....                          | <a href="#">508</a>   |
| Hunt Group .....                                     | <a href="#">647</a>   |
| Group Number .....                                   | <a href="#">508</a> , <a href="#">634</a> , <a href="#">648</a> , <a href="#">667</a> , <a href="#">673</a> , <a href="#">725</a> , <a href="#">786</a> , <a href="#">818</a> , <a href="#">828</a> , <a href="#">860</a> , <a href="#">968</a> , <a href="#">983</a> |
| Coverage Answer Group .....                          | <a href="#">508</a>   |
| Hunt Group .....                                     | <a href="#">648</a> , <a href="#">667</a>   |
| Intercom Group .....                                 | <a href="#">673</a>   |
| Signaling Group .....                                | <a href="#">860</a>   |
| Group Paging Using Speakerphone .....                | <a href="#">633</a> , <a href="#">634</a>   |
| alert .....  | <a href="#">634</a>   |
| Group Timeout (secs) .....                           | <a href="#">634</a>   |
| Group Type .....                                     | <a href="#">648</a> , <a href="#">668</a> , <a href="#">725</a> , <a href="#">736</a> , <a href="#">786</a> , <a href="#">818</a> , <a href="#">860</a> , <a href="#">983</a> , <a href="#">1000</a>  |
| Hunt Group .....                                     | <a href="#">648</a> , <a href="#">668</a>   |

|                                   |   |
|-----------------------------------|---|
| Signaling Group .....             | <a href="#">860</a>                       |
| Group/Port                        |   |
| Announcements/Audio Sources ..... | <a href="#">445</a>                       |
| groups                            |   |
| defined .....                     | <a href="#">76</a> , <a href="#">1087</a> |
| Grp No .....                      | <a href="#">845</a>                       |
| Gtwy to .....                     | <a href="#">835</a>                       |

## H

|   |   |
|---|---|
| H.235 Annex H Required .....                        | <a href="#">860</a>   |
| H.245 DTMF Signal Tone Duration (msec) .....        | <a href="#">860</a>   |
| H.248 Gateways .....                                | <a href="#">682</a>   |
| H.320 Conversion .....                              | <a href="#">71</a> , <a href="#">450</a> , <a href="#">891</a> , <a href="#">1082</a> |
| H.323 IP Endpoints .....                            | <a href="#">694</a>   |
| H.323 Link Bounce Recovery .....                    | <a href="#">694</a>   |
| H.323 Security Procedures .....                     | <a href="#">696</a>   |
| H.323 Station Outgoing Direct Media .....           | <a href="#">860</a>   |
| H0 .....  | <a href="#">757</a> , <a href="#">834</a>   |
| H1 Handover .....                                   | <a href="#">961</a>   |
| H11 .....   | <a href="#">757</a> , <a href="#">834</a>   |
| H12 .....   | <a href="#">758</a> , <a href="#">834</a>   |
| H2 Handover .....                                   | <a href="#">961</a>   |
| Handset Expander Enabled .....                      | <a href="#">966</a>   |
| Harvest Archives page .....                         | <a href="#">1124</a> , <a href="#">1126</a>   |
| Headset .....                                       | <a href="#">74</a> , <a href="#">891</a> , <a href="#">1085</a>                       |
| Hear Zip Tone Following VOA? .....                  | <a href="#">606</a>   |
| Held Call UCID .....                                | <a href="#">754</a>   |
| Hold .....  | <a href="#">400</a>   |
| Hold Time (min) .....                               | <a href="#">786</a>   |
| Hold/Unhold Notifications .....                     | <a href="#">1012</a>  |
| Holiday After Coverage .....                        | <a href="#">508</a>   |
| Holiday Coverage .....                              | <a href="#">508</a>   |
| Holiday Table .....                                 | <a href="#">508</a>   |
| Holidays .....                                      | <a href="#">467</a> , <a href="#">953</a>   |
| Home .....  | <a href="#">891</a>   |
| Hop Lmt .....                                       | <a href="#">845</a>   |
| Hospitality .....                                   | <a href="#">636</a> , <a href="#">946</a>   |
| Hospitality (G3V3 Enhancements) .....               | <a href="#">946</a>   |
| Host .....  | <a href="#">712</a> , <a href="#">714</a>   |
| Hot Desking Enhancement Station Lock .....          | <a href="#">581</a>   |
| HOT LINE DESTINATION .....                          | <a href="#">455</a>   |
| Hour .....  | <a href="#">526</a>   |
| Hourglass Tone .....                                | <a href="#">394</a>   |
| Housekeeper Information Configuration .....         | <a href="#">637</a>   |
| Housekeeping Status (Client Room) Access Code ..... | <a href="#">571</a>   |
| Housekeeping Status (Station) Access Code .....     | <a href="#">571</a>   |
| Howler After Busy .....                             | <a href="#">938</a>   |
| Hundreds Select Button Assignments .....            | <a href="#">452</a>   |
| hunt group .....                                    | <a href="#">645</a>   |
| Hunt Group  |   |

|   |   |   |  |
|---|---|---|--|
| Interruptible Aux Threshold .....               | <a href="#">650</a>   | Incoming .....  | <a href="#">796</a>                        |
| Service Level Target (% in sec) .....           | <a href="#">658</a>   | Incoming Backward Signal Types (Tones to CO) .....            | <a href="#">802</a>                        |
| Hunt Group Busy Activation/Deactivation .....   | <a href="#">564</a>   | Incoming Backward Signal Types (Tones to CO), Group A .....   | <a href="#">802</a>                        |
| Hunt Groups                                     |   | Incoming Backward Signal Types (Tones to CO), Group B .....   | <a href="#">803</a>                        |
| adding announcements .....                      | <a href="#">307</a>   | Incoming Call Handling Treatment .....                        | <a href="#">668</a>                        |
| changing group .....                            | <a href="#">306</a>   | Incoming Call Type .....                                      | <a href="#">792</a>                        |
| dynamic hunt group .....                        | <a href="#">305</a>   | Incoming Calling Number - Delete .....                        | <a href="#">1000</a>                       |
| setting .....                                   | <a href="#">304</a>   | Incoming Calling Number - Format .....                        | <a href="#">727</a> , <a href="#">1000</a> |
| setting queue .....                             | <a href="#">306</a>   | Incoming Calling Number - Insert .....                        | <a href="#">1001</a>                       |
| TTY callers .....                               | <a href="#">307</a>   | Incoming Calling Number Insert .....                          | <a href="#">728</a>                        |
| Hunt Groups using Basic Mode complexes .....    | <a href="#">400</a>   | Incoming Calls  |  |
| Hunt Groups using Enhanced Mode Complexes ..... | <a href="#">414</a>   | Vectors .....   | <a href="#">308</a> , <a href="#">309</a>  |
| Hunt-to Station .....                           | <a href="#">63</a> , <a href="#">892</a> , <a href="#">1074</a> | VDNs .....  | <a href="#">308</a>                        |
| hyperactive registration alarms .....           | <a href="#">705</a>   | ACD   |  |
| Hyperactive Registration Window (minutes) ..... | <a href="#">705</a>   | automatic call distribution .....                             | <a href="#">317</a>                        |
| <hr/>   |   |   |  |
| <b>I</b>  |   | advanced call coverage .....                                  | <a href="#">266</a>                        |
| IAA .....                                       | <a href="#">576</a>   | assigning terminating extension group .....                   | <a href="#">318</a>                        |
| IAS (Branch) .....                              | <a href="#">501</a>   | basic call coverage .....                                     | <a href="#">264</a>                        |
| IAS Att. Access Code .....                      | <a href="#">500</a>   | call forwarding .....   | <a href="#">270</a>                        |
| IAS Tie Trunk Group No. ....                    | <a href="#">501</a>   | call pickup .....   | <a href="#">287</a> , <a href="#">399</a>  |
| ICLID Information                               |   | hunt groups .....   | <a href="#">304</a>                        |
| Displaying .....                                | <a href="#">255</a>   | night service .....   | <a href="#">280</a> , <a href="#">402</a>  |
| ID Range Start/End .....                        | <a href="#">1058</a>  | Incoming Destination .....                                    | <a href="#">985</a>                        |
| Identity Certificates page .....                | <a href="#">46</a>  | Incoming Dial Guard (msec) .....                              | <a href="#">1026</a>                       |
| Identity When Bridging .....                    | <a href="#">604</a>   | Incoming Dial Tone .....                                      | <a href="#">1001</a>                       |
| Idle .....                                      | <a href="#">629</a>   | Incoming Dial Type .....                                      | <a href="#">1001</a>                       |
| Idle Appearance Preference .....                | <a href="#">71</a> , <a href="#">892</a> , <a href="#">1082</a> | Incoming Dialog Loopbacks .....                               | <a href="#">861</a>                        |
| Idle Code .....                                 | <a href="#">541</a> , <a href="#">861</a>                       | incoming digital PPM per country protocol .....               | <a href="#">549</a>                        |
| Idle Traffic Interval (seconds) .....           | <a href="#">694</a>   | Incoming Disconnect (msec) .....                              | <a href="#">1026</a>                       |
| Idle/Active Ringing (Callmaster) .....          | <a href="#">892</a>   | Incoming Disconnect Send (msec) .....                         | <a href="#">1026</a>                       |
| IGAR .....                                      | <a href="#">589</a> , <a href="#">698</a>                       | Incoming Forward Signal Types (Tones from CO) ....            | <a href="#">800</a>                        |
| IGAR Over IP Trunks .....                       | <a href="#">589</a>   | Incoming Forward Signal Types (Tones from CO), Group I .....  | <a href="#">800</a>                        |
| Ignore Connectivity in Server Arbitration ..... | <a href="#">711</a>   | Incoming Forward Signal Types (Tones from CO), Group II ..... | <a href="#">801</a>                        |
| Ignore Network Answer Supervision .....         | <a href="#">933</a>   | Incoming Glare Guard (msec) .....                             | <a href="#">1027</a>                       |
| Ignore Rotary Digits .....                      | <a href="#">893</a>   | Incoming Incomplete Dial Alarm (sec) .....                    | <a href="#">1027</a>                       |
| Immediate .....                                 | <a href="#">507</a> , <a href="#">809</a>                       | Incoming LDN Extension .....                                  | <a href="#">695</a>                        |
| Immediate Access Code .....                     | <a href="#">573</a>   | Incoming Partial Dial (sec) .....                             | <a href="#">1027</a>                       |
| Immediate Redirection on Receipt of PROGRESS    |   | Incoming Rotary Timeout (sec) .....                           | <a href="#">1002</a>                       |
| Inband Information .....                        | <a href="#">930</a>   | Incoming Seizure (msec) .....                                 | <a href="#">1027</a>                       |
| Import Global Settings page .....               | <a href="#">1557</a>  | Incoming Tone (DTMF) ANI .....                                | <a href="#">1013</a>                       |
| Import Groups page .....                        | <a href="#">1183</a>  | Incoming/Outgoing .....                                       | <a href="#">799</a>                        |
| Import Roles – Job Details page .....           | <a href="#">1225</a>  | Incomplete Dial Timer (sec) .....                             | <a href="#">792</a>                        |
| Import Roles page .....                         | <a href="#">1223</a>  | Increasing Text Fields for Feature Buttons .....              | <a href="#">205</a>                        |
| Import Status page .....                        | <a href="#">37</a>  | Increment (Start) .....                                       | <a href="#">528</a>                        |
| Import Users .....                              | <a href="#">35</a> , <a href="#">1553</a>                       | incremental synchronization                                   |  |
| importing groups .....                          | <a href="#">1165</a>  | synchronizing Communication Manager data ....                 | <a href="#">130</a>                        |
| IMS Enabled .....                               | <a href="#">861</a>   |   |  |
| In-VDN Time .....                               | <a href="#">754</a>   |   |  |
| INADS .....                                     | <a href="#">852</a>   |   |  |
| Inc Attd Call Record .....                      | <a href="#">471</a>   |   |  |

|   |   |  |  |
|---|---|--|--|
| Index .....   | <a href="#">829</a>   | Internal Coverage .....                                | <a href="#">784</a>  |
| Individual Attendant Access .....                             | <a href="#">505</a>   | International Access Code .....                        | <a href="#">605</a> , <a href="#">775</a>  |
| Inflow Threshold (sec) .....                                  | <a href="#">655</a>   | International Call Routing .....                       | <a href="#">605</a>  |
| Information Transfer Capability .....                         | <a href="#">846</a>   | International CPN Prefix .....                         | <a href="#">600</a>  |
| Initial IP-IP Direct Media .....                              | <a href="#">862</a>   | Interposition .....                                    | <a href="#">505</a>  |
| initial setup of the Session Manager .....                    | <a href="#">1229</a>  | Interruptible .....                                    | <a href="#">838</a>  |
| initializing synchronization                                  |   | Interruptible Aux Deactivation Threshold (%) .....     | <a href="#">620</a>  |
| synchronizing Communication Manager data .....                | <a href="#">129</a>   | Interruptible Aux Notification Display .....           | <a href="#">620</a>  |
| Insert .....  | <a href="#">464</a> , <a href="#">669</a> , <a href="#">720</a>                       | Interruptible Aux Notification Timer (sec) .....       | <a href="#">620</a>  |
| Call Type Analysis Table .....                                | <a href="#">464</a>   | Interruptible Aux Threshold .....                      | <a href="#">650</a>  |
| Incoming Call Handling Treatment .....                        | <a href="#">669</a>   | INTERVAL 1, 2, 3 .....                                 | <a href="#">972</a>  |
| Insert Digits .....   | <a href="#">1044</a>  | Interval For Applying Periodic Alerting Tone .....     | <a href="#">599</a>  |
| Inserted Digits .....   | <a href="#">845</a>   | Intervening-regions .....                              | <a href="#">699</a>  |
| Install License page .....                                    | <a href="#">1134</a>  | Interworking Feat-flag .....                           | <a href="#">471</a>  |
| Install New Phones .....                                      | <a href="#">167</a>   | Interworking Message .....                             | <a href="#">542</a> , <a href="#">764</a> , <a href="#">862</a>  |
| installing .....  | <a href="#">136</a>   | Interworking with DCS .....                            | <a href="#">955</a>  |
| Installing  |   | Intra-Location .....                                   | <a href="#">537</a>  |
| phone message files .....                                     | <a href="#">257</a>   | Intra-region IP-IP Direct Audio .....                  | <a href="#">690</a>  |
| installing a license file .....                               | <a href="#">1131</a>  | Intra-Switch CDR .....                                 | <a href="#">471</a> , <a href="#">674</a>  |
| Installing Avaya Site Administration .....                    | <a href="#">136</a>   | Intra-System IP DTMF Transmission Mode .....           | <a href="#">706</a>  |
| Installing ESM .....  | <a href="#">379</a>   | Intrusion Tone .....                                   | <a href="#">592</a>  |
| Instance .....  | <a href="#">959</a>   | Invalid Number Dialed .....                            | <a href="#">592</a>  |
| Integrated Announcement Boards .....                          | <a href="#">671</a>   | Invalid Number Dialed Display .....                    | <a href="#">627</a>  |
| Integrated Announcement Extension .....                       | <a href="#">642</a>   | Invalid Number Dialed Intercept Treatment .....        | <a href="#">627</a>  |
| Integrated Announcement Translations .....                    | <a href="#">672</a>   | inventory list .....                                   | <a href="#">127</a>  |
| INTEGRATED CSU OPTIONS .....                                  | <a href="#">555</a>   | inward restriction override .....                      | <a href="#">484</a>  |
| Inter-Exchange Carrier (IXC) Codes .....                      | <a href="#">673</a>   | IP Address .....                                       | <a href="#">460</a> , <a href="#">700</a> , <a href="#">712</a> , <a href="#">714</a> , <a href="#">921</a>  |
| Inter-exchange carrier calls .....                            | <a href="#">324</a>   | Survivable Processor .....                             | <a href="#">921</a>  |
| Inter-Gateway Alternate Routing .....                         | <a href="#">589</a> , <a href="#">695</a>   | IP Address Mapping .....                               | <a href="#">674</a>  |
| Inter-Location .....  | <a href="#">537</a>   | IP Attendant Consoles .....                            | <a href="#">946</a>  |
| Inter-location Loss Group .....                               | <a href="#">778</a>   | IP Audio Hairpinning ....                              | <a href="#">71</a> , <a href="#">452</a> , <a href="#">627</a> , <a href="#">631</a> , <a href="#">690</a> , <a href="#">863</a> , <a href="#">893</a> ,<br><a href="#">1082</a> |
| Inter-PBX Attendant Service (IAS) .....                       | <a href="#">498</a>   | Signaling Group .....                                  | <a href="#">71</a> , <a href="#">863</a> , <a href="#">1082</a>  |
| Inter-region IP-IP Direct Audio .....                         | <a href="#">690</a>   | Station .....  | <a href="#">893</a>  |
| Inter-System IP DTMF Transmission Mode .....                  | <a href="#">706</a>   | IP Codec Set .....                                     | <a href="#">675</a>  |
| Interactions .....  | <a href="#">165</a> , <a href="#">415</a>   | IP Control .....                                       | <a href="#">711</a>  |
| Intercept Treatment .....                                     | <a href="#">402</a>   | IP DTMF transmission mode .....                        | <a href="#">706</a>  |
| Intercept Treatment on Failed Trunk Transfers ....            | <a href="#">607</a> ,<br><a href="#">627</a>  | IP DTMF Transmission Mode .....                        | <a href="#">706</a>  |
| Intercom Group .....  | <a href="#">672</a>   | IP forwarding  |  |
| Interconnect .....  | <a href="#">541</a>   | disabling .....  | <a href="#">134</a>  |
| Interdigit Pause .....  | <a href="#">939</a>   | enabling .....   | <a href="#">134</a>  |
| Interface .....   | <a href="#">542</a> , <a href="#">761</a> , <a href="#">763</a> , <a href="#">862</a> | IP Interfaces .....                                    | <a href="#">682</a>  |
| ISDN BRI Trunk Circuit Pack .....                             | <a href="#">761</a>   | IP network region .....                                | <a href="#">689</a>  |
| Interface Channel .....                                       | <a href="#">835</a> , <a href="#">924</a>   | IP Network Region .....                                | <a href="#">689</a>  |
| Interface Companding .....                                    | <a href="#">542</a> , <a href="#">761</a> , <a href="#">862</a>                       | IP network region page 2 .....                         | <a href="#">695</a>  |
| Interface Link .....  | <a href="#">836</a> , <a href="#">924</a>   | IP Node Names .....                                    | <a href="#">700</a>  |
| Interflow VDN .....   | <a href="#">461</a>   | IP parameter emergency location .....                  | <a href="#">477</a>  |
| Interflow-qpos EWT Threshold .....                            | <a href="#">612</a>   | IP Parameter Emergency Location .....                  | <a href="#">478</a>  |
| Internal Alert .....  | <a href="#">1013</a>  | IP Phone Group ID .....                                | <a href="#">68</a> , <a href="#">893</a> , <a href="#">1079</a>  |
| Internal Auto-Answer of Attd-Extended/Transferred Calls ..... | <a href="#">576</a>   | IP Routing .....                                       | <a href="#">708</a>  |
|   |   | IP Server Interface (IPSI) Administration page 1 ..... | <a href="#">711</a>  |

|   |   |  |   |
|---|---|--|---|
| IP Server Interface Administration .....          | <a href="#">710</a>   | IXC codes .....  | <a href="#">673</a>   |
| IP Services .....                                 | <a href="#">716</a>   | IXC Name .....   | <a href="#">673</a>   |
| IP Softphone .....                                | <a href="#">71</a> , <a href="#">893</a> , <a href="#">1082</a>                       | IXC Prefix .....   | <a href="#">674</a>   |
| IP Softphones .....                               | <a href="#">186</a> , <a href="#">189</a> , <a href="#">942</a>                       |  |   |
| Troubleshooting .....                             | <a href="#">189</a>   | <b>J</b>   |   |
| video capable .....                               | <a href="#">942</a>   | Jack .....   | <a href="#">73</a> , <a href="#">894</a> , <a href="#">1084</a> |
| IP Stations .....                                 | <a href="#">946</a>   | Jitter (ms) .....  | <a href="#">688</a>   |
| IP telephones                                     |   | Job Details page .....                                   | <a href="#">1556</a> , <a href="#">1559</a>                     |
| Changing from dual-connect to single-connect .... | <a href="#">191</a>   | Job Scheduling -Edit Job page .....                      | <a href="#">1331</a>  |
| Setting up emergency calls .....                  | <a href="#">193</a>   | Job Scheduling -On Demand Job page .....                 | <a href="#">1332</a>  |
| IP Telephones .....                               | <a href="#">190</a>   | Job Scheduling -View Job page .....                      | <a href="#">1330</a>  |
| IP Trunks .....                                   | <a href="#">947</a>   | Joining a multimedia conference after T.120 data sharing |   |
| IP Video .....                                    | <a href="#">69</a> , <a href="#">863</a> , <a href="#">893</a> , <a href="#">1080</a> | has been enabled. ....                                   | <a href="#">398</a>   |
| IP Video Softphone .....                          | <a href="#">893</a>   | Journal/Schedule Endpoint .....                          | <a href="#">637</a>   |
| IPEI .....  | <a href="#">893</a>   |  |   |
| IPSI administration .....                         | <a href="#">710</a>   | <b>K</b>   |   |
| IPSI Connection up time .....                     | <a href="#">960</a>   | Keep Held SBA at Coverage Point .....                    | <a href="#">931</a>   |
| IQ (appl ccr) .....                               | <a href="#">617</a>   | Keep-Alive Count .....                                   | <a href="#">694</a>   |
| ISDN Access Code .....                            | <a href="#">564</a>   | Keep-Alive Interval (seconds) .....                      | <a href="#">694</a>   |
| ISDN Caller Disp .....                            | <a href="#">650</a> , <a href="#">968</a>   | KYBD Dialing .....                                       | <a href="#">521</a>   |
| ISDN Feature Plus .....                           | <a href="#">947</a>   |  |   |
| ISDN Network Call Redirection .....               | <a href="#">947</a>   | <b>L</b>   |   |
| ISDN Network Facilities .....                     | <a href="#">812</a>   | Label Language .....                                     | <a href="#">427</a>   |
| ISDN Numbering                                    |   | LABELS FOR 2420/4620 STATIONS .....                      | <a href="#">427</a>   |
| Calling Party Number Conversion for Tandem Calls  |   | LAI .....  | <a href="#">467</a>   |
| .....   | <a href="#">719</a>   | Language translations .....                              | <a href="#">765</a>   |
| ISDN Parameters .....                             | <a href="#">599</a>   | Language Translations                                    |   |
| ISDN Precedence Call Timeout (sec) .....          | <a href="#">809</a>   | Automatic Wakeup .....                                   | <a href="#">765</a>   |
| ISDN Protocol .....                               | <a href="#">418</a>   | button labels .....                                      | <a href="#">766</a>   |
| ISDN Trunk Group .....                            | <a href="#">721</a>   | Enhanced Abbreviated Dialing .....                       | <a href="#">766</a>   |
| ISDN Trunk Groups .....                           | <a href="#">402</a>   | Leave Word Calling .....                                 | <a href="#">766</a>   |
| ISDN-BRI Trunk Circuit Pack .....                 | <a href="#">759</a>   | Malicious Call Trace .....                               | <a href="#">766</a>   |
| TN2185 circuit pack .....                         | <a href="#">759</a>   | miscellaneous call identifiers .....                     | <a href="#">767</a>   |
| ISDN-BRI Trunk Circuit Pack page 2 .....          | <a href="#">763</a>   | Miscellaneous features .....                             | <a href="#">767</a>   |
| ISDN-BRI Trunk Pack                               |   | Property Management Interface .....                      | <a href="#">767</a>   |
| TN556B, TN2198 circuit packs .....                | <a href="#">762</a>   | Self Administration .....                                | <a href="#">768</a>   |
| ISDN-BRI Trunks .....                             | <a href="#">947</a>   | Softkey Labels .....                                     | <a href="#">768</a>   |
| ISDN-PRI .....                                    | <a href="#">947</a>   | Transfer Conference .....                                | <a href="#">768</a>   |
| ISDN-PRI Layer 3 public-access connections .....  | <a href="#">546</a>   | View Buttons .....                                       | <a href="#">769</a>   |
| ISDN-PRI Trunk Group .....                        | <a href="#">351</a>   | Vustats .....  | <a href="#">769</a>   |
| Issue of the Day .....                            | <a href="#">138</a>   | LAR .....  | <a href="#">846</a>   |
| Issue Of The Day .....                            | <a href="#">139</a>   | Last Board Location Saved .....                          | <a href="#">671</a>   |
| Italian DCS Protocol .....                        | <a href="#">609</a>   | Last Number Dialed Access Code .....                     | <a href="#">564</a>   |
| Italian Protocol Enabled .....                    | <a href="#">609</a>   | Layer 1 Stable .....                                     | <a href="#">761</a>   |
| ITC .....   | <a href="#">517</a> , <a href="#">846</a> , <a href="#">986</a>                       | Layer 1 timer .....                                      | <a href="#">938</a>   |
| ITC (Information Transfer Capability) .....       | <a href="#">430</a> , <a href="#">893</a>   | Least Occupied Agent .....                               | <a href="#">951</a>   |
| ITN-C7 Long Timers .....                          | <a href="#">543</a>   | Leave Word Calling .....                                 | <a href="#">766</a>   |
| IXC .....   | <a href="#">846</a>   | Leave Word Calling Cancel A Message .....                | <a href="#">565</a>   |
| IXC Access Number .....                           | <a href="#">673</a>   |  |   |
| IXC Code Format .....                             | <a href="#">673</a>   |  |   |

|   |  |   |  |
|---|--|---|--|
| Leave Word Calling Message Retrieval Lock .....                           | <a href="#">564</a>                        | Local Facility .....                              | <a href="#">707</a>  |
| Leave Word Calling Message Retrieval Unlock .....                         | <a href="#">564</a>                        | Local Facility # .....                            | <a href="#">715</a>  |
| Leave Word Calling Send A Message .....                                   | <a href="#">565</a>                        | Local Information Calls .....                     | <a href="#">326</a>  |
| legal notice .....  | <a href="#">2</a>                          | Local Node .....                                  | <a href="#">717</a> , <a href="#">925</a>  |
| Len .....   | <a href="#">1045</a>                       | Local Node Name .....                             | <a href="#">970</a>  |
| Length .....  | <a href="#">477</a> , <a href="#">1046</a> | Local Node Number .....                           | <a href="#">534</a>  |
| CDR System Parameters .....   | <a href="#">477</a>                        | Local Only .....                                  | <a href="#">921</a>  |
| Length of Dial Code .....   | <a href="#">673</a>                        | Local Port .....                                  | <a href="#">717</a> , <a href="#">926</a>  |
| Length of Time to Remain Connected to Announcement<br><a href="#">643</a> |  | Local Preferred .....                             | <a href="#">922</a>  |
| Level .....   | <a href="#">716</a>                        | Local Survivable Processor .....                  | <a href="#">947</a>  |
| Level 1 Code .....  | <a href="#">603</a>                        | Location .....                                    | <a href="#">60</a> , <a href="#">420</a> , <a href="#">422</a> , <a href="#">464</a> , <a href="#">532</a> , <a href="#">544</a> , <a href="#">691</a> , <a href="#">712</a> , <a href="#">714</a> , <a href="#">761</a> ,<br><a href="#">781</a> , <a href="#">841</a> , <a href="#">894</a> , <a href="#">918</a> , <a href="#">939</a> , <a href="#">973</a> , <a href="#">1071</a> |
| Level 1 Threshold (sec) .....   | <a href="#">655</a>                        | Call Type Digit Analysis Table .....              | <a href="#">464</a>  |
| Level 2 Code .....  | <a href="#">603</a>                        | DS1 Circuit Pack .....                            | <a href="#">544</a>  |
| Level 2 Threshold (sec) .....   | <a href="#">656</a>                        | ISDN BRI Trunk Circuit Pack .....                 | <a href="#">761</a>  |
| Level of Tone Detection .....   | <a href="#">607</a>                        | primary IPSI board .....                          | <a href="#">712</a>  |
| Limit .....   | <a href="#">955</a>                        | secondary IPSI board .....                        | <a href="#">714</a>  |
| Limit Number of Concurrent Calls Activation/<br>Deactivation .....        | <a href="#">565</a>                        | System Parameters Customer Options .....          | <a href="#">939</a>  |
| Limitations .....   | <a href="#">228</a>                        | Location ARS FAC .....                            | <a href="#">321</a>  |
| Line Appearance Conferencing .....  | <a href="#">597</a>                        | location deletion .....                           | <a href="#">1239</a>   |
| Line Coding .....   | <a href="#">543</a>                        | location details .....                            | <a href="#">1240</a>   |
| Line Compensation .....   | <a href="#">544</a>                        | Location for Covered and Forwarded Calls .....    | <a href="#">928</a>  |
| Line Intercept Tone Timer .....   | <a href="#">593</a>                        | Location for Routing Incoming Calls .....         | <a href="#">863</a>  |
| Line Length .....   | <a href="#">1002</a>                       | Location Name .....                               | <a href="#">461</a>  |
| Line Load Control .....   | <a href="#">487</a>                        | Location Parameters .....                         | <a href="#">773</a> , <a href="#">775</a>  |
| Line Load Control Restriction Level .....                                 | <a href="#">810</a>                        | Long Distance Access Code .....                   | <a href="#">775</a>  |
| Lines Per Page .....  | <a href="#">588</a>                        | Off-PBX Feature Name Extension Set .....          | <a href="#">775</a>  |
| Link Failure .....  | <a href="#">701</a> , <a href="#">704</a>  | locations .....                                   | <a href="#">1239</a>   |
| Link Loss Delay Timeout (minutes) .....                                   | <a href="#">701</a>                        | Locations .....                                   | <a href="#">770</a>  |
| Link Loss Delay Timer (minutes) .....                                     | <a href="#">701</a>                        | Lock .....  | <a href="#">461</a> , <a href="#">467</a>  |
| Link Loss Delay Timer (sec) .....   | <a href="#">863</a>                        | Call Vector .....                                 | <a href="#">467</a>  |
| Linkage .....   | <a href="#">509</a>                        | Lock Messages .....                               | <a href="#">60</a> , <a href="#">894</a> , <a href="#">1071</a>  |
| List Number .....   | <a href="#">426</a> , <a href="#">536</a>  | Log CTA/PSA/TTI Transactions in History Log ..... | <a href="#">780</a>  |
| list of XML Schema Definitions and Sample XMLs for<br>bulk Import .....   | <a href="#">1420</a>                       | Log Data Values .....                             | <a href="#">779</a>  |
| list usage extension .....  | <a href="#">92</a>                         | log harvester overview .....                      | <a href="#">1114</a>   |
| List1 .....   | <a href="#">455</a> , <a href="#">520</a>  | Log Harvester page .....                          | <a href="#">1122</a>   |
| List1, List2, List3 .....   | <a href="#">501</a>                        | Log IP Registrations and Events .....             | <a href="#">780</a>  |
| listed directory number (LDN) .....                                       | <a href="#">500</a>                        | log on to System Manager .....                    | <a href="#">19</a>   |
| Listed Directory Numbers .....  | <a href="#">770</a>                        | Log PMS/AD Transactions .....                     | <a href="#">780</a>  |
| Listing MASI Terminals .....  | <a href="#">354</a>                        | log types .....                                   | <a href="#">1101</a>   |
| Loc Number .....  | <a href="#">771</a>                        | Logged-In ACD Agents .....                        | <a href="#">953</a>  |
| Loc Parm .....  | <a href="#">771</a>                        | Logged-In Advocate Agents .....                   | <a href="#">953</a>  |
| Local Agent Preference .....  | <a href="#">651</a>                        | Logged-In IP Softphone Agents .....               | <a href="#">953</a>  |
| Local Call Preference .....   | <a href="#">441</a>                        | logging .....                                     | <a href="#">1101</a>   |
| Local Country Code .....  | <a href="#">605</a>                        | logging all submission failures .....             | <a href="#">780</a>  |
| Local Cvg Subsequent Redirection/CFWD No Ans<br>Interval (rings) .....    | <a href="#">928</a>                        | Logging Configuration page .....                  | <a href="#">1109</a> , <a href="#">1306</a>  |
| Local E.164 Country Code .....  | <a href="#">775</a>                        | logging in .....                                  | <a href="#">133</a>  |
| Local Ext .....   | <a href="#">872</a> , <a href="#">874</a>  | logging in for remote administration .....        | <a href="#">133</a>  |
|   |  | Logging in with Access Security Gateway .....     | <a href="#">137</a>  |
|   |  | Logging in with ASG .....                         | <a href="#">138</a>  |
|   |  | Logging into the system .....                     | <a href="#">133</a>  |

|   |   |   |   |
|---|---|---|---|
| Logging Levels .....                        | <a href="#">779</a>   | manage public contact list .....                              | <a href="#">1655</a>  |
| Logging off the System .....                | <a href="#">140</a>   | manage resources .....  | <a href="#">1186</a>  |
| Logging page .....                          | <a href="#">1104</a>  | Manage Roles .....  | <a href="#">1195</a>  |
| login .....                                 | <a href="#">138</a>   | Manage Roles page .....                                       | <a href="#">1211</a>  |
| Login .....                                 | <a href="#">137</a> , <a href="#">138</a> , <a href="#">556</a> , <a href="#">557</a> , <a href="#">704</a>                       | manage shared address .....                                   | <a href="#">1670</a>  |
| IP Options .....                            | <a href="#">704</a>   | manage users .....  | <a href="#">1389</a>  |
| Login Access Code .....                     | <a href="#">569</a>   | managing application instances .....                          | <a href="#">21</a>  |
| Login Administration .....                  | <a href="#">779</a>   | Managing Displays .....                                       | <a href="#">254</a>   |
| Login ID                                    |   | Managing telephones   |   |
| Agent Login ID .....                        | <a href="#">438</a>   | Gathering necessary information .....                         | <a href="#">168</a>   |
| Login messages .....                        | <a href="#">138</a>   | Manual Unlock allowed .....                                   | <a href="#">972</a>   |
| LoginID for ISDN Display .....              | <a href="#">438</a>   | Manual-In Access Code .....                                   | <a href="#">569</a>   |
| Logins .....                                | <a href="#">140</a>   | Map-to Station .....  | <a href="#">896</a>   |
| Logout .....                                | <a href="#">838</a>   | Mapped String .....   | <a href="#">443</a>   |
| Logout Access Code .....                    | <a href="#">569</a>   | Mapping Mode .....  | <a href="#">895</a> , <a href="#">919</a>   |
| Logout Reason Code Type .....               | <a href="#">438</a> , <a href="#">622</a>   | Marginal / Unacceptable .....                                 | <a href="#">1036</a>  |
| Long Distance Access Code .....             | <a href="#">775</a>   | Marginal Threshold  |   |
| Long Hold Recall Timer .....                | <a href="#">593</a>   | --Dev - 2804 Hz .....   | <a href="#">1036</a>  |
| Long Holding Time (hours) .....             | <a href="#">1013</a>  | --Dev - 404 Hz Loss .....                                     | <a href="#">1036</a>  |
| Look Ahead Routing .....                    | <a href="#">551</a>   | --+Dev - 2804 Hz .....  | <a href="#">1036</a>  |
| Lookahead Interflow .....                   | <a href="#">951</a>   | --+Dev - 404 Hz Loss .....                                    | <a href="#">1036</a>  |
| Loss Group .....                            | <a href="#">65</a> , <a href="#">894</a> , <a href="#">1076</a>   | Max - 1004 Hz Loss .....                                      | <a href="#">1037</a>  |
| Loss of Carrier Disconnect .....            | <a href="#">787</a>   | Maximum C Message Noise .....                                 | <a href="#">1037</a>  |
| Loss Plans .....                            | <a href="#">777</a>   | Maximum C Notched Noise .....                                 | <a href="#">1037</a>  |
| Loudspeaker Paging .....                    | <a href="#">780</a>   | Min -1004 Hz Loss .....                                       | <a href="#">1037</a>  |
| Lower Bound (msec) .....                    | <a href="#">776</a>   | Minimum ERL .....   | <a href="#">1037</a>  |
| LRQ Required .....                          | <a href="#">863</a>   | Minimum SRL-HI .....  | <a href="#">1037</a>  |
| LWC Activation .....                        | <a href="#">71</a> , <a href="#">894</a> , <a href="#">1082</a>   | Minimum SRL-LO .....  | <a href="#">1037</a>  |
| LWC Log External Calls .....                | <a href="#">71</a> , <a href="#">895</a> , <a href="#">1082</a>   | Mark Users as Phone .....                                     | <a href="#">1042</a>  |
| LWC Reception .....                         | <a href="#">65</a> , <a href="#">438</a> , <a href="#">663</a> , <a href="#">895</a> , <a href="#">969</a> , <a href="#">1076</a> | MASI .....  | <a href="#">343</a> , <a href="#">348</a> , <a href="#">356</a> , <a href="#">358</a> , <a href="#">359</a> , <a href="#">362</a> |
| <hr/>                                       |   | MASI Path Parameters .....                                    | <a href="#">351</a>   |
| <b>M</b>                                    |   | MASI Terminals .....  | <a href="#">353</a>   |
| MAC Address .....                           | <a href="#">1060</a>  | Mask CPN/Name for Internal Calls .....                        | <a href="#">487</a>   |
| Mach ID .....                               | <a href="#">529</a> , <a href="#">836</a> , <a href="#">872</a> , <a href="#">874</a>   | Masking CPN/Name Override .....                               | <a href="#">494</a>   |
| Maid status function .....                  | <a href="#">491</a>   | Matching Pattern .....  | <a href="#">422</a> , <a href="#">831</a> , <a href="#">1045</a>  |
| mailbox administration                      |   | Max .....   | <a href="#">420</a> , <a href="#">422</a> , <a href="#">830</a> , <a href="#">831</a> , <a href="#">973</a>                       |
| subscriber management .....                 | <a href="#">102</a>   | Max Message Size to Send .....                                | <a href="#">736</a>   |
| Main Number .....                           | <a href="#">512</a>   | Max NCA TSC .....   | <a href="#">764</a>   |
| Maintain SBA At Principal .....             | <a href="#">931</a>   | Max number of CA TSC .....                                    | <a href="#">864</a>   |
| Maintenance Call Type .....                 | <a href="#">792</a>   | Max number of NCA TSC .....                                   | <a href="#">864</a>   |
| MAINTENANCE PARAMETERS                      |   | Max Ports .....   | <a href="#">1058</a>  |
| DS1 Circuit Pack .....                      | <a href="#">551</a>   | Max# Chan .....   | <a href="#">756</a>   |
| Maintenance Tests .....                     | <a href="#">741</a> , <a href="#">832</a> , <a href="#">1013</a>  | Maximum Administered Ad-hoc Video Conferencing<br>Ports ..... | <a href="#">941</a>   |
| Maintenance-related system parameters ..... | <a href="#">783</a>   | Maximum Administered IP Trunks .....                          | <a href="#">941</a>   |
| Make (msec) .....                           | <a href="#">1034</a>  | Maximum Administered Remote Office Trunks .....               | <a href="#">941</a>   |
| Malicious Call Trace .....                  | <a href="#">402</a> , <a href="#">479</a> , <a href="#">766</a>   | Maximum Administered SIP Trunks .....                         | <a href="#">941</a>   |
| Malicious Call Trace Activation .....       | <a href="#">565</a>   | Maximum Agent Occupancy AUX Reason Code .....                 | <a href="#">623</a>   |
| Malicious Call Trace parameters .....       | <a href="#">948</a>   | Maximum Agent Occupancy Parameters .....                      | <a href="#">622</a>   |
| MALICIOUS CALL TRACE PARAMETERS .....       | <a href="#">589</a>   | Maximum Agent Occupancy Percentage .....                      | <a href="#">623</a>   |
| manage groups .....                         | <a href="#">1161</a>  | Maximum Auto Reserve Agents .....                             | <a href="#">656</a>   |
| manage Presence access control lists .....  | <a href="#">1673</a>  |   |   |

|  |                                      |  |   |
|--|--------------------------------------|--|---|
| Maximum Bandwidth Per Call for Direct-IP Multimedia (units) .....            | <a href="#">680</a>                  | Media Parameters .....                                     | <a href="#">690</a>                     |
| Maximum Bandwidth Per Call for Direct-IP Multimedia (value) .....            | <a href="#">680</a>                  | Media-Gateway .....  | <a href="#">783</a>                     |
| Maximum Concurrently Registered IP eCons .....                               | <a href="#">941</a>                  | Meet-me Conf .....   | <a href="#">468</a>                     |
| Maximum Concurrently Registered IP Stations .....                            | <a href="#">941</a>                  | Meet-me Conference .....                                   | <a href="#">1049</a>                    |
| Maximum Entries .....  | <a href="#">814</a>                  | Meet-me Conference Access Code Change .....                | <a href="#">565</a>                     |
| Maximum G250/G350/G700 VAL Sources .....                                     | <a href="#">941</a>                  | Member Assignment Method .....                             | <a href="#">728</a>                     |
| Maximum Length .....   | <a href="#">600</a>                  | Member Range Allowed .....                                 | <a href="#">668</a>                     |
| Maximum Number of Call Forwarding Hops .....                                 | <a href="#">934</a>                  | Merging extension with TTI .....                           | <a href="#">180</a>                     |
| Maximum Number of Digits for Directed Group Call Pickup .....                | <a href="#">632</a>                  | Message Center .....                                       | <a href="#">664</a>                     |
| Maximum Number of DS1 Boards with Echo Cancellation .....                    | <a href="#">941</a>                  | Message Center AUDIX Name .....                            | <a href="#">664</a>                     |
| Maximum Number of Expanded Meet-me Conference Ports .....                    | <a href="#">942</a>                  | Message Center MSA Name .....                              | <a href="#">664</a>                     |
| Maximum Number of External Calls Logged Per Station .....                    | <a href="#">579</a>                  | message lamp .....   | <a href="#">477</a>                     |
| Maximum Number of Messages Per Station .....                                 | <a href="#">580</a>                  | Message Lamp .....   | <a href="#">478</a>                     |
| Maximum Number of Trunks to Use for IGAR .....                               | <a href="#">695</a>                  | Message Lamp Ext .....                                     | <a href="#">60, 896, 1071</a>           |
| Maximum Off-PBX Telephones .....   | <a href="#">940</a>                  | Message Sequence Trace (MST) Disable .....                 | <a href="#">565</a>                     |
| Maximum Off-PBX Telephones - OPS .....                                       | <a href="#">940</a>                  | Message Server Name .....                                  | <a href="#">896</a>                     |
| Maximum Off-PBX Telephones - PVFMC .....                                     | <a href="#">940</a>                  | Message Waiting .....                                      | <a href="#">402</a>                     |
| Maximum Off-PBX Telephones - SCCAN .....                                     | <a href="#">940</a>                  | Message Waiting Configuration .....                        | <a href="#">638</a>                     |
| Maximum Off-PBX Telephones — PBFMC .....                                     | <a href="#">940</a>                  | Message Waiting Indication for External Calls .....        | <a href="#">580</a>                     |
| Maximum Percentage of Trunks Which Can Be Removed From Service by ATMS ..... | <a href="#">1038</a>                 | Message Waiting Indicator .....                            | <a href="#">896</a>                     |
| Maximum Ports per Expanded Meet-me Conf .....                                | <a href="#">597</a>                  | Message Waiting Lamp Indicates Status For .....            | <a href="#">610</a>                     |
| Maximum Precedence Level .....   | <a href="#">487</a>                  | Message Waiting Type .....                                 | <a href="#">897</a>                     |
| Maximum Resend Requests .....  | <a href="#">793</a>                  | messages .....   | <a href="#">138</a>                     |
| Maximum Size of UUI IE Contents .....  | <a href="#">741</a>                  | messaging class of service .....                           | <a href="#">100</a>                     |
| Maximum Stations .....   | <a href="#">940</a>                  | messaging COS .....  | <a href="#">100</a>                     |
| Maximum Suppression Time .....   | <a href="#">461</a>                  | Messaging Server Name for Messaging .....                  | <a href="#">439</a>                     |
| Maximum time agent in ACW before logout (sec) .....                          | <a href="#">439</a>                  | Metric .....   | <a href="#">710</a>                     |
| Maximum TN2501 VAL Boards .....  | <a href="#">942</a>                  | MF ANI Prefix .....  | <a href="#">483</a>                     |
| Maximum TN2602 Boards with 320 VoIP Channels ....<br><a href="#">942</a>     |                                      | MF Incoming Call Trace .....                               | <a href="#">487</a>                     |
| Maximum TN2602 Boards with 80 VoIP Channels ....<br><a href="#">942</a>      |                                      | MF Interdigit Timer (sec) .....                            | <a href="#">777</a>                     |
| Maximum Video Capable IP Softphones .....                                    | <a href="#">942</a>                  | MF Signaling Intercept Treatment - Incoming .....          | <a href="#">793</a>                     |
| Maximum Video Capable Stations .....   | <a href="#">942</a>                  | MF Signaling Intercept Treatment - Outgoing .....          | <a href="#">793</a>                     |
| Maximum XMOBILE Stations .....   | <a href="#">941</a>                  | MF Tariff Free .....                                       | <a href="#">1014</a>                    |
| Maximum Time Agent in ACW before Logout (sec.) ....<br><a href="#">623</a>   |                                      | MFE Type .....   | <a href="#">793</a>                     |
| MCSNIC .....   | <a href="#">494</a>                  | MGR1 .....   | <a href="#">852</a>                     |
| MCT group extensions, 1 to 100 .....   | <a href="#">558</a>                  | MIA Across Skills .....                                    | <a href="#">439</a>                     |
| MCT Voice Recorder Trunk Group .....   | <a href="#">590</a>                  | MIA Splits or Skills .....                                 | <a href="#">616</a>                     |
| mct-control .....  | <a href="#">558</a>                  | Migrate H.248 MG to primary .....                          | <a href="#">957</a>                     |
| Measured .....   | <a href="#">656, 741, 1013, 1049</a> | Milliseconds Before PMS Link Acknowledgment Timeout .....  | <a href="#">639</a>                     |
| Media Complex Ext .....  | <a href="#">67, 896, 1078</a>        | MIM Mtce/Mgt .....   | <a href="#">525, 897</a>                |
| Media Encryption .....   | <a href="#">677, 864</a>             | MIM Support .....  | <a href="#">515, 525</a>                |
|  |                                      | MIM Support (Management Information Message Support) ..... | <a href="#">897</a>                     |
|  |                                      | Min .....  | <a href="#">420, 422, 830, 831, 973</a> |
|  |                                      | Min# Chan .....  | <a href="#">756</a>                     |
|  |                                      | Minimum Agent-LoginID Password Length .....                | <a href="#">610</a>                     |
|  |                                      | Minimum Digit Length .....                                 | <a href="#">605</a>                     |
|  |                                      | Minimum Station Security Code Length .....                 | <a href="#">853</a>                     |
|  |                                      | Minimum time of network stability .....                    | <a href="#">957</a>                     |
|  |                                      | Minute .....   | <a href="#">526</a>                     |

|   |   |  |  |
|---|---|--|--|
| Miscellaneous Call .....                              | <a href="#">505</a>   | modifying data retention rules .....                   | <a href="#">1299</a> , <a href="#">1311</a>  |
| Miscellaneous features .....                          | <a href="#">767</a>   | modifying dial patterns .....                          | <a href="#">1283</a>   |
| Miscellaneous Parameters .....                        | <a href="#">434</a>   | modifying domains .....                                | <a href="#">1234</a>   |
| Misoperation Alerting .....                           | <a href="#">607</a>   | modifying groups .....                                 | <a href="#">1163</a>   |
| MLPP Service Domain .....                             | <a href="#">487</a>   | modifying locations .....                              | <a href="#">1238</a>   |
| MM (WSM) Route Pattern .....                          | <a href="#">961</a>   | modifying port .....                                   | <a href="#">25</a>   |
| MM Early Answer .....                                 | <a href="#">651</a>   | modifying regular expressions .....                    | <a href="#">1289</a>   |
| MMCH .....  | <a href="#">375</a> , <a href="#">381</a> , <a href="#">383</a> , <a href="#">389</a> , <a href="#">417</a> | modifying routing policies .....                       | <a href="#">1276</a>   |
| MMI Cabling Board .....                               | <a href="#">544</a>   | modifying SIP entities .....                           | <a href="#">1258</a>   |
| MMI Interface .....                                   | <a href="#">545</a>   | modifying the default settings .....                   | <a href="#">1293</a>   |
| Mobile Call (CTI) Extension .....                     | <a href="#">816</a>   | modifying the details of a private contact .....       | <a href="#">1603</a>   |
| Mobility Trunk Group .....                            | <a href="#">897</a>   | modifying the details of a public contact .....        | <a href="#">1656</a> , <a href="#">1660</a>  |
| Mode .....  | <a href="#">836</a> , <a href="#">924</a> , <a href="#">1040</a>  | modifying time ranges .....                            | <a href="#">1271</a>   |
| Survivable Processor .....                            | <a href="#">924</a>   | modifying user account .....                           | <a href="#">1390</a>   |
| Mode Code for Centralized Voice Mail .....            | <a href="#">948</a>   | modifying user roles .....                             | <a href="#">1197</a>   |
| Mode Code Interface .....                             | <a href="#">593</a>   | MOH Group .....  | <a href="#">789</a>  |
| Mode code related system parameters .....             | <a href="#">783</a>   | MOH Group Name .....                                   | <a href="#">790</a>  |
| Mode Codes (From Switch to VMS) .....                 | <a href="#">783</a>   | MOH Source Location .....                              | <a href="#">789</a>  |
| Model .....   | <a href="#">898</a>   | Monitoring MMCH .....                                  | <a href="#">417</a>  |
| Modem   |   | Month .....  | <a href="#">527</a>  |
| Adding .....  | <a href="#">184</a>   | Month (Start) .....                                    | <a href="#">528</a>  |
| Enabling transmission over IP networks .....          | <a href="#">185</a>   | Month (Stop) .....                                     | <a href="#">528</a>  |
| Modem Mode .....                                      | <a href="#">681</a>   | more actions .....                                     | <a href="#">98</a>   |
| Modem Name .....                                      | <a href="#">787</a>   | more actions field description .....                   | <a href="#">93</a>   |
| Modem Pool Group .....                                | <a href="#">785</a>   | More Members Exist .....                               | <a href="#">668</a>  |
| modem pool group number .....                         | <a href="#">786</a>   | More VDN's .....                                       | <a href="#">556</a>  |
| modem pool group type .....                           | <a href="#">786</a>   | Mounting .....   | <a href="#">73</a> , <a href="#">898</a> , <a href="#">1084</a>  |
| Modified Circuit ID Display .....                     | <a href="#">472</a>   | move .....   | <a href="#">91</a>   |
| modify groups .....                                   | <a href="#">1163</a>  | Move Group page .....                                  | <a href="#">1182</a>   |
| Modify Local WebLM page .....                         | <a href="#">1150</a>  | moving an announcement .....                           | <a href="#">91</a>   |
| Modify Tandem Calling Number .....                    | <a href="#">742</a> , <a href="#">1014</a>  | moving announcements .....                             | <a href="#">91</a>   |
| modifying a communication address .....               | <a href="#">1562</a>  | moving groups .....                                    | <a href="#">1165</a>   |
| modifying a contact address of a private contact .... | <a href="#">1608</a>  | Moving telephones .....                                | <a href="#">177</a>  |
| modifying a contact in a contact list .....           | <a href="#">1596</a>  | Moving Telephones .....                                | <a href="#">179</a>  |
| modifying a high priority enforced ACL rule .....     | <a href="#">1675</a>  | MSA Names .....  | <a href="#">460</a>  |
| modifying a local WebLM server configuration .....    | <a href="#">1139</a>  | Multi-switch data collaboration .....                  | <a href="#">398</a> , <a href="#">412</a>  |
| modifying a low priority enforced ACL rule .....      | <a href="#">1676</a>  | Multifrequency Signaling .....                         | <a href="#">948</a>  |
| modifying a messaging profile .....                   | <a href="#">1566</a>  | Multifrequency-Signaling-Related Parameters .          | <a href="#">790</a> , <a href="#">797</a> ,<br><a href="#">799</a> , <a href="#">804</a>   |
| Modifying a policy for Enforced User ACL rules .....  | <a href="#">1681</a>  | Multifrequency-Signaling-Related Parameters page 1 ... | <a href="#">790</a>  |
| modifying a postal address of a private contact ..... | <a href="#">1605</a>  | Multimedia .....                                       | <a href="#">468</a>  |
| modifying a postal address of a public contact .....  | <a href="#">1658</a>  | Multimedia Appl. Server Interface (MASI) .....         | <a href="#">948</a>  |
| modifying a shared address .....                      | <a href="#">1671</a>  | Multimedia Applications Server Interface .....         | <a href="#">340</a>  |
| modifying a station profile .....                     | <a href="#">1569</a>  | Multimedia Call Access Code .....                      | <a href="#">571</a>  |
| modifying a System ACL rule .....                     | <a href="#">1678</a>  | Multimedia Call Handling ....                          | <a href="#">375</a> , <a href="#">377–380</a> , <a href="#">385</a> , <a href="#">387</a> , <a href="#">395</a> ,<br><a href="#">397</a> , <a href="#">398</a> , <a href="#">403</a> , <a href="#">410</a> , <a href="#">411</a> |
| modifying a system rule .....                         | <a href="#">1682</a>  | Multimedia Call Handling (Basic) .....                 | <a href="#">948</a>  |
| modifying a user address .....                        | <a href="#">1400</a>  | Multimedia Call Handling Enhanced .....                | <a href="#">948</a>  |
| modifying Adaptations .....                           | <a href="#">1247</a>  | Multimedia Calling .....                               | <a href="#">340</a> , <a href="#">341</a>  |
| modifying an access point .....                       | <a href="#">23</a>  |  |  |
| modifying an appender .....                           | <a href="#">1111</a> , <a href="#">1302</a>   |  |  |
| modifying an application instance .....               | <a href="#">23</a>  |  |  |

|   |   |   |                   |
|---|---|---|-------------------|
| Multimedia Complex                              | 389, 390, 394–400, 402, 403, 408, 409, 412–415, 417   | IP Node Names                                   | 700               |
| Multimedia Data Conference Activation           | 572   | ISDN BRI Trunk Circuit Pack                     | 761               |
| Multimedia Data Conference Deactivation         | 572   | Signaling Group                                 | 865               |
| Multimedia Early Answer                         | 71, 898, 1083   | Station   | 898               |
| Multimedia IP SIP Trunking                      | 948   | Terminating Extension Group                     | 969               |
| Multimedia Multi-Address Access Code            | 572   | National CPN Prefix                             | 601               |
| Multimedia Parameter Access Code                | 572   | nc Trk Call Splitting                           | 471               |
| Multimedia vectors                              | 414   | NCA-TSC Trunk Member                            | 742               |
| Multinational Locations                         | 948   | Near End Establishes TCP Signaling Socket       | 696               |
| Multiple call appearance operation              | 409   | Near End TCP Port Max                           | 697               |
| Multiple Call Handling                          | 657, 951  | Near End TCP Port Min                           | 697               |
| Multiple Call Handling (Forced)                 | 951   | Near-end CSU                                    | 553               |
| Multiple Level Precedence                       | 488   | Near-end Listen Port                            | 865               |
| Multiple Level Precedence & Preemption (MLPP)   |   | Near-end Node Name                              | 865               |
| Parameters                                      | 808   | Net   | 423, 831, 1045    |
| Multiple Level Precedence and Preemption        | 948   | NET   | 852               |
| Multiple Level Precedence and Preemption (MLPP) | 572   | Net Redir                                       | 462               |
| Multiple Locations                              | 328, 948  | Network (Japan) Needs Connect Before Disconnect | 742               |
| Music (or Silence) On Transferred Trunk Calls   | 576   | Network Bits                                    | 710               |
| Music on Hold                                   | 483   | Network Call Redirection                        | 742, 1014, 1043   |
| Music Source                                    | 963   | Network Call Transfer                           | 865               |
| Music Sources                                   | 811   | network device inventory                        | 126               |
| MUSIC/ANNOUNCEMENTS IP-CODEC                    |   | network device inventory list                   | 126, 128          |
| PREFERENCES                                     | 707   | network discovery                               | 115               |
| Music/Tone on Hold                              | 577   | Network Facilities                              | 812               |
| Mute Button Enabled                             | 72, 898, 1083   | Network Feedback During Tone Detection          | 607               |
| MWI - Number of Digits per Voice Mail           | 600   | Network Level                                   | 603               |
| MWI Served User Type                            | 61, 898, 1072   | Network Management Protocol                     | 554               |
| <hr/>   |   | Network region                                  | 684               |
| <b>N</b>  |   | Network Region                                  | 675, 842          |
| Name  | 430, 432, 439, 450, 455, 456, 468, 508, 514, 517, 545, 556, 635, 668, 673, 689, 700, 758, 761, 770, 772, 812, 827–829, 832, 865, 898, 969, 1040, 1050, 1058 | network subnets                                 | 124               |
| Access Endpoint                                 | 430   | Network uses 1's for Broadnet Addresses         | 684               |
| Administered Connection                         | 432   | New Application Instance page                   | 28                |
| Agent Login ID                                  | 439   | new domains                                     | 1236              |
| Attendant Console                               | 450, 455, 456   | New Group page                                  | 1177, 1190        |
| Call Vector                                     | 468   | New High Priority Enforced User ACL page        | 1689              |
| Coverage Answer Group                           | 508   | New Private Contact List page                   | 1609              |
| CTI Link  | 514   | New Public Contact List page                    | 1665              |
| Data Module                                     | 517   | New Role page                                   | 1213              |
| DS1 Circuit Pack                                | 545   | New System ACL page                             | 1696              |
| Duplicate Vector                                | 556   | New System Rule page                            | 1701              |
| Group Paging Using Speakerphone                 | 635   | New User Profile page                           | 1586, 1633        |
| Holiday Table                                   | 635   | Next ANI Digit                                  | 796               |
| Hunt Group                                      | 668   | Next Path Number                                | 509               |
| Intercom Group                                  | 673   | Night   | 758, 1041         |
| IP Network Region                               | 689   | night bells                                     | 568               |
|   |   | Night Destination                               | 770, 963          |
|   |   | Night Serv                                      | 670               |
|   |   | Night Service                                   | 280, 282–286, 986 |
|   |   | external alerting                               | 284               |

|  |  |   |  |
|--|--|---|--|
| LDN calls .....                                      | <a href="#">285</a>  | Number of Pings Per Measurement Interval .....      | <a href="#">703</a>                        |
| setting external alerting .....                      | <a href="#">284</a>  | Number of Recordings .....                          | <a href="#">671</a>                        |
| setting hunt groups .....                            | <a href="#">286</a>  | Number of Registrations within the Window .....     | <a href="#">705</a>                        |
| setting night console service .....                  | <a href="#">282</a>  | Number of Rings .....                               | <a href="#">509</a>                        |
| setting night station service .....                  | <a href="#">282</a>  | Numbering — Public/Unknown Format .....             | <a href="#">814</a>                        |
| setting trunk answer .....                           | <a href="#">283</a>  | Numbering Format .....                              | <a href="#">742</a> , <a href="#">847</a>  |
| setting trunk group .....                            | <a href="#">285</a>  | Numbering-Private Format .....                      | <a href="#">813</a>                        |
| setting up service to voice mail .....               | <a href="#">280</a>  | NxDS0 .....   | <a href="#">758</a>                        |
| Night Service Act. Ext. ....                         | <a href="#">501</a>  | NXDS0 .....   | <a href="#">834</a>                        |
| Night Service Destination .....                      | <a href="#">651</a>  |   |  |
| Night Service Disconnect Timer .....                 | <a href="#">593</a>  | <b>O</b>  |  |
| No Answer Timeout (sec) .....                        | <a href="#">502</a>  | Object .....  | <a href="#">716</a>                        |
| No Dial Tone Conferencing .....                      | <a href="#">597</a>  | Observe an Agent Answer .....                       | <a href="#">1053</a>                       |
| No Hold Conference Timeout .....                     | <a href="#">597</a>  | obtaining the license file .....                    | <a href="#">1130</a>                       |
| No Service Time Out Interval .....                   | <a href="#">961</a>  | Off .....   | <a href="#">784</a>                        |
| No-cadence call classification modes and End OCM     |  | Off Premises Station .....                          | <a href="#">899</a>                        |
| timer .....  | <a href="#">339</a>  | Off-Hook Alert .....                                | <a href="#">492</a>                        |
| setting up announcement extension .....              | <a href="#">339</a>  | Off-Net Cvg Subsequent Redirection/CFWD No Ans      |  |
| setting up End OCM timer .....                       | <a href="#">339</a>  | Interval (rings) .....                              | <a href="#">929</a>                        |
| setting up no-cadence call classification modes .... | <a href="#">339</a>  | Off-PBX Feature Name Extension Set .....            | <a href="#">775</a>                        |
| No. Del. Digits .....                                | <a href="#">847</a>  | Off-PBX telephone configuration set .....           | <a href="#">494</a>                        |
| No. Dgts Subaddress .....                            | <a href="#">847</a>  | Off-PBX telephone feature name extensions .....     | <a href="#">558</a>                        |
| No. of Calls .....                                   | <a href="#">840</a>  | Off-PBX Telephone Mobile Feature Extensions .....   | <a href="#">816</a>                        |
| Node Name .....                                      | <a href="#">684</a> , <a href="#">688</a> , <a href="#">842</a> , <a href="#">922</a>  | Off-PBX telephone station-mapping .....             | <a href="#">916</a>                        |
| Survivable Processor .....                           | <a href="#">922</a>  | Off-Premises Tone Detect Timeout Interval .....     | <a href="#">577</a>                        |
| Node Num .....                                       | <a href="#">1045</a>   | On-hook Dialing on 607/2400/4600/6400/8400          |  |
| Node Number .....                                    | <a href="#">421</a> , <a href="#">813</a>  | Terminals .....                                     | <a href="#">607</a>                        |
| Node Number (Local PBX ID) .....                     | <a href="#">472</a>  | One-Step Recording .....                            | <a href="#">598</a>                        |
| Node Number Routing .....                            | <a href="#">813</a>  | operator assisted calls .....                       | <a href="#">324</a>                        |
| non-station objects; view                            |  | Originating Auto Restoration .....                  | <a href="#">833</a>                        |
| Communication Manager objects; view .....            | <a href="#">83</a>   | Originating Extension .....                         | <a href="#">512</a> , <a href="#">850</a>  |
| Normal Outgoing Seize Send (msec) .....              | <a href="#">1028</a>   | Originating multimedia calls .....                  | <a href="#">390</a>                        |
| NPA .....  | <a href="#">772</a> , <a href="#">847</a>  | Originating Multimedia calls .....                  | <a href="#">403</a>                        |
| Num  |  | Originating voice calls .....                       | <a href="#">389</a>                        |
| Best Service Routing .....                           | <a href="#">462</a>  | Originator .....                                    | <a href="#">432</a>                        |
| Number .....   | <a href="#">462</a> , <a href="#">468</a> , <a href="#">635</a> , <a href="#">829</a> , <a href="#">853</a> , <a href="#">1050</a> | Other considerations .....                          | <a href="#">414</a>                        |
| Best Service Routing .....                           | <a href="#">462</a>  | Other LAI Information .....                         | <a href="#">755</a>                        |
| Call Vector .....                                    | <a href="#">468</a>  | Other Related Parameters .....                      | <a href="#">784</a>                        |
| Holiday Table .....                                  | <a href="#">635</a>  | Other Stations When Call Is Active .....            | <a href="#">629</a>                        |
| Service Hours Table .....                            | <a href="#">853</a>  | Other Stations When Call Is Put On-Hold .....       | <a href="#">629</a>                        |
| Number Format .....                                  | <a href="#">721</a>  | Outg Attd Call Record .....                         | <a href="#">472</a>                        |
| Number of Codes Administered .....                   | <a href="#">460</a>  | Outg Trk Call Splitting .....                       | <a href="#">472</a>                        |
| Number of Digits from PMS .....                      | <a href="#">643</a>  | Outgoing .....                                      | <a href="#">796</a>                        |
| Number of Digits in PMS Coverage Path .....          | <a href="#">643</a>  | Outgoing ANI .....                                  | <a href="#">743</a> , <a href="#">1015</a> |
| Number of Emergency Calls Allowed in Attendant Queue |  | Outgoing Backward Signal Types (Tones from CO) .... |  |
| .....  | <a href="#">585</a>  | .....   | <a href="#">805</a>                        |
| Number of Housekeeper ID Digits .....                | <a href="#">638</a>  | Outgoing Backward Signal Types (Tones from CO),     |  |
| Number of Incoming ANI Digits .....                  | <a href="#">797</a>  | Group A .....                                       | <a href="#">805</a>                        |
| Number of Members .....                              | <a href="#">728</a> , <a href="#">987</a>  | Outgoing Backward Signal Types (Tones from CO),     |  |
| Number of Outgoing ANI Digits .....                  | <a href="#">797</a>  | Group B .....                                       | <a href="#">807</a>                        |
|  |  | Outgoing Call Type .....                            | <a href="#">794</a>                        |

|   |   |   |  |
|---|---|---|--|
| Outgoing Channel ID Encoding .....                          | <a href="#">743</a>   | Pass Prefixed CPN to ASAI .....                     | <a href="#">601</a>  |
| Outgoing Dial Guard (msec) .....                            | <a href="#">1028</a>  | Passphrase .....                                    | <a href="#">865</a>  |
| Outgoing Dial Type .....                                    | <a href="#">824</a> , <a href="#">1002</a>                      | Password .....                                      | <a href="#">440</a> , <a href="#">556</a> , <a href="#">557</a> , <a href="#">704</a> , <a href="#">706</a> , <a href="#">719</a>  |
| Outgoing Disconnect (msec) .....                            | <a href="#">1028</a>  | Agent Login ID .....                                | <a href="#">440</a>  |
| Outgoing Disconnect Send (msec) .....                       | <a href="#">1028</a>  | IP Options .....                                    | <a href="#">704</a> , <a href="#">706</a>  |
| Outgoing Display .....                                      | <a href="#">728</a> , <a href="#">820</a> , <a href="#">987</a> | Password (enter again)                              |  |
| Outgoing End of Dial (sec) .....                            | <a href="#">1029</a>  | Agent Login ID .....                                | <a href="#">440</a>  |
| Outgoing Forward Signal Absent Timer (sec) .....            | <a href="#">794</a>   | Password to Change COR by FAC .....                 | <a href="#">626</a>  |
| Outgoing Forward Signal Present Timer (sec) .....           | <a href="#">794</a>   | PASTE (Display PBX Data on telephone) .....         | <a href="#">484</a>  |
| Outgoing Forward Signal Types (Tones to CO) .....           | <a href="#">804</a>   | PASTE (Display PBX Data) .....                      | <a href="#">951</a>  |
| Outgoing Forward Signal Types (Tones to CO), Group I .....  | <a href="#">804</a>   | PASTE Access Code .....                             | <a href="#">565</a>  |
| Outgoing Forward Signal Types (Tones to CO), Group II ..... | <a href="#">805</a>   | Path Replacement .....                              | <a href="#">750</a>  |
| Outgoing Glare Guard (msec) .....                           | <a href="#">1029</a>  | Path Replacement Method .....                       | <a href="#">743</a> , <a href="#">750</a> , <a href="#">1015</a>   |
| Outgoing II by COR .....                                    | <a href="#">798</a>   | Path Replacement While in Queue/Vectoring .....     | <a href="#">601</a>  |
| Outgoing Last Digit (sec) .....                             | <a href="#">1029</a>  | Path Replacement with Measurements .....            | <a href="#">601</a>  |
| Outgoing Rotary Dial Interdigit (msec) .....                | <a href="#">1030</a>  | Path Replacement with Retention .....               | <a href="#">750</a> , <a href="#">1015</a>   |
| Outgoing Seizure (msec) .....                               | <a href="#">1030</a>  | Pattern Choices .....                               | <a href="#">842</a>  |
| Outgoing Seizure Response (sec) .....                       | <a href="#">1030</a>  | pattern list .....                                  | <a href="#">1286</a>   |
| Outgoing Shuttle Exchange Cycle Timer (sec) .....           | <a href="#">777</a>   | Pattern Name .....                                  | <a href="#">848</a>  |
| Outgoing Start Timer (sec) .....                            | <a href="#">794</a>   | Pattern Number .....                                | <a href="#">848</a>  |
| Outgoing Trunk Alerting Timer .....                         | <a href="#">487</a>   | Pause (msec) .....                                  | <a href="#">512</a> , <a href="#">753</a> , <a href="#">1032</a>   |
| Outgoing Trunk Disconnect Timer .....                       | <a href="#">488</a> , <a href="#">489</a>                       | Pause Duration .....                                | <a href="#">875</a>  |
| Outpulse Without Tone .....                                 | <a href="#">607</a>   | PBX ID .....  | <a href="#">1016</a>   |
| Outpulsing Information .....                                | <a href="#">1033</a>  | PC Non-Predictive Reports Skill .....               | <a href="#">620</a>  |
| Overlap Sending on Link-to-Link Tandem Calls .....          | <a href="#">794</a>   | PCOL/TEG Call Alerting .....                        | <a href="#">899</a>  |
| Overuse page .....  | <a href="#">1159</a>  | Peer Protocol .....                                 | <a href="#">545</a>  |
| overview  |   | Pending Jobs page .....                             | <a href="#">1325</a>   |
| Session Manager routing .....                               | <a href="#">1227</a>  | Per Button Ring Control .....                       | <a href="#">72</a> , <a href="#">899</a> , <a href="#">1083</a>  |
| Overview  |   | Per Call CPN Blocking Code .....                    | <a href="#">744</a> , <a href="#">1016</a>   |
| Communication Manager capabilities overview .....           | <a href="#">48</a>  | Per Call CPN Blocking Code Access Code .....        | <a href="#">565</a>  |
| System Manager; overview .....                              | <a href="#">48</a>  | Per Call CPN Unblocking Code .....                  | <a href="#">744</a> , <a href="#">1016</a>   |
| overview of SIP entity references .....                     | <a href="#">1266</a>  | Per Call CPN Unblocking Code Access Code .....      | <a href="#">565</a>  |
| Overview timer to Group Queue .....                         | <a href="#">503</a>   | Per Call CPN/BN .....                               | <a href="#">670</a>  |
|   |   | Per Station CPN - Send Calling Number .....         | <a href="#">62</a> , <a href="#">900</a> , <a href="#">1073</a>  |
|   |   | Percent Full .....                                  | <a href="#">421</a> , <a href="#">423</a> , <a href="#">532</a> , <a href="#">830</a> , <a href="#">973</a> , <a href="#">1045</a> |
|   |   | Performing backups .....                            | <a href="#">144</a>  |
|   |   | Period .....  | <a href="#">829</a>  |
|   |   | Periodic Registration Timer (min) .....             | <a href="#">702</a>  |
|   |   | Periodic Status .....                               | <a href="#">1158</a>   |
|   |   | Permanently Disable .....                           | <a href="#">840</a>  |
|   |   | Permit Mismatch .....                               | <a href="#">523</a>  |
|   |   | Personal CO Line Group .....                        | <a href="#">817</a> , <a href="#">826</a> , <a href="#">827</a>  |
|   |   | Personal List .....                                 | <a href="#">74</a> , <a href="#">425</a> , <a href="#">426</a> , <a href="#">1085</a>  |
|   |   | Personal Station Access (PSA) .....                 | <a href="#">493</a> , <a href="#">948</a>  |
|   |   | Personal Station Access (PSA) Associate Code .....  | <a href="#">565</a>  |
|   |   | Personal Station Access (PSA) Dissociate Code ..... | <a href="#">566</a>  |
|   |   | Personalized Ringing Pattern .....                  | <a href="#">62</a> , <a href="#">899</a> , <a href="#">1074</a>  |
|   |   | PGN # .....   | <a href="#">971</a>  |
|   |   | PGN 1 (through PGN 8) .....                         | <a href="#">816</a>  |
|   |   | PGN/TN/COR for Covered and Forwarded Calls .....    | <a href="#">929</a>  |

## P

|  |   |
|--|---|
| PA (Percent Allocation) .....                                    | <a href="#">441</a>                       |
| Packet loss (%) .....  | <a href="#">688</a>                       |
| Packet Loss (%) .....  | <a href="#">703</a>                       |
| Packet Resp Timer .....  | <a href="#">718</a> , <a href="#">927</a> |
| Packet Size (ms) .....   | <a href="#">678</a>                       |
| Pager Number .....   | <a href="#">512</a>                       |
| Parameters for creating QSIG selection numbers .....             | <a href="#">603</a>                       |
| Parameters for Media Gateway Alarms .....                        | <a href="#">705</a>                       |
| Parameters for Network Region Registration (NR-REG) Alarms ..... | <a href="#">705</a>                       |
| Parity .....   | <a href="#">523</a>                       |
| Partition Routing Table .....                                    | <a href="#">816</a>                       |
| Partitioned Group Number .....                                   | <a href="#">484</a> , <a href="#">813</a> |

|   |   |   |   |
|---|---|---|---|
| Phantom Calls .....   | <a href="#">954</a>   | Port Extension  |   |
| Phone message file loads  |   | Agent Login ID .....  | <a href="#">440</a>   |
| Checking the status .....   | <a href="#">258</a>   | Port Network Support .....  | <a href="#">949</a>   |
| Phone message files   |   | Port Pair Assignments .....   | <a href="#">789</a>   |
| obtaining and installing .....  | <a href="#">257</a>   | Post Connect Dialing Options .....                                      | <a href="#">497</a>   |
| phone number .....  | <a href="#">916</a>   | Posted Messages .....   | <a href="#">566</a> , <a href="#">949</a>                       |
| Phone Number  |   | Posting a message .....   | <a href="#">143</a>   |
| Stations With Off-PBX Telephone Integration .....   | <a href="#">917</a>   | PPM .....   | <a href="#">1034</a>  |
| Physical Installation .....   | <a href="#">378</a>   | PPM per country protocol .....  | <a href="#">549</a>   |
| Pickup Group .....  | <a href="#">292-294</a> , <a href="#">828</a>                   | PPS .....   | <a href="#">1034</a>  |
| deleting pickup groups .....  | <a href="#">294</a>   | Precedence Call Timeout (sec) .....                                     | <a href="#">810</a>   |
| getting list of extended groups .....   | <a href="#">292</a> , <a href="#">293</a>                       | Precedence Call Waiting .....   | <a href="#">72</a> , <a href="#">901</a> , <a href="#">1083</a> |
| removing from extended pickup group .....   | <a href="#">292</a> , <a href="#">293</a>                       | Precedence Calling Access Code .....                                    | <a href="#">572</a>   |
| Pickup Group Number .....   | <a href="#">557</a>   | Precedence Calling-Dialed Digit Assignment .....                        | <a href="#">808</a>   |
| Pickup Number .....   | <a href="#">557</a>   | Precedence Incoming .....   | <a href="#">1016</a>  |
| Pickup Numbers .....  | <a href="#">297</a>   | Precedence Outgoing .....   | <a href="#">1016</a>  |
| Pickup on Transfer .....  | <a href="#">630</a>   | Precedence Routing Digit Analysis Table .....                           | <a href="#">830</a>   |
| PIN Checking for Private Calls .....  | <a href="#">566</a> , <a href="#">632</a>                       | Precedence Routing Digit Conversion Table .....                         | <a href="#">831</a>   |
| Pin Number .....  | <a href="#">513</a>   | Preempt Emergency Call .....  | <a href="#">810</a>   |
| Ping Test Interval (sec) .....  | <a href="#">703</a>   | Preempt Method .....  | <a href="#">830</a>   |
| pings per measurement interval .....  | <a href="#">703</a>   | Preemptable .....   | <a href="#">488</a>   |
| Plan # .....  | <a href="#">756</a>   | Prefer use of G.711 by Announcement Sources .....                       | <a href="#">708</a>   |
| Planning .....  | <a href="#">380</a>   | Prefer use of G.711 by IP Endpoints Listening to<br>Announcements ..... | <a href="#">708</a>   |
| Platform  |   | Prefer use of G.711 by IP Endpoints Listening to Music<br>.....         | <a href="#">708</a>   |
| System Parameters Customer Options .....  | <a href="#">941</a>   | Prefer use of G.711 by Music Sources .....                              | <a href="#">705</a> , <a href="#">708</a>                       |
| Platform Maximum Ports .....  | <a href="#">941</a>   | Preferred Minimum Session Refresh Interval (sec) ....                   | <a href="#">1003</a>  |
| PMS Endpoint .....  | <a href="#">639</a>   | Prefix .....  | <a href="#">772</a>   |
| PMS Link Maximum Retransmission Requests .....  | <a href="#">638</a>   | Prefix Mark .....   | <a href="#">848</a>   |
| PMS Link Maximum Retransmissions .....  | <a href="#">638</a>   | Prefix-1 .....  | <a href="#">825</a> , <a href="#">987</a>                       |
| PMS Log Endpoint .....  | <a href="#">638</a>   | Preinstallation tasks for firmware download .....                       | <a href="#">197</a>   |
| PMS Protocol Mode .....   | <a href="#">639</a>   | Prepend "+" to Calling Number .....                                     | <a href="#">1043</a>  |
| PMS Sends Prefix .....  | <a href="#">643</a>   | Prerequisites .....   | <a href="#">341</a>   |
| PN  |   | Presence ACL page .....   | <a href="#">1685</a>  |
| system parameters port networks .....   | <a href="#">960</a>   | Prgm Group List Access Code .....                                       | <a href="#">559</a>   |
| PN Cold Reset Delay Timer (sec) .....   | <a href="#">961</a>   | PRI Endpoint .....  | <a href="#">832</a>   |
| PNC duplication .....   | <a href="#">956</a>   | Primary   |   |
| PNC Duplication .....   | <a href="#">948</a>   | Hunt Group .....  | <a href="#">665</a>   |
| Point1, Point2, ... ..  | <a href="#">510</a>   | Primary D Channel .....   | <a href="#">866</a>   |
| Policy Routing Table .....  | <a href="#">828</a>   | Primary IPSI .....  | <a href="#">711</a>   |
| Port ... <a href="#">58</a> , <a href="#">450</a> , <a href="#">478</a> , <a href="#">514</a> , <a href="#">517</a> , <a href="#">577</a> , <a href="#">759</a> , <a href="#">761</a> , <a href="#">764</a> , <a href="#">781</a> , <a href="#">900</a> , |   | PRIMARY LEVELS .....  | <a href="#">967</a>   |
| <a href="#">1041</a> ,  | <a href="#">1069</a>  | Primary Output Endpoint .....   | <a href="#">472</a>   |
| Attendant Console .....   | <a href="#">450</a>   | Primary Output Format .....   | <a href="#">473</a>   |
| Change Station Extension .....  | <a href="#">478</a>   | Primary Search Time (seconds) .....                                     | <a href="#">702</a>   |
| CTI Link .....  | <a href="#">514</a>   | Priority .....  | <a href="#">435</a> , <a href="#">507</a> , <a href="#">810</a> |
| Data Module .....   | <a href="#">517</a>   | Priority Access Code .....  | <a href="#">573</a>   |
| Feature-Related System Parameters .....   | <a href="#">577</a>   | Priority Calling .....  | <a href="#">493</a>   |
| Station .....   | <a href="#">58</a> , <a href="#">900</a> , <a href="#">1069</a> | Priority Calling Access Code .....                                      | <a href="#">566</a>   |
| Port # .....  | <a href="#">707</a> , <a href="#">716</a>                       | Priority Factory Number .....   | <a href="#">1058</a>  |
| IP Options .....  | <a href="#">707</a>   |   |   |
| Port Board Security .....   | <a href="#">852</a>   |   |   |
| Port Board Security Notification Interval .....   | <a href="#">852</a>   |   |   |



|   |   |  |   |
|---|---|--|---|
| Record Agent ID on Incoming .....   | <a href="#">473</a>   | Remove # From Called Number .....  | <a href="#">474</a>                         |
| Record Agent ID on Outgoing .....   | <a href="#">473</a>   | Remove Agent Skill Access Code .....   | <a href="#">570</a>                         |
| Record Call-Assoc TSC .....   | <a href="#">474</a>   | Remove Inactive BCMS/VuStats Agents .....                                    | <a href="#">619</a>                         |
| Record Called Vector Directory Number Instead of Group<br>or Member .....   | <a href="#">474</a>   | removing a local WebLM server .....  | <a href="#">1139</a>                        |
| Record Length .....   | <a href="#">477</a>   | removing a mailing address .....   | <a href="#">1401</a>                        |
| Record Non-Call-Assoc TSC .....   | <a href="#">474</a>   | removing a user from groups .....  | <a href="#">1397</a>                        |
| Record Outgoing Calls Only .....  | <a href="#">474</a>   | removing an appender from a logger .....                                     | <a href="#">1111</a> , <a href="#">1302</a> |
| Recording Delay Timer .....   | <a href="#">599</a>   | removing an association between a station and a user<br>.....                | <a href="#">1569</a>                        |
| Recovery Rule Number .....  | <a href="#">957</a>   | removing an association between a subscriber and a<br>user .....             | <a href="#">1566</a>                        |
| Redirect Notification .....   | <a href="#">72</a> , <a href="#">901</a> , <a href="#">1083</a>                       | removing assigned applications .....   | <a href="#">24</a>                          |
| Redirect on IP/OPTIM Failure to VDN .....   | <a href="#">661</a>   | removing assigned resources from a group .....                               | <a href="#">1173</a>                        |
| Redirect on No Answer (rings) .....   | <a href="#">662</a>   | removing attributes from a permission .....                                  | <a href="#">1210</a>                        |
| Redirect on No Answer to VDN .....  | <a href="#">662</a>   | removing groups and resources from a permission ....<br><a href="#">1209</a> |   |
| Redirect on OPTIM failure .....   | <a href="#">1004</a>  | removing license file .....  | <a href="#">1133</a>                        |
| Redirected Call .....   | <a href="#">505</a>   | removing permissions from a role .....                                       | <a href="#">1208</a>                        |
| Redirected DID Call .....   | <a href="#">506</a>   | removing roles .....   | <a href="#">1395</a>                        |
| Redundancy .....  | <a href="#">681</a>   | removing subnets .....   | <a href="#">120</a>                         |
| Referral Destination .....  | <a href="#">850</a>   | Removing telephones .....  | <a href="#">183</a>                         |
| Refresh MW Lamp .....   | <a href="#">784</a>   | removing trusted certificates .....  | <a href="#">41</a>                          |
| Refresh Terminal Parameters Access Code .....   | <a href="#">567</a>   | removing user account .....  | <a href="#">1392</a>                        |
| Region .....  | <a href="#">689</a>   | removing users from roles .....  | <a href="#">1200</a> , <a href="#">1399</a> |
| registration alarms .....   | <a href="#">705</a>   | repairing a replica node .....   | <a href="#">1313</a>                        |
| regular expression deletion .....   | <a href="#">1290</a>  | Repetitive Call Waiting Interval (sec) .....                                 | <a href="#">608</a>                         |
| regular expression details .....  | <a href="#">1291</a>  | Repetitive Call Waiting Tone .....   | <a href="#">608</a>                         |
| regular expression list .....   | <a href="#">1292</a>  | Replace Identity Certificate page .....                                      | <a href="#">47</a>                          |
| regular expressions .....   | <a href="#">1291</a>  | Replace Restricted Numbers .....   | <a href="#">744</a>                         |
| Rel .....   | <a href="#">956</a>   | Replace Unavailable Numbers .....  | <a href="#">744</a> , <a href="#">1017</a>  |
| Related screens .....   | <a href="#">381</a>   | Replacement String .....   | <a href="#">423</a> , <a href="#">831</a>   |
| related topics .....  | <a href="#">142</a>   | replacing identity certificate .....   | <a href="#">42</a>                          |
| Release Ack Send (msec) .....   | <a href="#">1031</a>  | Replica Groups page .....  | <a href="#">1315</a>                        |
| Reliable Protocol .....   | <a href="#">718</a> , <a href="#">927</a>   | Replica Nodes page .....   | <a href="#">1315</a>                        |
| Remote Access .....   | <a href="#">402</a> , <a href="#">838</a>   | Reporting for PC Non-Predictive Calls .....                                  | <a href="#">621</a>                         |
| Remote Access Dial Tone .....   | <a href="#">840</a>   | Request Call Category at Start of Call .....                                 | <a href="#">798</a>                         |
| Remote Access Extension .....   | <a href="#">840</a>   | Request Category .....   | <a href="#">1018</a>                        |
| remote administration .....   | <a href="#">133</a>   | Request CPN at Start of Call .....   | <a href="#">798</a>                         |
| Remote Attendant Route String .....   | <a href="#">810</a>   | Request Incoming ANI (non-AAR/ARS) .....                                     | <a href="#">795</a>                         |
| Remote Call Coverage Table .....  | <a href="#">841</a>   | Reserved Slots for Attendant Priority Queue .....                            | <a href="#">585</a>                         |
| Remote Logout of Agent .....  | <a href="#">488</a>   | Reset Shift Timer .....  | <a href="#">594</a>                         |
| Remote Logout of Agent Access Code .....  | <a href="#">570</a>   | Resource page  |   |
| Remote Loop-Around Test .....   | <a href="#">518</a>   | search resource .....  | <a href="#">1184</a>                        |
| Remote Node .....   | <a href="#">717</a> , <a href="#">926</a>   | Resource Synchronization page .....  | <a href="#">1183</a>                        |
| Remote Office .....   | <a href="#">193</a> , <a href="#">841</a> , <a href="#">867</a> , <a href="#">949</a> | Resources page   |   |
| Remote Office Phone .....   | <a href="#">901</a>   | search resource .....  | <a href="#">1192</a>                        |
| remote office trunks .....  | <a href="#">941</a>   | Restart ANI from Caller Category .....                                       | <a href="#">799</a>                         |
| Remote Port .....   | <a href="#">717</a> , <a href="#">926</a>   | restore .....  | <a href="#">90</a>                          |
| Remote Send All Calls .....   | <a href="#">567</a>   | Restore page .....   | <a href="#">1305</a>                        |
| Remote Softphone Emergency Calls ....<br><a href="#">63</a> , <a href="#">453</a> , <a href="#">902</a> ,<br><a href="#">1074</a> |   | restoring a system backup from a local machine ....<br><a href="#">1299</a>  |   |
| Remote VMS Extensions - Second .....  | <a href="#">784</a>   |  |   |
| Remote VMS Extensions- First .....  | <a href="#">784</a>   |  |   |



|  |  |
|--|--|
| SAC/CF Override Protection for Priority Call and Dialing<br>490          | Attendant Console .....451   |
| SAC/CF Override Protection for Team Btn .....490                         | Security Code for Terminal Self Administration Required<br>853       |
| save .....88   | Security violation notification .....850, 853                        |
| save translations .....144   | Security violation notification parameters .....850, 851             |
| saving an announcement .....88   | Seize Ack Delay (msec) .....1031                                     |
| saving announcements .....88   | Seize Ack Send (msec) .....1032                                      |
| saving CM translations .....130  | Seize When Maintenance Busy .....1018                                |
| saving Communication Manager translations .....130                       | Select Attributes page .....1222                                     |
| saving, committing, and synchronizing configuration<br>changes .....1233 | select device type list .....125                                     |
| SBS .....744, 751, 868   | Select Groups and Resource page .....1221                            |
| SCCAN .....849, 1004   | Select Last Used Appearance .....70, 904, 1081                       |
| Schedule Backup page .....1304   | select network subnet list .....125                                  |
| Schedule Download .....633   | Selected Survivable Processor Node Names .....871                    |
| Scheduled .....756   | Self Administration .....768   |
| scheduler overview .....1318   | Self Station Display Activation .....567                             |
| scheduling a data backup on a local machine .....1298                    | Self-Station Display Enabled .....578                                |
| scheduling a global user settings importing job .....1417                | Send All Call Options .....590                                       |
| scheduling a user importing job .....1412                                | Send All Calls Activation/Deactivation .....567                      |
| scheduling roles importing job .....1203                                 | Send All Calls and Call Forwarding (SAC/CF) Override<br>.....489     |
| Scope .....1046  | Send All Calls Applies to .....590                                   |
| Script tags and abbreviations .....259                                   | Send ANI for MFE .....485  |
| Scroll Status messages Timer (sec.) .....625                             | Send ANSI-T1.403 One-Second Performance Reports<br>.....554          |
| Search Archives page .....1126   | Send Answer Supervision .....1004                                    |
| searching for a text in a log file .....1118                             | Send Called/Busy/Connected Number .....745, 1019                     |
| searching for alarms .....1100   | Send Calling Number .....745, 1019                                   |
| searching for logs .....1103   | Send Codeset 6/7 LAI IE .....746                                     |
| searching for presentities .....1684                                     | Send Connected Number .....746, 1020                                 |
| searching for resources .....1169, 1170, 1188                            | Send Custom Messages Through QSIG? .....602                          |
| searching for roles .....1199  | Send Disconnect Event for Bridged Appearance .....515                |
| searching for watchers .....1685   | Send EMU Visitor CPN .....1020                                       |
| searching groups .....1172   | Send Incoming/Outgoing Disconnect Timers to TN465<br>Ports .....1032 |
| searching users .....1394  | Send ISDN Trunk Group Name on Tandem Calls ...602                    |
| Second .....527  | Send Name .....746, 1021   |
| Second Announcement Delay (sec) .....665                                 | Send Non-ISDN Trunk Group Name as Connected<br>Name .....602         |
| Second Announcement Extension .....666                                   | Send Release Ack .....1004   |
| Second Announcement Recurring .....666                                   | Send Reroute Request .....666  |
| Secondary Alert on Held Reminder Calls? .....503                         | Send Space Disconnect .....787                                       |
| Secondary data module .....518   | Send Transferring Party Information .....1043                        |
| Secondary Data Module .....949   | Send UCID .....747   |
| Secondary IPSI .....714  | Send UCID to ASAI .....617   |
| Secondary Output Endpoint .....474                                       | Send UUI IE .....747   |
| Secondary Output Format .....475   | Sending Delay .....785   |
| Seconds Before PMS Link Idle Timeout .....639                            | Separating TTI from telephone .....181                               |
| Secure   | Serial Call .....506   |
| Enable File Transfer .....556  | Server ID .....719, 922, 923   |
| Enable Session .....557  | server IP address .....704   |
| Secure SIP .....849  |  |
| Secure Terminal Equip .....904   |  |
| Security Code .....59, 440, 451, 820, 904, 969, 1070                     |  |

|  |   |  |  |
|--|---|--|--|
| Server IP Address .....                                    | <a href="#">692</a>   | Setting up a trunk group .....                               | <a href="#">195</a>  |
| server port .....  | <a href="#">704</a>   | Setting up emergency calls on IP telephones .....            | <a href="#">193</a>  |
| Server Port .....  | <a href="#">692</a>   | Setting Up Extension To Cellular Feature Access Button ..... | <a href="#">232</a>  |
| Server Properties Page .....                               | <a href="#">1137</a>  | Setting up Remote Office on network regions .....            | <a href="#">196</a>  |
| Service Hours Table .....                                  | <a href="#">853</a>   | Setting Up Terminal Self-Administration .....                | <a href="#">233</a>  |
| Service Interruption .....                                 | <a href="#">808</a>   | Settings Administration .....                                | <a href="#">383</a>  |
| Service Level Algorithm for SLM .....                      | <a href="#">621</a>   | Sfx .....  | <a href="#">671</a> , <a href="#">759</a> , <a href="#">1041</a>                       |
| Service Level Interval .....                               | <a href="#">658</a>   | shared address .....   | <a href="#">1673</a>   |
| Service Level Maximizer .....                              | <a href="#">952</a>   | Shared UI Feature Priorities .....                           | <a href="#">754</a>  |
| Service Level Maximizer Algorithm .....                    | <a href="#">616</a>   | Short Holding Threshold .....                                | <a href="#">1021</a>   |
| Service Level Supervisor .....                             | <a href="#">658</a>   | Short Holding Time (seconds) .....                           | <a href="#">1021</a>   |
| Service Level Supervisor Call Selection Override .....     | <a href="#">616</a>   | Short Interdigit Timer .....                                 | <a href="#">594</a>  |
| Service Level Target (% in sec) .....                      | <a href="#">658</a>   | Short/Prefixed Registration Allowed .....                    | <a href="#">702</a> , <a href="#">905</a>  |
| Service Link Mode .....                                    | <a href="#">64</a> , <a href="#">905</a> , <a href="#">1075</a>   | Show ANSWERED BY on Display .....                            | <a href="#">747</a> , <a href="#">1022</a>   |
| Service Objective .....                                    | <a href="#">442</a> , <a href="#">659</a> , <a href="#">1050</a>  | Shuttle .....  | <a href="#">1022</a>   |
| Service Observing .....                                    | <a href="#">481</a> , <a href="#">614</a>   | Side .....   | <a href="#">550</a> , <a href="#">761</a> , <a href="#">763</a>                        |
| Warning Tone .....   | <a href="#">614</a>   | Sig Bit Inversion .....                                      | <a href="#">1004</a>   |
| SERVICE OBSERVING .....                                    | <a href="#">613</a>   | Sig Grp .....  | <a href="#">529</a> , <a href="#">759</a> , <a href="#">837</a>                        |
| Service Observing (Basic) .....                            | <a href="#">952</a>   | signaling group  |  |
| Service Observing (Remote/By FAC) .....                    | <a href="#">952</a>   | Incoming Dialog Loopbacks .....                              | <a href="#">861</a>  |
| Service Observing (VDNs) .....                             | <a href="#">952</a>   | RFC 3389 Comfort Noise .....                                 | <a href="#">867</a>  |
| Service Observing Allowed with Exclusion .....             | <a href="#">614</a>   | Signaling group .....  | <a href="#">854</a>  |
| Service Observing by Recording Device .....                | <a href="#">488</a>   | Signaling Group .....  | <a href="#">730</a> , <a href="#">833</a> , <a href="#">989</a> , <a href="#">1022</a> |
| Service Observing Listen Only Access Code .....            | <a href="#">570</a>   | Signaling Mode .....   | <a href="#">550</a> , <a href="#">868</a>  |
| Service Observing Listen/Talk Access Code .....            | <a href="#">570</a>   | signaling trunks, Russian and R2-MFC .....                   | <a href="#">483</a>  |
| Service Observing No Talk Access Code .....                | <a href="#">570</a>   | Silence Suppression .....                                    | <a href="#">678</a>  |
| SERVICE OBSERVING PERMISSION .....                         | <a href="#">490</a>   | Simple extended pickup groups .....                          | <a href="#">295</a> , <a href="#">296</a>  |
| Service Type .....   | <a href="#">717</a> , <a href="#">718</a> , <a href="#">729</a> , <a href="#">926</a> , <a href="#">927</a> , <a href="#">988</a> | creating .....   | <a href="#">296</a>  |
| Service/Feature .....                                      | <a href="#">670</a> , <a href="#">757</a> , <a href="#">849</a> , <a href="#">873</a> , <a href="#">874</a>                       | Simultaneous Calls .....                                     | <a href="#">833</a>  |
| services port  |   | Single server or switch data collaboration .....             | <a href="#">398</a> , <a href="#">412</a>  |
| accessing System Platform through .....                    | <a href="#">134</a>   | SIP elements   |  |
| Session - Local/Remote .....                               | <a href="#">836</a> , <a href="#">925</a>   | authentication .....   | <a href="#">1255</a>   |
| Session Connect Message Cntr .....                         | <a href="#">719</a> , <a href="#">927</a>   | TLS layer validation .....                                   | <a href="#">1256</a>   |
| Session Establishment Timer (min) .....                    | <a href="#">868</a>   | SIP entities   |  |
| Session Manager Communication profile administration ..... | <a href="#">1563</a>  | IP and transport layer validation .....                      | <a href="#">1256</a>   |
| Set Color .....  | <a href="#">74</a> , <a href="#">905</a> , <a href="#">1085</a>   | SIP entity .....   | <a href="#">1260</a>   |
| Set Layer 1 timer T1 to 30 seconds .....                   | <a href="#">938</a>   | SIP entity deletion .....                                    | <a href="#">1260</a>   |
| Setting  |   | SIP entity details .....                                     | <a href="#">1261</a>   |
| directory buttons .....                                    | <a href="#">263</a>   | SIP entity link deletion .....                               | <a href="#">1268</a>   |
| setting enrollment password .....                          | <a href="#">38</a>  | SIP entity list .....  | <a href="#">1263</a>   |
| Setting Issue Of The Day And Message Of The Day ....       | <a href="#">139</a>   | SIP Reference Trunk Group .....                              | <a href="#">752</a>  |
| Setting MASI command permissions .....                     | <a href="#">356</a>   | SIP Signaling Group .....                                    | <a href="#">868</a>  |
| setting the order .....                                    | <a href="#">116</a>   | SIP Video Infrastructure Enhancements .....                  | <a href="#">364</a>  |
| setting the order in SNMP Access list .....                | <a href="#">116</a>   | SIT Ineffective Other .....                                  | <a href="#">875</a>  |
| setting the system date and time .....                     | <a href="#">142</a>   | SIT Reorder .....  | <a href="#">876</a>  |
| Setting Time of Day Clock Synchronization .....            | <a href="#">142</a>   | SIT Treatment for Call Classification .....                  | <a href="#">874</a>  |
| Setting Up .....   | <a href="#">228</a>   | SIT Vacant Code .....  | <a href="#">876</a>  |
| Setting up a signaling group .....                         | <a href="#">195</a>   | Site Data .....  | <a href="#">73</a> , <a href="#">842</a> , <a href="#">877</a> , <a href="#">1084</a>  |
| Setting up a station to access a new group list .....      | <a href="#">225</a>   | building .....   | <a href="#">73</a> , <a href="#">1084</a>  |
|  |   | cable .....  | <a href="#">73</a> , <a href="#">1084</a>  |

|  |   |  |   |
|--|---|--|---|
| floor .....  | <a href="#">73</a> , <a href="#">1084</a>                       | Start Position .....                                 | <a href="#">1022</a>                      |
| jack .....   | <a href="#">73</a> , <a href="#">1084</a>                       | Start Time .....                                     | <a href="#">434</a>                       |
| room .....   | <a href="#">73</a> , <a href="#">1084</a>                       | Start/End  |   |
| Size (multiple of 5) .....                           | <a href="#">424–426</a> , <a href="#">428</a>                   | Service Hours Table .....                            | <a href="#">853</a>                       |
| Skill  |   | Starting .....                                       | <a href="#">137</a>                       |
| Hunt Group .....                                     | <a href="#">660</a>   | Starting Avaya Site Administration .....             | <a href="#">137</a>                       |
| SL (Skill Level) .....                               | <a href="#">442</a>   | Starting Extension .....                             | <a href="#">502</a>                       |
| Slip Detection .....                                 | <a href="#">553</a>   | Station  |   |
| SLM Count Abandoned Calls .....                      | <a href="#">660</a>   | access a new group list .....                        | <a href="#">225</a>                       |
| Slot   |   | Change Station Extension .....                       | <a href="#">478</a>                       |
| IP Interfaces .....                                  | <a href="#">684</a>   | Station and Trunk MSP .....                          | <a href="#">949</a>                       |
| SN (Skill Number) .....                              | <a href="#">442</a>   | Station as Virtual Extension .....                   | <a href="#">949</a>                       |
| SNMP Access .....                                    | <a href="#">118</a>   | Station Call Transfer Recall Timer .....             | <a href="#">594</a>                       |
| SNMP Access list .....                               | <a href="#">115</a> , <a href="#">116</a>                       | Station Coverage Path For Coverage After Forwarding  |   |
| SNMP access list field description .....             | <a href="#">118</a>   | .....  | <a href="#">934</a>                       |
| SNMP Access profile .....                            | <a href="#">117</a>   | station extension .....                              | <a href="#">916</a>                       |
| SNMP Access; field descriptions .....                | <a href="#">115</a>   | Station Extension .....                              | <a href="#">917</a>                       |
| Softkey Labels .....                                 | <a href="#">768</a>   | Station Firmware Download Access Code .....          | <a href="#">567</a>                       |
| Software Package .....                               | <a href="#">941</a>   | Station Hunt Before Coverage .....                   | <a href="#">932</a>                       |
| Source .....   | <a href="#">811</a>   | Station Hunting .....                                | <a href="#">403</a>                       |
| SOURCE ADDRESSES .....                               | <a href="#">707</a>   | Station Lock .....                                   | <a href="#">164</a> , <a href="#">489</a> |
| Source File .....                                    | <a href="#">633</a>   | Station Lock Activation/Deactivation .....           | <a href="#">567</a>                       |
| Source No .....                                      | <a href="#">811</a>   | Station Lock administering screens .....             | <a href="#">166</a>                       |
| SPDU Cntr .....                                      | <a href="#">719</a> , <a href="#">927</a>                       | Station Lock by time of day .....                    | <a href="#">165</a>                       |
| Speaker .....  | <a href="#">74</a> , <a href="#">906</a> , <a href="#">1085</a> | Station Lock COR .....                               | <a href="#">489</a>                       |
| Speakerphone .....                                   | <a href="#">65</a> , <a href="#">906</a> , <a href="#">1076</a> | station name .....                                   | <a href="#">477</a>                       |
| speakerphone group paging .....                      | <a href="#">633</a>   | Station Name   |   |
| Special Character for Restricted Number .....        | <a href="#">515</a>   | Change Station Extension .....                       | <a href="#">478</a>                       |
| Special Dial Tone .....                              | <a href="#">594</a> , <a href="#">624</a>                       | Station Putting Call On-Hold .....                   | <a href="#">630</a>                       |
| Special Dial Tone for Digital / IP Stations .....    | <a href="#">624</a>   | Station Security Code Change .....                   | <a href="#">567</a>                       |
| Special Dialing Option .....                         | <a href="#">906</a>   | Station Security Code verification .....             | <a href="#">853</a>                       |
| SPECIAL DIALING OPTION .....                         | <a href="#">455</a> , <a href="#">521</a>                       | Station Tone Forward Disconnect .....                | <a href="#">608</a>                       |
| Special Digit Conversion .....                       | <a href="#">962</a>   | Station User Admin of FBI Assign .....               | <a href="#">567</a>                       |
| specifying overuse limit for licensed features ..... | <a href="#">1143</a>  | Station User Button Ring Control .....               | <a href="#">567</a>                       |
| Speed .....  | <a href="#">687</a> , <a href="#">713</a> , <a href="#">787</a> | Station When Call is Active .....                    | <a href="#">630</a>                       |
| IP Interfaces .....                                  | <a href="#">687</a>   | Station-Button Display of UUI IE Data .....          | <a href="#">488</a>                       |
| Speed dialing .....                                  | <a href="#">225</a>   | Stations .....                                       | <a href="#">237</a>                       |
| SPEEDS .....   | <a href="#">524</a>   | Stations With Off PBX Telephone Integration .....    | <a href="#">918</a>                       |
| SPID .....   | <a href="#">525</a> , <a href="#">765</a>                       | stations with Off-PBX telephone integration .....    | <a href="#">916</a>                       |
| SPID — (Service Profile Identifier) .....            | <a href="#">906</a>   | Stations With System-wide Retrieval Permission ..... | <a href="#">580</a>                       |
| split supervisor .....                               | <a href="#">569</a>   | Status .....   | <a href="#">719</a>                       |
| src rgn .....  | <a href="#">699</a>   | status functions .....                               | <a href="#">491</a>                       |
| Standard Factory Number .....                        | <a href="#">1058</a>  | Status Poll VDN .....                                | <a href="#">462</a>                       |
| Start .....  | <a href="#">1046</a>  | Step .....   | <a href="#">976</a>                       |
| Start B Signal .....                                 | <a href="#">1022</a>  | Stop Confirmation page .....                         | <a href="#">1334</a>                      |
| Start Date/Time .....                                | <a href="#">633</a>   | Stop Date/Time .....                                 | <a href="#">633</a>                       |
| Start Day .....                                      | <a href="#">636</a>   | stopping pending jobs .....                          | <a href="#">1325</a>                      |
| Start Days (Sun through Sat) .....                   | <a href="#">433</a>   | Store to disk .....                                  | <a href="#">926</a>                       |
| Start Hour .....                                     | <a href="#">636</a>   | Store VDN Name in Station's Local Call Log .....     | <a href="#">613</a>                       |
| Start Min .....                                      | <a href="#">636</a>   | Strategies for assigning CORs .....                  | <a href="#">163</a>                       |
| Start Month .....                                    | <a href="#">636</a>   | submitting a request for harvesting log files .....  | <a href="#">1117</a>                      |

|   |   |   |  |
|---|---|---|--|
| subnet .....  | <a href="#">120</a>   | SVN Station Security Code Violation Notification      |  |
| Subnet Bits .....                                     | <a href="#">675</a>   | Enabled .....   | <a href="#">853</a>  |
| Subnet Mask .....                                     | <a href="#">685</a> , <a href="#">688</a> , <a href="#">712</a> , <a href="#">715</a> | Swap phones .....                                     | <a href="#">176</a>  |
| subnet(s) list .....                                  | <a href="#">119</a>   | Switch Hook Query Response Timeout .....              | <a href="#">622</a>  |
| subnets .....   | <a href="#">119</a> , <a href="#">120</a>   | Switch Name .....                                     | <a href="#">589</a>  |
| subscriber class of service .....                     | <a href="#">100</a>   | Switch Node .....                                     | <a href="#">462</a>  |
| subscriber COS .....                                  | <a href="#">100</a>   | switch to table view .....                            | <a href="#">1166</a>   |
| subscriber list .....                                 | <a href="#">104</a>   | Switchhook Flash .....                                | <a href="#">908</a>  |
| Subscriber Number .....                               | <a href="#">837</a>   | Switching between Basic and Enhanced modes .....      | <a href="#">412</a>  |
| subscriber template list .....                        | <a href="#">1067</a>  | switching to table view .....                         | <a href="#">1166</a>   |
| subscriber template versions .....                    | <a href="#">1061</a>  | switching to tree view .....                          | <a href="#">1167</a>   |
| subscriber templates; delete                          |   | Synch Source .....                                    | <a href="#">761</a>  |
| deleting subscriber templates                         |   | Synchronization .....                                 | <a href="#">737</a> , <a href="#">788</a> , <a href="#">1006</a> |
| deleting templates; subscriber .....                  | <a href="#">1066</a>  | Synchronizing Communication Manager data              |  |
| subscriber templates; duplicate                       |   | Synchronizing messaging data                          |  |
| duplicating subscriber templates                      |   | Incremental Synchronization                           |  |
| duplicating templates; subscribers .....              | <a href="#">1067</a>  | Initializing Synchronization .....                    | <a href="#">128</a>  |
| subscriber templates; edit                            |   | synchronizing messaging data                          |  |
| editing subscriber templates                          |   | synchronizing data .....                              | <a href="#">130</a>  |
| editing templates; subscriber .....                   | <a href="#">1065</a>  | synchronizing resources .....                         | <a href="#">1166</a>   |
| subscriber templates; view                            |   | synchronizing System Manager master database and      |  |
| viewing subscriber templates                          |   | replica computer database .....                       | <a href="#">1313</a> , <a href="#">1314</a>                      |
| viewing templates; subscriber .....                   | <a href="#">1066</a>  | synchronizing users with Active Directory .....       | <a href="#">1346</a>   |
| subscriber; view                                      |   | System CESID Default .....                            | <a href="#">469</a>  |
| viewing subscribers .....                             | <a href="#">103</a>   | System In Day Service .....                           | <a href="#">784</a>  |
| subscribers; add                                      |   | System In Night Service .....                         | <a href="#">784</a>  |
| adding subscribers .....                              | <a href="#">102</a>   | System List .....                                     | <a href="#">426</a>  |
| subscribers; new .....                                | <a href="#">102</a>   | System Management Data Transfer .....                 | <a href="#">949</a>  |
| subscribers; delete                                   |   | System Manager security authentication mechanism .... | <a href="#">1347</a>   |
| deleting subscribers                                  |   | System parameters                                     |  |
| removing subscribers .....                            | <a href="#">103</a>   | multifrequency signaling .....                        | <a href="#">790</a>  |
| subscribers; edit                                     |   | Security violation notification .....                 | <a href="#">850</a> , <a href="#">851</a>                        |
| editing a subscriber .....                            | <a href="#">102</a>   | System Parameters - SCCAN .....                       | <a href="#">961</a>  |
| editing subscribers .....                             | <a href="#">102</a>   | System Parameters Media Gateway Automatic             |  |
| Suite Check-in .....                                  | <a href="#">645</a>   | Recovery Rule .....                                   | <a href="#">956</a>  |
| Supervisor Extension .....                            | <a href="#">660</a>   | System parameters OCM call classification .....       | <a href="#">957</a>  |
| Supplementary Service Protocol .....                  | <a href="#">737</a> , <a href="#">1005</a>  | System parameters, mode code .....                    | <a href="#">783</a>  |
| Supplementary Services with Rerouting .....           | <a href="#">955</a>   | System Preferred .....                                | <a href="#">923</a>  |
| Supply CPE Loopback Jack Power .....                  | <a href="#">554</a>   | SYSTEM PRINTER PARAMETERS .....                       | <a href="#">588</a>  |
| Supported Set Type .....                              | <a href="#">443</a>   | System Requirements .....                             | <a href="#">236</a>  |
| Suppress # Outpulsing .....                           | <a href="#">748</a> , <a href="#">1023</a>  | System Updates Time On Station Displays .....         | <a href="#">608</a>  |
| Suppress CDR for Ineffective Call Attempts .....      | <a href="#">475</a>   |   |  |
| Survivable COR .....                                  | <a href="#">66</a> , <a href="#">907</a> , <a href="#">1077</a>                       |   |  |
| Survivable GK Node Name .....                         | <a href="#">66</a> , <a href="#">907</a> , <a href="#">1077</a>                       |   |  |
| Survivable Processor .....                            | <a href="#">920</a>   |   |  |
| Survivable Trunk Dest .....                           | <a href="#">70</a> , <a href="#">908</a> , <a href="#">1081</a>                       |   |  |
| SVN Authorization Code Violation Notification Enabled |   |   |  |
| .....   | <a href="#">851</a>   |   |  |
| SVN Login .....                                       | <a href="#">851</a>   |   |  |
| SVN Remote Access Violation Notification Enabled .... | <a href="#">851</a>   |   |  |

## T

|  |   |
|--|---|
| T2 (Backward Signal) Activation Timer (secs) ..... | <a href="#">627</a>   |
| T3 Timer Length (sec) .....                        | <a href="#">762</a>   |
| T303 Timer (sec) .....                             | <a href="#">868</a>   |
| T303 Timer (sec) .....                             | <a href="#">551</a>   |
| Table Active .....                                 | <a href="#">972</a>   |
| TAC .....  | <a href="#">730</a> , <a href="#">820</a> , <a href="#">989</a> |
| Take Down Link for Lost Messages .....             | <a href="#">639</a>   |

|  |                               |   |                               |
|--|-------------------------------|---|-------------------------------|
| Talk Duration .....                                      | <a href="#">877</a>           | Tests   |                               |
| Target % .....   | <a href="#">829</a>           | Station .....   | <a href="#">908</a>           |
| Target Socket Load .....                                 | <a href="#">685</a>           | Text lines on Bulletin Board .....                                      | <a href="#">463</a>           |
| Target socket load and Warning level .....               | <a href="#">685</a>           | TFTP Server .....   | <a href="#">969</a>           |
| TCP Signaling Link Establishment for Avaya H.323         |                               | TFTP Server Node Name .....   | <a href="#">970</a>           |
| Endpoints .....  | <a href="#">696</a>           | TFTP Server Port .....  | <a href="#">970</a>           |
| TDD/TTY Mode .....                                       | <a href="#">681</a>           | Threshold for Blocking Off-Net Redirection of Incoming                  |                               |
| Team Btn Display Name .....                              | <a href="#">490</a>           | Trunk Calls .....   | <a href="#">930</a>           |
| Team Btn Silent if Active .....                          | <a href="#">490</a>           | Tie Call .....  | <a href="#">506</a>           |
| Team Pick Up by Going Off Hook .....                     | <a href="#">490</a>           | Time  |                               |
| TEI .....  | <a href="#">525, 762, 908</a> | system parameters port networks .....                                   | <a href="#">961</a>           |
| Station .....  | <a href="#">908</a>           | Time (sec) to Drop Call on No Answer .....                              | <a href="#">1023</a>          |
| Telecommuter mode  |                               | Time (Start) .....  | <a href="#">529</a>           |
| Adding .....   | <a href="#">189</a>           | Time (Stop) .....   | <a href="#">529</a>           |
| Telecommuting Access .....                               | <a href="#">962</a>           | Time Before Off-Hook Alert .....  | <a href="#">586</a>           |
| Telecommuting Access Extension .....                     | <a href="#">962</a>           | Time Delay .....  | <a href="#">788</a>           |
| Telephone  |                               | Time In Queue Warning (sec) .....                                       | <a href="#">503</a>           |
| Feature buttons table .....                              | <a href="#">206</a>           | Time Interval .....   | <a href="#">851</a>           |
| Telephone Display .....                                  | <a href="#">403</a>           | Time of Day Chart .....   | <a href="#">485</a>           |
| Telephone Displays                                       |                               | Time of Day Clock Synchronization .....                                 | <a href="#">142</a>           |
| Troubleshooting .....                                    | <a href="#">262</a>           | Time of Day Coverage Table .....  | <a href="#">970, 971</a>      |
| Telephone Event Payload Type .....                       | <a href="#">1043</a>          | Time of Day Lock Table .....  | <a href="#">66, 909, 1077</a> |
| Telephone Features .....                                 | <a href="#">203</a>           | Time of Day Routing .....   | <a href="#">950</a>           |
| template list .....                                      | <a href="#">1067</a>          | Time of Day Routing Plan .....  | <a href="#">971, 972</a>      |
| template versioning .....                                | <a href="#">1061</a>          | Time of Day Station Lock Table .....                                    | <a href="#">972</a>           |
| template versions .....                                  | <a href="#">1061</a>          | Time of Scheduled Emergency Access Summary Report                       |                               |
| templates .....  | <a href="#">1061</a>          | <a href="#">643</a>   |                               |
| Temporary Bridged Appearance on Call Pickup .....        | <a href="#">632</a>           | Time of Scheduled Wakeup Activity Report .....                          | <a href="#">644</a>           |
| Tenant .....   | <a href="#">962-964</a>       | Time of Scheduled Wakeup Summary Report .....                           | <a href="#">644</a>           |
| attendant group .....                                    | <a href="#">962</a>           | time range deletion .....   | <a href="#">1272</a>          |
| Tenant Description .....                                 | <a href="#">964</a>           | time range list .....   | <a href="#">1273</a>          |
| Tenant Partitioning .....                                | <a href="#">403, 949</a>      | time ranges .....   | <a href="#">1272</a>          |
| Terminal Dial-Up Access Code .....                       | <a href="#">568</a>           | Time Remaining .....  | <a href="#">671</a>           |
| Terminal Endpoint Identifier (TEI) .....                 | <a href="#">525</a>           | Time Reminder on Hold (sec) .....                                       | <a href="#">503</a>           |
| Terminal Equipment Identifier (TEI) .....                | <a href="#">525</a>           | Time to Login .....   | <a href="#">557</a>           |
| Terminal Parameters .....                                | <a href="#">965</a>           | Time Warning Extension .....  | <a href="#">652</a>           |
| Terminal Self-Administration .....                       | <a href="#">233</a>           | Time Warning Threshold .....  | <a href="#">653</a>           |
| Terminal Trans. Init. (TTI) .....                        | <a href="#">950</a>           | Timed ACW .....   | <a href="#">952</a>           |
| Terminal Translation Initialization .....                | <a href="#">179</a>           | Timed ACW Interval (sec) .....  | <a href="#">660</a>           |
| Terminal Translation Initialization Enabled .....        | <a href="#">581</a>           | Timezone Offset .....   | <a href="#">772</a>           |
| Terminal Translation Initialization Merge Code .....     | <a href="#">568</a>           | TN ... <a href="#">59, 431, 440, 448, 451, 455, 519, 635, 653, 732,</a> |                               |
| Terminal Translation Initialization Separation Code .... | <a href="#">568</a>           | <a href="#">770, 833, 840, 909, 969, 990, 1051, 1070</a>                |                               |
| <a href="#">568</a>                                      |                               | Agent LoginID .....   | <a href="#">440</a>           |
| Terminate to Coverage Pts. with Bridged Appearances      |                               | Data Module .....   | <a href="#">519</a>           |
| .....  | <a href="#">511</a>           | Group Paging Using Speakerphone .....                                   | <a href="#">635</a>           |
| Terminating Extension Group .....                        | <a href="#">967</a>           | TN2185 circuit pack .....   | <a href="#">759</a>           |
| Terminating Extension Groups .....                       | <a href="#">403</a>           | TN2198 circuit packs .....  | <a href="#">762</a>           |
| Termination Type .....                                   | <a href="#">762</a>           | TN2501 VAL Boards .....   | <a href="#">942</a>           |
| TestCall BCC .....                                       | <a href="#">730</a>           | TN2501 VAL Maximum Capacity .....                                       | <a href="#">950</a>           |
| Testcall ITC .....                                       | <a href="#">731</a>           | TN2602 Boards with 320 VoIP Channels .....                              | <a href="#">942</a>           |
| Testcall Service .....                                   | <a href="#">731</a>           | TN2602 Boards with 80 VoIP Channels .....                               | <a href="#">942</a>           |

|  |  |  |   |
|--|--|--|---|
| TN556B circuit packs .....                           | <a href="#">762</a>  | Numbering Format .....                       | <a href="#">742</a>   |
| to board .....                                       | <a href="#">672</a>  | Trunk Group for Channel Selection .....      | <a href="#">869</a>   |
| To IP Address .....                                  | <a href="#">675</a>  | Trunk Groups .....                           | <a href="#">1059</a>  |
| Toll Analysis .....                                  | <a href="#">972</a> , <a href="#">973</a>                        | Trunk Grp No .....                           | <a href="#">920</a>   |
| Location .....                                       | <a href="#">973</a>  | Trunk Hunt .....                             | <a href="#">737</a> , <a href="#">1006</a>  |
| Toll List .....                                      | <a href="#">850</a> , <a href="#">974</a>                        | Trunk Length .....                           | <a href="#">1035</a>  |
| Toll Restricted .....                                | <a href="#">990</a>  | trunk selection .....                        | <a href="#">916</a>   |
| Tone (Frequency/Level) .....                         | <a href="#">976</a>  | Trunk Selection .....                        | <a href="#">917</a>   |
| Tone (msec) .....                                    | <a href="#">753</a> , <a href="#">1032</a>                       | Trunk Signaling Type .....                   | <a href="#">990</a>   |
| Tone Continuous .....                                | <a href="#">959</a>  | Trunk Termination .....                      | <a href="#">827</a> , <a href="#">1007</a>  |
| Tone Detection Mode .....                            | <a href="#">939</a>  | Trunk Type .....                             | <a href="#">738</a> , <a href="#">826</a> , <a href="#">1007</a>  |
| Tone Generation .....                                | <a href="#">975</a>  | Trunk Type (in/out) .....                    | <a href="#">991</a>   |
| Tone Generation Plan .....                           | <a href="#">775</a>  | Trunk Vendor .....                           | <a href="#">1035</a>  |
| Tone Name .....                                      | <a href="#">959</a> , <a href="#">977</a>                        | Trunk-to-Trunk Transfer .....                | <a href="#">578</a>   |
| Total Administered .....                             | <a href="#">814</a>  | Trusted Certificates page .....              | <a href="#">43</a>  |
| Total Administered Members .....                     | <a href="#">668</a> , <a href="#">759</a> , <a href="#">1041</a> | TSC .....                                    | <a href="#">850</a>   |
| Total CPN Len .....                                  | <a href="#">816</a>  | TSC Index .....                              | <a href="#">529</a> , <a href="#">837</a>   |
| Total Len .....                                      | <a href="#">814</a>  | TSC Method for Auto Callback .....           | <a href="#">752</a>   |
| Total Length .....                                   | <a href="#">469</a> , <a href="#">532</a> , <a href="#">920</a>  | TSC per MWI Interrogation .....              | <a href="#">666</a>   |
| CAMA Numbering Format .....                          | <a href="#">469</a>  | TSC Supplementary Service Protocol .....     | <a href="#">869</a>   |
| Totals .....   | <a href="#">829</a>  | TTI .....                                    | <a href="#">179</a>   |
| Touch Tone Sidetone (dB) .....                       | <a href="#">965</a> , <a href="#">967</a>                        | TTI Security Code .....                      | <a href="#">582</a>   |
| Touch Tone Transmit (dB) .....                       | <a href="#">967</a>  | TTI State .....                              | <a href="#">582</a>   |
| Transfer Conference .....                            | <a href="#">768</a>  | TTL Contact .....                            | <a href="#">1035</a>  |
| Transfer Into QSIG Voice Mail .....                  | <a href="#">955</a>  | TTL Type .....                               | <a href="#">1035</a>  |
| Transfer to Voice Mail Access Code .....             | <a href="#">568</a>  | TTL Vendor .....                             | <a href="#">1036</a>  |
| Transfer Upon Hang-Up .....                          | <a href="#">598</a>  | TTY  |   |
| Transferred Ring Pattern .....                       | <a href="#">608</a>  | Enabling transmission over IP networks ..... | <a href="#">185</a>   |
| Translation-ID Number Mismatch Interval (days) ..... | <a href="#">852</a>  | Two-Digit Aux Work Reason Codes .....        | <a href="#">515</a> , <a href="#">622</a>   |
| transmission mode for inter-system IP DTMF .....     | <a href="#">706</a>  | Type .....                                   | <a href="#">451</a> , <a href="#">464</a> , <a href="#">514</a> , <a href="#">519</a> , <a href="#">527</a> , <a href="#">578</a> , <a href="#">686</a> , <a href="#">829</a> , <a href="#">909</a> , <a href="#">923</a> ,<br><a href="#">1041</a> , <a href="#">1047</a> , <a href="#">1059</a> |
| transmission mode for Intra-System IP DTMF .....     | <a href="#">706</a>  | Attendant Console .....                      | <a href="#">451</a>   |
| Transmit LBO .....                                   | <a href="#">555</a>  | Call Type Analysis Table .....               | <a href="#">464</a>   |
| Transmit Line Build-Out .....                        | <a href="#">555</a>  | CTI Link .....                               | <a href="#">514</a>   |
| Transmitted Signal Gain (dB) .....                   | <a href="#">796</a>  | Data Module .....                            | <a href="#">519</a>   |
| Transport Method .....                               | <a href="#">868</a>  | Date and Time .....                          | <a href="#">527</a>   |
| Trk Grp(s) .....                                     | <a href="#">721</a> , <a href="#">814</a> , <a href="#">816</a>  | Feature-Related System Parameters .....      | <a href="#">578</a>   |
| Trk-to-Trk Restriction Override .....                | <a href="#">493</a>  | IP Interfaces .....                          | <a href="#">686</a>   |
| Troubleshooting .....                                | <a href="#">362</a> , <a href="#">417</a>                        | Station .....                                | <a href="#">909</a>   |
| Troubleshooting Abbreviated Dialing Lists .....      | <a href="#">226</a>  | Survivable Processor .....                   | <a href="#">923</a>   |
| Troubleshooting ESM .....                            | <a href="#">389</a>  | Type (Column) .....                          | <a href="#">811</a>   |
| Troubleshooting IP Softphones .....                  | <a href="#">189</a>  | Type (field) .....                           | <a href="#">812</a>   |
| Troubleshooting TTI .....                            | <a href="#">181</a>  | Type of 3PCC Enabled .....                   | <a href="#">914</a>   |
| Truncate Station Number in ANI .....                 | <a href="#">799</a>  | Type of roles .....                          | <a href="#">1196</a>  |
| Trunk Alerting Tone Interval .....                   | <a href="#">595</a>  |  |   |
| Trunk Answer Any Station Access Code .....           | <a href="#">568</a>  | <b>U</b>                                     |   |
| Trunk Contact .....                                  | <a href="#">1035</a>   | UCID Network Node ID .....                   | <a href="#">591</a>   |
| Trunk COR .....                                      | <a href="#">595</a>  | UDP Extension Search Order .....             | <a href="#">534</a>   |
| Trunk Direction .....                                | <a href="#">825</a>  | UDP Port Range .....                         | <a href="#">691</a>   |
| Trunk Flash .....                                    | <a href="#">990</a>  | UDP Port Range Max .....                     | <a href="#">691</a>   |
| Trunk Gain .....                                     | <a href="#">826</a> , <a href="#">1006</a>                       | UDP Port Range Min .....                     | <a href="#">691</a>   |
| Trunk Group .....                                    | <a href="#">742</a> , <a href="#">977</a>                        |  |   |

|   |   |  |   |
|---|---|--|---|
| Unacceptable Threshold                          |   | Use System Level Parameter Values                            | <a href="#">713</a>                         |
| --Dev - 2804 Hz                                 | <a href="#">1038</a>                        | Use System Syslog Values                                     | <a href="#">716</a>                         |
| --Dev - 404 Hz                                  | <a href="#">1038</a>                        | Use Time Adjustments from Location                           | <a href="#">854</a>                         |
| --+Dev - 2804 Hz                                | <a href="#">1038</a>                        | Used   |   |
| --+Dev - 404 Hz                                 | <a href="#">1038</a>                        | System Parameters Customer Options page 1                    | <a href="#">941</a>                         |
| Max - 1004 Hz Loss                              | <a href="#">1038</a>                        | System Parameters Customer Options page 2                    | <a href="#">942</a>                         |
| Maximum C Message Noise                         | <a href="#">1039</a>                        | Virtual MAC Addresses  | <a href="#">1060</a>                        |
| Maximum C Notched Noise                         | <a href="#">1039</a>                        | Used for DCS   | <a href="#">1023</a>                        |
| Min - 1004 Hz Loss                              | <a href="#">1039</a>                        | Used Only for Paging   | <a href="#">1023</a>                        |
| Minimum ERL                                     | <a href="#">1039</a>                        | User Control Restrict Activation/Deactivation                | <a href="#">568</a>                         |
| Minimum SRL-HI                                  | <a href="#">1039</a>                        | User Delete Confirmation page                                | <a href="#">1648</a>                        |
| Minimum SRL-LO                                  | <a href="#">1039</a>                        | User Guidance Display  | <a href="#">604</a>                         |
| Unanswered DID Call Timer                       | <a href="#">595</a>                         | user management  | <a href="#">1389</a>                        |
| UnAssign Roles page                             | <a href="#">1221</a> , <a href="#">1654</a> | User Management page   | <a href="#">1616</a>                        |
| Unauthorized Precedence Level                   | <a href="#">808</a>                         | User Profile   | <a href="#">1046</a>                        |
| understanding                                   |   | User Profile Duplicate page                                  | <a href="#">1642</a>                        |
| groups  | <a href="#">76</a> , <a href="#">1087</a>   | User Profile Edit page                                       | <a href="#">1577</a> , <a href="#">1624</a> |
| Unhold  | <a href="#">598</a>                         | User Profile View page                                       | <a href="#">1571</a> , <a href="#">1617</a> |
| Unicode   |   | User Profiles  | <a href="#">140</a>                         |
| Native name support                             | <a href="#">259</a>                         | User Restore Confirmation Page                               | <a href="#">1652</a>                        |
| Unicode Display                                 |   | users  | <a href="#">1390</a>                        |
| Administering                                   | <a href="#">256</a>                         | using advanced search  | <a href="#">127</a>                         |
| Unicode Name                                    | <a href="#">1008</a>                        | Using alias  | <a href="#">174</a>                         |
| Uniform dial plan                               |   | Using Avaya Site Administration                              | <a href="#">135</a>                         |
| UDP   | <a href="#">1060</a>                        | Using Bulletin Board   | <a href="#">142</a>                         |
| Uniform Dial Plan Table                         | <a href="#">1044</a>                        | using filters  |   |
| Uniform Dialing Plan                            | <a href="#">950</a>                         | filtering endpoints  | <a href="#">56</a>                          |
| Uninstall License page                          | <a href="#">1136</a>                        | Using Native Name  | <a href="#">52</a>                          |
| Universal Call ID                               | <a href="#">590</a> , <a href="#">755</a>   | Using the system default Issue of the Day                    | <a href="#">138</a>                         |
| Unknown Numbers Considered Internal for AUDIX   | <a href="#">602</a>                         | Using wild cards   | <a href="#">326</a>                         |
| Unnamed Registrations and PSA for IP Telephones | <a href="#">582</a>                         | USNI Calling Name for Outgoing Calls                         | <a href="#">602</a>                         |
| Unrestricted Call List                          | <a href="#">485</a> , <a href="#">974</a>   | UII IE Treatment   | <a href="#">748</a>                         |
| Unsupported Communication Manager features      | <a href="#">358</a>                         |  |   |
| Upgrade Telephones                              | <a href="#">176</a>                         | <b>V</b>   |   |
| Upon DTE LOS                                    | <a href="#">555</a>                         | VAC  | <a href="#">1047</a>                        |
| Upper Bound (msec)                              | <a href="#">777</a>                         | Vacant Code  | <a href="#">808</a>                         |
| US NI Delayed Calling Name Update               | <a href="#">748</a>                         | Validate BCMS/VuStats Login IDs                              | <a href="#">619</a>                         |
| USA Default Algorithm                           | <a href="#">958</a>                         | validating connectivity to local WebLM servers for a product | <a href="#">1141</a>                        |
| USA SIT Algorithm                               | <a href="#">958</a>                         | Value Added (VALU)   | <a href="#">955</a>                         |
| Usage Alloc                                     | <a href="#">732</a>                         | Var  | <a href="#">1047</a> , <a href="#">1056</a> |
| Usage Allocation Enhancements                   | <a href="#">950</a>                         | Variables for Vectors  | <a href="#">1046</a>                        |
| Usage by Local WebLM page                       | <a href="#">1152</a>                        | VDN Name   | <a href="#">755</a> , <a href="#">829</a>   |
| Usage Summary page                              | <a href="#">1152</a>                        | VDN of Origin Annc. Extension                                | <a href="#">1051</a>                        |
| Use COR for All Group II Responses              | <a href="#">796</a>                         | VDN of Origin Announcement                                   | <a href="#">483</a> , <a href="#">953</a>   |
| Use COR for Calling Party Category              | <a href="#">796</a>                         | VDN Override for ASAI Messages                               | <a href="#">1054</a>                        |
| Use Default Server Parameters                   | <a href="#">692</a>                         | VDN Return Destination                                       | <a href="#">953</a>                         |
| Use Enhanced Formats                            | <a href="#">475</a>                         | VDN Time Zone Offset   | <a href="#">1057</a>                        |
| Use ISDN Layouts                                | <a href="#">475</a>                         | VDN Timed ACW Interval                                       | <a href="#">1054</a>                        |
| Use Legacy CDR Formats                          | <a href="#">476</a>                         |  |   |

|   |   |   |   |
|---|---|---|---|
| VDN Variables .....   | <a href="#">1056</a>  | View Peak Usage Page .....                                  | <a href="#">1135</a>                        |
| Vector .....  | <a href="#">314</a> , <a href="#">556</a> , <a href="#">653</a>                     | View Private Contact List page .....                        | <a href="#">1612</a>                        |
| administering vector variables .....  | <a href="#">314</a>   | View Profile  |   |
| Hunt Group .....  | <a href="#">653</a>   | Alarming UI page .....                                      | <a href="#">1342</a>                        |
| Vector Direcotry Numbers  |   | Communication System Management Configuration               |   |
| viewing .....   | <a href="#">317</a>   | page .....  | <a href="#">1373</a>                        |
| Vector Directory Number .....   | <a href="#">317</a> , <a href="#">1047</a> , <a href="#">1053</a>                   | Logging page .....  | <a href="#">1364</a>                        |
| adding .....  | <a href="#">317</a>   | Logging Service page .....                                  | <a href="#">1366</a>                        |
| Send VDN as Called Ringing Name Over QSIG ....  | <a href="#">1053</a>  | Role Bulk Import Profile page .....                         | <a href="#">1376</a>                        |
| Vector Disconnect Timer (min) .....   | <a href="#">608</a>   | System Manager Element Manager page .....                   | <a href="#">1361</a>                        |
| Vector Number .....   | <a href="#">1051</a>  | User Bulk Import Profile page .....                         | <a href="#">1378</a> , <a href="#">1380</a> |
| Vector Problem  |   | View Profile Enterprise Directory Synchronization page      |   |
| fixing .....  | <a href="#">316</a>   | .....   | <a href="#">1343</a> , <a href="#">1344</a> |
| Vector Variable x .....   | <a href="#">571</a>   | View Profile System Manager page .....                      | <a href="#">1338</a>                        |
| Vectoring (ANI/II-Digits Routing) .....   | <a href="#">952</a>   | View Public Contact List page .....                         | <a href="#">1662</a>                        |
| Vectoring (Basic) .....   | <a href="#">952</a>   | View Role page .....  | <a href="#">1217</a>                        |
| Vectoring (Best Service Routing) .....  | <a href="#">952</a>   | View Scheduler Profile page .....                           | <a href="#">1368</a>                        |
| Vectoring (CINFO) .....   | <a href="#">952</a>   | View SNMP Profile page .....                                | <a href="#">1370</a>                        |
| Vectoring (G3V4 Advanced Routing) .....   | <a href="#">952</a>   | view software feature profiles .....                        | <a href="#">1339</a>                        |
| Vectoring (Holidays) .....  | <a href="#">953</a>   | View System ACL page .....                                  | <a href="#">1700</a>                        |
| Vectoring (Prompting) .....   | <a href="#">953</a>   | View Trust Certificate page .....                           | <a href="#">45</a>                          |
| Vectors   |   | View WebLM page .....                                       | <a href="#">1340</a>                        |
| handling TTY calls .....  | <a href="#">315</a>   | viewing a high priority enforced ACL rule .....             | <a href="#">1674</a>                        |
| variables .....   | <a href="#">314</a>   | viewing a user importing job in Scheduler .....             | <a href="#">1414</a>                        |
| Verification .....  | <a href="#">356</a>   | viewing alarms .....  | <a href="#">1099</a>                        |
| Verify Wakeup Announcement Access Code .....  | <a href="#">571</a>   | viewing allocations by features .....                       | <a href="#">1142</a>                        |
| Verizon Adapter (VerizonAdapter) .....  | <a href="#">1251</a>  | viewing allocations by local WebLM .....                    | <a href="#">1144</a>                        |
| Version .....   | <a href="#">992</a>   | viewing an announcement .....                               | <a href="#">88</a>                          |
| Video (Norm) .....  | <a href="#">699</a>   | viewing an audio group .....                                | <a href="#">97</a>                          |
| Video (Prio) .....  | <a href="#">699</a>   | viewing an importing global user settings job in            |   |
| Video (Shr) .....   | <a href="#">700</a>   | Scheduler .....   | <a href="#">1419</a>                        |
| Video 802.1p Priority .....   | <a href="#">693</a>   | viewing announcements .....                                 | <a href="#">88</a>                          |
| Video Bridge .....  | <a href="#">1057</a>  | viewing associated endpoints                                |   |
| video capable IP Softphones .....   | <a href="#">942</a>   | viewing endpoints .....                                     | <a href="#">1064</a>                        |
| video capable stations .....  | <a href="#">942</a>   | viewing associated subscribers                              |   |
| Video PHB Value .....   | <a href="#">693</a>   | viewing subscribers .....                                   | <a href="#">1067</a>                        |
| Video Telephony Solution .. <a href="#">363</a> , <a href="#">366</a> , <a href="#">367</a> , <a href="#">370</a> , <a href="#">371</a> , <a href="#">373</a> , |   | viewing audio groups .....                                  | <a href="#">97</a>                          |
| <a href="#">374</a>   |   | viewing class of service data .....                         | <a href="#">111</a>                         |
| view .....  | <a href="#">88</a> , <a href="#">97</a> , <a href="#">111</a> , <a href="#">126</a> | viewing completed jobs .....                                | <a href="#">1319</a> , <a href="#">1321</a> |
| View Application Instance page .....  | <a href="#">28</a>  | viewing data retention rules .....                          | <a href="#">1299</a> , <a href="#">1310</a> |
| View Buttons .....  | <a href="#">769</a>   | viewing deleted users                                       |   |
| View by Feature page .....  | <a href="#">1145</a>  | view deleted users .....                                    | <a href="#">1398</a>                        |
| View by Local WebLM page .....  | <a href="#">1145</a>  | viewing details of a completed job .....                    | <a href="#">1320</a>                        |
| View Contact List Member page .....   | <a href="#">1600</a>  | viewing details of a global user settings importing job ... |   |
| view endpoint .....   | <a href="#">58</a> , <a href="#">1069</a>   | <a href="#">1418</a>  |   |
| View Group page .....   | <a href="#">1176</a>  | viewing details of a job .....                              | <a href="#">1203</a>                        |
| View High Priority Enforced User ACL page .....   | <a href="#">1694</a>  | viewing details of a job in Scheduler .....                 | <a href="#">1204</a>                        |
| View IAM Profile page .....   | <a href="#">1348</a>  | viewing details of a log harvesting profile .....           | <a href="#">1122</a>                        |
| View License Capacity Page .....  | <a href="#">1134</a>  | viewing details of a log harvesting request .....           | <a href="#">1117</a>                        |
| View Local WebLMs page .....  | <a href="#">1148</a>  | viewing details of a low priority enforced ACL rule ....    |   |
|   |   | <a href="#">1676</a>  |   |

|  |   |   |   |
|--|---|---|---|
| viewing details of a pending job .....                   | <a href="#">1319</a> , <a href="#">1320</a> | VMS Hunt Group Extension .....                      | <a href="#">785</a>   |
| viewing details of a system ACL rule .....               | <a href="#">1678</a>                        | VOA messages .....                                  | <a href="#">483</a>   |
| viewing details of a user .....                          | <a href="#">1390</a>                        | Voice Coverage Message Retrieval Access Code ....   | <a href="#">568</a>   |
| viewing details of an application instance .....         | <a href="#">22</a>                          | Voice Do Not Disturb Access Code .....              | <a href="#">571</a>   |
| viewing details of an user importing job .....           | <a href="#">1415</a>                        | Voice Mail Extension .....                          | <a href="#">667</a>   |
| viewing enterprise usage of a license feature .....      | <a href="#">1142</a>                        | Voice Mail Handle .....                             | <a href="#">667</a>   |
| viewing groups, viewing resources for a group .....      | <a href="#">1162</a>                        | Voice Mail Hunt Group Ext .....                     | <a href="#">598</a>   |
| viewing harvested log files in an archive .....          | <a href="#">1116</a>                        | Voice mail Number .....                             | <a href="#">914</a>   |
| viewing identity certificates .....                      | <a href="#">41</a>                          | Voice Mail Number .....                             | <a href="#">73</a> , <a href="#">530</a> , <a href="#">667</a> , <a href="#">1084</a> |
| viewing last contacted status of local WebLM servers ... | <a href="#">1140</a>                        | Voice Paging Timeout (sec) .....                    | <a href="#">782</a> , <a href="#">1024</a>  |
| viewing license capacity .....                           | <a href="#">1132</a>                        | Voice Paging, COR .....                             | <a href="#">782</a>   |
| viewing license capacity of a feature .....              | <a href="#">1140</a>                        | Voice Paging, TAC .....                             | <a href="#">782</a>   |
| viewing list of backup files .....                       | <a href="#">1297</a>                        | Voice Paging, TN .....                              | <a href="#">783</a>   |
| viewing log details .....                                | <a href="#">1102</a>                        | Voice Principal Message Retrieval Access Code ....  | <a href="#">568</a>   |
| viewing loggers for a log file .....                     | <a href="#">1109</a> , <a href="#">1300</a> | Voice Receive (dB) .....                            | <a href="#">965</a> , <a href="#">967</a>   |
| viewing logs   |   | Voice Sidetone (dB) .....                           | <a href="#">965</a> , <a href="#">967</a>   |
| pending jobs   |   | Voice station audio vs. H.320 DVC system audio .... | <a href="#">412</a>   |
| completed jobs .....                                     | <a href="#">1320</a>                        | Voice Terminal .....                                | <a href="#">60</a> , <a href="#">1071</a>   |
| viewing network device inventory .....                   | <a href="#">126</a>                         | Voice Transmit (dB) .....                           | <a href="#">965</a> , <a href="#">967</a>   |
| viewing peak usage .....                                 | <a href="#">1132</a>                        | Volume for DCP Types .....                          | <a href="#">966</a>   |
| viewing pending jobs .....                               | <a href="#">1319</a>                        | Volume for IP Types .....                           | <a href="#">966</a>   |
| viewing periodic status of master and local WebLM        |   | Vustats .....                                       | <a href="#">769</a>   |
| servers .....  | <a href="#">1143</a>                        | VuStats .....                                       | <a href="#">619</a> , <a href="#">953</a>   |
| viewing replica groups .....                             | <a href="#">1312</a>                        | VuStats (G3V4 Enhanced) .....                       | <a href="#">953</a>   |
| viewing replica nodes in a replica group .....           | <a href="#">1313</a>                        | VuStats Objective .....                             | <a href="#">661</a>   |
| viewing replication details for a replica node .....     | <a href="#">1314</a>                        |   |   |
| viewing server properties .....                          | <a href="#">1133</a>                        | <b>W</b>  |   |
| viewing subscriber templates CMM; field description      |   | Wait Answer Supervision Timer .....                 | <a href="#">609</a>   |
| CMM field description .....                              | <a href="#">1088</a>                        | wakeup announcement .....                           | <a href="#">571</a>   |
| viewing subscriber templates MM; field description       |   | WAN-BW limits (units) .....                         | <a href="#">700</a>   |
| MM field description .....                               | <a href="#">1090</a>                        | WAN-BW limits (value) .....                         | <a href="#">700</a>   |
| viewing the contents of harvested log files .....        | <a href="#">1118</a>                        | Warning for redirected calls .....                  | <a href="#">162</a>   |
| viewing the details of a contact in the contact list ... | <a href="#">1597</a>                        | Warning when telephones are off-hook .....          | <a href="#">162</a>   |
| viewing the details of a private contact .....           | <a href="#">1604</a>                        | WebLM Home page .....                               | <a href="#">1134</a>  |
| viewing the details of a public contact .....            | <a href="#">1657</a>                        | WebLM overview .....                                | <a href="#">1129</a>  |
| viewing trusted certificates .....                       | <a href="#">40</a>                          | What is an announcement .....                       | <a href="#">85</a>  |
| viewing usage by WebLM .....                             | <a href="#">1141</a>                        | What is an audio group .....                        | <a href="#">96</a>  |
| viewing usage summary .....                              | <a href="#">1145</a>                        | what is new in this release .....                   | <a href="#">17</a>  |
| viewing user roles                                       |   | What's new .....                                    | <a href="#">17</a>  |
| view user roles .....                                    | <a href="#">1196</a>                        | When to use Bridged Call Appearances .....          | <a href="#">230</a>   |
| VIP Caller .....   | <a href="#">494</a>                         | Whisper Page .....                                  | <a href="#">628</a>   |
| VIP Wakeup .....   | <a href="#">644</a>                         | Whisper Page Activation Access Code .....           | <a href="#">569</a>   |
| VIP Wakeup Reminder Call .....                           | <a href="#">506</a>                         | Whisper Page Tone Given To .....                    | <a href="#">628</a>   |
| VIP Wakeups Per 5 Minutes .....                          | <a href="#">644</a>                         | Wideband Support .....                              | <a href="#">748</a> , <a href="#">1024</a>  |
| Virtual Channel Identifier .....                         | <a href="#">870</a>                         | Wideband Support Options .....                      | <a href="#">757</a> , <a href="#">833</a>   |
| Virtual MAC Addresses .....                              | <a href="#">1059</a>                        | Wideband Switching .....                            | <a href="#">950</a>   |
| Virtual Path Identifier .....                            | <a href="#">870</a>                         | Width .....   | <a href="#">431</a> , <a href="#">833</a>   |
| VIS FEATURE OPTIONS .....                                | <a href="#">454</a>                         | Wink Timer (msec) .....                             | <a href="#">1009</a>  |
| VLAN .....   | <a href="#">675</a> , <a href="#">686</a>   | Wireless .....                                      | <a href="#">950</a>   |
|  |   | Without Flash .....                                 | <a href="#">598</a>   |



