Administering Avaya Aura® System Manager for Release 7.0

Release 7.0
Issue 3
November 2017

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

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 websites referenced within this site or documentation 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 Avaya hardware and software. 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 website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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 You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product 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 unless expressly authorized by Avaya. 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.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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 Toll 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 website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 24
Purpose 24
Intended audience 24
Document changes since last issue 24
Related resources 25
Documentation 25
Training 26
Viewing Avaya Mentor videos 27
Support 28
Warranty 28
Chapter 2: System Manager overview 29
New in this release 31
Out of Band Management in System Manager 33
New in the Communication Manager element 34
Infrastructure and serviceability updates 35
System Manager security enhancements 36
Log on to System Manager 36
Turning off the compatibility mode 36
System Manager web console 37
Logging on to the System Manager web console 38
Logon information for users with user name *admin* 38
Tenant Management web console 39
Password and security policies for all administrators 41
Password aging policy enforcement 41
Password strength policy enforcement 41
Password history policy enforcement 42
Password lockout policy enforcement 42
Inactive session termination policy 42
Change Password field descriptions 42
Logon warning banner 43
Editing password policies 43
Editing Session Properties 44
Security settings 44
Editing the logon warning banner 44
Customized interface 45
Adding the corporate logo 45
Password policies field descriptions 45
Session Properties field descriptions 47
Customized Interface field descriptions 48

Chapter 3: Directory synchronization 49
Directory synchronization overview 49
Results of synchronization from the LDAP directory server to System Manager 50
Results of synchronization from System Manager to the LDAP directory server 50
Limitations in the synchronization of the LDAP directory server 51
Adding the synchronization datasource 51
Editing the synchronization datasource 53
Deleting a synchronization datasource 54
User synchronization datasource field descriptions 54
Creating the user synchronization job 60
Scheduling a user synchronization job 61
Deleting a user synchronization job 61
User active synchronization job field descriptions 62
Synchronization job history 62
Synchronization job history field descriptions 62
Viewing Job Summary 63
Viewing Job Summary field descriptions 63
Chapter 4: Geographic Redundancy 65
Geographic Redundancy overview 65
Licensing in Geographic Redundancy 66
Architecture and deployment diagrams for Geographic Redundancy 66
Geographic Redundancy terminology 67
Geographic Redundancy replication 69
Prerequisites for servers on Appliance Virtualization Platform in the Geographic Redundancy setup 69
Prerequisites for System Manager on VMware in the Geographic Redundancy setup 70
Key tasks for Geographic Redundancy 71
Configuring Geographical Redundancy 73
Enabling the Geographic Redundancy replication 75
Disabling the Geographic Redundancy replication 76
Activating the secondary System Manager server 76
Deactivating the secondary System Manager server 78
Restoring the primary System Manager server 78
Reconfiguring Geographic Redundancy 81
Converting the primary System Manager server to the standalone server 83
About the Health Monitoring service 83
Configuring the timeout interval for health monitoring 84
Geographic Redundancy field descriptions 85
GR Health field descriptions 86
Configuring the GR-unaware elements to work with System Manager 88
Geographic Redundancy-unaware elements overview 88
Elements Geographic Redundancy manageability status matrix 89
Configuring various elements to change to the secondary System Manager 90

Introduction 90
Session Manager 6.3 configuration 90
Communication Manager configuration 93
CS 1000 configuration 96
Meeting Exchange configuration 99
Presence Server configuration 100
CallPilot configuration 101
Messaging configuration 102
Avaya Aura® Conferencing configuration 105
IP Office configuration 109
Visualization, Performance, and Fault Manager 112
Application Enablement Services 112
Avaya Aura® Contact Center 112
Avaya Multimedia Messaging configuration 112
Replacing System Manager servers 113
Replacement of System Manager servers 113
Moving the existing primary System Manager server to a different location 113
Restoring the primary System Manager server using the old primary server backup data 114
Restoring the primary System Manager server using the data on the secondary System Manager server 115
Replacing the secondary System Manager server on the site 116
Recovering the primary System Manager server from disaster 116
Chapter 5: Managing groups and roles for resources 119
Managing groups 119
Group management 119
Viewing groups 120
Creating groups 120
Modifying groups 121
Creating duplicate groups 121
Deleting groups 122
Moving groups 122
Synchronizing resources for a resource type 123
Assigning resources to a group 123
Searching for resources 124
Searching for groups 125
Filtering groups 125
Filtering resources 126
Removing assigned resources from a group 127
Group Management field descriptions 127
New Group field descriptions 129
View Group field descriptions 131
Edit Group field descriptions 132
Delete Group Confirmation field descriptions 134

Duplicate Group field descriptions.... 134
Move Group field descriptions.... 135
Resource Synchronization field descriptions.... 136
Managing resources.... 136
Manage resources.... 136
Accessing resources.... 136
Assigning resources to a new group.... 137
Adding resources to a selected group.... 138
Searching for resources.... 138
Filtering resources.... 139
Resources field descriptions.... 139
Choose Group field descriptions.... 141
Choose Parent Group field descriptions.... 142
Managing roles.... 143
Role Based Access Control.... 143
Built-in roles.... 143
Custom roles.... 147
Viewing user roles.... 147
Adding a custom role.... 148
Adding a custom tenant administrator role.... 149
Assigning permissions to access Solution Deployment Manager.... 150
Mapping permissions by using the template.... 152
Assigning users to a role.... 152
Unassigning users from role 153
Copying permission mapping for a role.... 153
Editing a custom role.... 154
Deleting custom roles.... 155
Roles field descriptions.... 155
Add New Role field descriptions.... 156
Role Details field descriptions.... 156
Add Mapping field descriptions.... 157
Assigned Users field descriptions.... 158
Permission mapping field descriptions.... 158
Permission mapping field descriptions.... 159
Chapter 6: Granular role based access control.... 160
Granular RBAC.... 160
Implicit permissions required for Communication Manager objects.... 161
Sample scenario for the range feature.... 163
Range in endpoints.... 163
Assigning range for endpoints.... 164
Assigning permissions in User Management.... 164
Assigning permissions through User Management.... 165
Field-level RBAC.... 166

Assigning permissions for fields in endpoints.......... 169

Chapter 7: Managing users, public contacts, and shared addresses.......... 171

Managing users.......... 171

Users, public contacts, and shared addresses.......... 171

Access to administrative users.......... 172

End user self provisioning.......... 173

Enabling self provisioning.......... 173

Changing the communication profile password from the self provisioning interface.......... 173

Viewing details of a user.......... 174

Creating a new user account.......... 175

Creating a new user profile using the user provisioning rule.......... 176

Results of using the user provisioning rule.......... 177

Modifying user accounts.......... 180

Creating duplicate users.......... 181

Removing user accounts.......... 182

Removing the deleted users from the database.......... 182

Editing users in bulk.......... 183

Viewing bulk user edit jobs.......... 183

Deleting the bulk user edit job.......... 184

Create new profile option.......... 184

User Provisioning Rules and User Bulk Editor.......... 185

User Bulk Editor field descriptions.......... 185

Filtering users.......... 194

Searching for users.......... 195

Assigning roles to a user.......... 195

Assigning roles to multiple users.......... 196

Removing roles from a user.......... 197

Assigning groups to a user.......... 197

Assigning groups to multiple users.......... 198

Removing a user from groups.......... 198

Viewing the deleted users.......... 199

Restoring a deleted user.......... 199

Assigning users to roles.......... 199

Unassigning users from role 200

Managing addresses.......... 200

Managing communication profiles.......... 204

Managing default contact list of the user.......... 222

Managing private contacts of a user.......... 229

User Management field descriptions.......... 241

User Profile View field descriptions.......... 244

New User Profile field descriptions.......... 257

User Profile Edit field descriptions.......... 277

User Profile Duplicate field descriptions.......... 295

User Delete Confirmation field descriptions........ 311
Assign Roles to Multiple Users field descriptions........ 311
Assign Roles field descriptions........ 312
Assign Groups field descriptions........ 312
Assign Groups to Multiple Users field descriptions........ 313
Deleted Users field descriptions........ 314
User Restore Confirmation field descriptions........ 315
Assign Users To Roles field descriptions........ 315
UnAssign Roles field descriptions........ 316
Managing bulk import and export........ 317
Managing public contacts........ 519
Manage public contact list........ 519
Adding a new public contact........ 519
Modifying details of a public contact 520
Deleting public contacts........ 520
Viewing the details of a public contact........ 521
Adding a postal address for a public contact........ 521
Modifying postal address of a public contact........ 522
Deleting the postal addresses of a public contact........ 522
Choosing a shared address for a public contact........ 522
Adding a contact address of a public contact........ 523
Modifying the details of a public contact........ 523
Deleting the contact address of a public contact........ 524
View Public Contact field descriptions........ 524
Edit Public Contact field descriptions........ 526
New Public Contact field descriptions........ 528
Public Contacts field descriptions........ 530
Managing shared addresses........ 531
Manage shared address........ 531
Assigning a shared address to the user........ 531
Adding a shared address........ 532
Modifying a shared address........ 533
Deleting a shared address........ 533
Add Address field descriptions........ 533
Edit Address field descriptions........ 534
Shared Address field descriptions........ 535
Managing presence access control lists........ 536
Manage Presence Access Control Lists........ 536
Presence ACL field descriptions........ 536
Communication profile password policy enforcement........ 538
Communication profile password policy........ 538
Editing the password policy for communication profile 538
Communication Profile Password Policy field descriptions........ 539

Chapter 8: Managing user provisioning rules 540
User Provisioning Rule 540
Capabilities and guidelines of user provisioning rules 541
Adding User Provisioning Rules 542
Creating the user provisioning rule 542
Modifying the user provisioning rule 543
Viewing the user provisioning rule 543
Creating a duplicate user provisioning rule 544
Deleting the user provisioning rule 544
User Provisioning Rules Management field descriptions 545
User Provisioning Rule field descriptions 545
Chapter 9: Managing elements 553
Registering CS 1000 or CallPilot with System Manager 553
Adding CallPilot to the element registry 553
Adding CallPilot certificate to System Manager 553
Importing users from Subscriber Manager to User Management 554
User data import to System Manager 554
Preparing the Subscriber Manager user data for import to User Management 555
Importing the Subscriber Manager user data to User Management 557
Subscriber Manager datasource parameters and attributes 558
Exporting the user data and creating the user profile 559
Importing users from CS 1000 Subscriber Manager to User Management 562
CS 1000 Subscriber Manager data import options 562
Preparing the CS 1000 Subscriber Manager user data for import to System Manager 562
Importing the CS 1000 Subscriber Manager user data to System Manager 562
Exporting the CS 1000 user data and creating the user profile 563
Preparing the CS 1000 Subscriber Manager user data for import to System Manager 563
Importing the CS 1000 UCM Subscriber Manager user data to System Manager 564
Exporting the CS 1000 user data and creating the user profile 565
Managing messaging 565
Messaging Class Of Service 565
Viewing Class Of Service 565
Class of Service List field descriptions 566
Messaging 566
Chapter 10: Managing Communication Manager 583
System Manager Communication Manager capabilities 583
Configuring Communication Manager user profile settings 584
Editing the Select All attribute in a table 585
Search component for Communication Manager objects 585
Managing Communication Manager objects 587
Communication Manager objects 587
Agents 591
Announcements 601

Audio Groups.......... 612
Vector Directory Number.......... 615
Vector Routing Table.......... 618
Coverage Path.......... 621
Coverage Time-of-day.......... 627
Element Cut-Through.......... 631
Endpoints.......... 632
Managing Off PBX Configuration Set.......... 680
Managing Off PBX Endpoint Mapping.......... 683
Xmobile Configuration.......... 685
Automatic Alternate Routing Digit Conversion.......... 690
Automatic Route Selection Digit Conversion.......... 693
Automatic Route Selection Toll.......... 696
Data Modules.......... 698
Class of service.......... 708
Authorization Code.......... 712
Class of Service Group.......... 714
Uniform Dial Plan Groups.......... 719
Uniform Dial Plan.......... 722
Usage options.......... 727
NRP Group.......... 729
Chapter 11: Managing IP Office.......... 733
IP Office Element Manager.......... 733
IP Office Element Manager.......... 733
Unlocking an IP Office device.......... 735
Starting the IP Office Element Manager.......... 735
Setting up System Manager to start IP Office element manager.......... 735
Setting up the environment variable in Windows XP to match the version of AdminLite.......... 737
Setting up the environment variable in Windows 7 to match the version of AdminLite.......... 738
Default login password for day one configuration of an IP Office device.......... 740
IP Office system configuration.......... 740
IP Office security configuration.......... 743
Backup and restore of the IP Office devices.......... 745
UCM or IP Office Application Server.......... 751
Voice Mail Pro Call Flow and System Configuration.......... 763
IP Office file transfer.......... 767
Transferring audio files to an IP Office device.......... 767
Transferring files to an IP Office device.......... 768
Uploading files to the System Manager repository.......... 768
Deleting an uploaded file.......... 769
IP Office file transfer field descriptions.......... 769
Initiating manual failback.......... 771
Failback policy.......... 771

Initiating failback 771
IP Office failback field descriptions 772
Upgrading IP Office 773
Overview of managing software 773
Get inventory 773
Analyzing the software 774
Downloading the software 774
Upgrading an IP Office device 775
Chapter 12: Managing backup and restore 777
Backup and restore 777
Disk space management for System Manager backup 778
Backup and restore on System Manager that is configured for Geographic Redundancy 778
Accessing the Backup and Restore service 779
Viewing list of backup files 779
Creating a data backup on a local server 780
Creating a data backup on a remote server 780
Scheduling a data backup on a local server 781
Scheduling a data backup on a remote server 782
Editing a scheduled backup job 782
Deleting the scheduled backup job 783
Restoring data backup from a local server 784
Restoring a backup from a remote server 785
Restoring the backup through the command line interface 786
Disk space required for backup 787
Time duration for backup and restore 787
Supported ciphers, key exchange algorithms, and mac algorithms 788
Backup and Restore field descriptions 789
Backup field descriptions 790
Schedule Backup field descriptions 791
Restore field descriptions 792
Chapter 13: Bulk import and export 794
Chapter 14: System Manager configuration 796
Managing data retention rules 796
Accessing the Data Retention Rules service 796
Data retention rules 796
Viewing data retention rules 796
Modifying data retention rules 797
Data Retention field descriptions 797
Configuring applications 798
Configuration management 798
View Profile: Agent Management field descriptions 798
View Profile: Alarm Management field descriptions 799
Configuring IP Office 800

IP Office profile field descriptions.... 801
View Profile: Communication System Management Configuration field descriptions.... 801
Edit Profile: Communication System Management Configuration field descriptions.... 802
View Profile: Event processor field descriptions.... 803
View Profile:Configuration field descriptions.... 804
View profile:Inventory field descriptions.... 805
Edit Profile:Inventory field descriptions.... 805
View and Edit profile Messaging field descriptions.... 806
View Profile: Data Transport Config field descriptions.... 807
View Profile: Data Transport Static Config field descriptions.... 810
View Profile SMGR field descriptions.... 810
Edit Profile:SMGR field descriptions.... 811
View Profile:Alarming UI field descriptions.... 811
Edit Profile:Alarming UI field descriptions.... 812
View Profile:Common Console field descriptions.... 813
Edit Profile:Common Console field descriptions.... 814
View Profile:Shutdown field descriptions.... 814
Edit Profile:Shutdown field descriptions.... 815
View Profile:HealthMonitor field descriptions.... 815
Edit Profile:HealthMonitor field descriptions.... 816
View Profile:Licenses field descriptions.... 816
Edit Profile:Licenses field descriptions.... 817
View Profile:Logging UI field descriptions.... 817
Edit Profile:Logging UI field descriptions.... 818
View Profile:Logging Service field descriptions.... 819
Edit Profile:Logging Service field descriptions.... 819
View Profile: SMGR Element Manager field descriptions.... 820
View Profile:SNMP field descriptions.... 822
View Profile:Scheduler field descriptions.... 823
Edit Profile:Scheduler field descriptions.... 823
Configuring the TrapListener service.... 824
TrapListener service field descriptions.... 824
View Profile: TrustManagement field descriptions.... 825
Edit Profile: TrustManagement field descriptions.... 826
View Profile: User Bulk Import Profile field descriptions.... 826
Edit Profile: User Bulk Import Profile field descriptions.... 828

Chapter 15: Managing inventory.... 831
Element management.... 831
Methods to add elements to System Manager.... 832
Manual addition of elements.... 832
Bulk import of elements.... 833
Discovering elements.... 834
Working with Elements in System Manager.... 850

Additional information required for creating the Communication Manager or Messaging element.... 850
Manage elements in System Manager configured with Geographic Redundancy.... 851
Determining the System Manager that manages a GR-aware element.... 851
Viewing details of an element.... 852
Modifying an element.... 852
Deleting an element.... 852
Exporting elements from the System Manager command line interface.... 853
runRTSCli.sh command.... 853
Assigning elements to an element.... 855
Removing assigned elements.... 855
Managing access profiles and ports.... 855
Managing and unmanaging elements from System Manager.... 858
Adding Platform type elements to System Manager.... 859
Adding System Platform to System Manager.... 859
Adding Application type elements to System Manager.... 860
Adding a Communication Manager instance to System Manager.... 860
Adding a Session Manager instance to System Manager.... 861
Adding a G430 or G450 gateway to System Manager.... 862
Field descriptions.... 862
Manage Elements field descriptions.... 862
Element details field descriptions.... 865
Delete Element Confirmation field descriptions.... 872
Import Elements field descriptions.... 872
Import Status field descriptions.... 875
Add Communication Manager field descriptions.... 876
Add IP Office field descriptions.... 879
Delete IP Office field descriptions.... 880
Other Managed Elements capabilities available in System Manager.... 881
Managing Serviceability Agents.... 881
Synchronization of Data.... 896
Communication Profiles synchronization.... 903
Configure options.... 907
Chapter 16: Managing events.... 909
Managing alarms.... 909
Alarming.... 909
Viewing alarms.... 909
Changing the alarm status.... 910
Exporting alarms.... 910
Deleting alarms.... 911
Filtering alarms.... 911
Searching for alarms.... 912
Configuring the throttling period alarm.... 912

Generating test alarms........ 913
Managing Geographic Redundancy related alarms........ 915
Alarming field descriptions........ 916
Alarming field descriptions........ 917
Managing logs........ 920
Logging service........ 920
Log Types........ 921
Managing log harvester........ 922
Managing log settings........ 936
Managing log viewer........ 942
TrapListener service........ 948
Chapter 17: Managing licenses........ 950
WebLM overview........ 950
Obtaining the license file........ 950
Accessing WebLM........ 951
Installing a license file........ 951
Client node locking........ 952
Viewing the license capacity and utilization of the product features 953
Viewing peak usage for a licensed product........ 953
Uninstalling a license file........ 954
Viewing the server properties........ 954
WebLM Home field descriptions........ 955
Install license field descriptions........ 955
View license capacity field descriptions........ 955
View peak usage field descriptions........ 956
Centralized licensing........ 957
About centralized licensing........ 957
Enabling centralized licensing........ 958
Configure centralized licensing field descriptions........ 958
Adding an element instance and assigning the element instance to a license file........ 959
Editing an element instance and license file assignment........ 960
Deleting an element instance........ 961
Element instance field descriptions........ 961
Disabling centralized licensing........ 962
Uninstall license field descriptions........ 962
Server Properties field descriptions........ 963
Enterprise licensing 963
Configuring enterprise licensing........ 963
Adding a local WebLM server........ 965
Modifying a local WebLM server configuration........ 966
Removing a local WebLM server........ 966
Viewing the license capacity of the licensed features of a product........ 967
Viewing the connectivity status of the local WebLM servers 967

Validating connectivity to local WebLM servers for a product.... 967
Viewing usage by WebLM.... 968
Viewing enterprise usage of a license feature.... 968
Viewing the periodic status of the master and local WebLM servers.... 969
Querying usage of feature licenses for master and local WebLM servers.... 969
Changing allocations of licensed features for a local WebLM server.... 970
Viewing allocations by features.... 970
Viewing allocations by the local WebLM server.... 970
Viewing usage summary.... 971
View by feature field descriptions.... 971
View by local WebLM field descriptions.... 972
Enterprise Configuration field descriptions.... 972
View Local WebLMs field descriptions.... 974
Add local WebLM field descriptions.... 975
Modify local WebLM field descriptions.... 976
Delete local WebLM field descriptions.... 978
Deletion of the local WebLM server.... 978
Usage Summary field descriptions.... 979
Usage by WebLM field descriptions.... 979
Enterprise Usage field descriptions.... 980
Query Usage field descriptions.... 981
Allocations by Features field descriptions.... 982
Allocations by Local WebLM field descriptions.... 983
Change Allocations field descriptions.... 984
Periodic Status field descriptions.... 985

Chapter 18: Data Replication Service.... 987
Data Replication Service.... 987
Synchronization in a Geographic Redundancy scenario.... 988
DRS client audit.... 988
Viewing replica groups.... 989
Viewing replica nodes in a replica group.... 989
Repairing a replica node.... 990
Repairing all replica nodes in a replica group.... 990
Viewing replication details for a replica node.... 990
Removing a replica node.... 991
Removing a replica node from the queue.... 991
Replica Groups field descriptions.... 991
Replica Nodes field descriptions.... 992
Replication Node Details field descriptions.... 995

Chapter 19: Managing reports.... 998
Reports.... 998
Reports Definition List field descriptions.... 998
Generating a detailed report.... 999

Generating a basic report.. 1000
New report field descriptions.. 1001
Editing report parameters.. 1003
Rerunning reports.. 1004
Customizing reports... 1004
Downloading reports.. 1005
Reports history field descriptions... 1006
Configuring email properties for reports.. 1006
Sending reports through email.. 1007
Deleting reports... 1007
Configuring report properties.. 1007
Remote server configuration... 1008
Adding a remote server.. 1008
Viewing the details of a remote server.. 1008
Editing the details of a remote server.. 1008
Deleting a remote server... 1009
Remote Server configuration field descriptions.. 1009
Chapter 20: Managing scheduled jobs... 1010
Scheduler.. 1010
Accessing scheduler.. 1011
Assigning permissions to access Scheduler... 1011
Viewing pending jobs.. 1012
Viewing completed jobs.. 1012
Viewing logs for a job... 1012
Filtering jobs.. 1013
Editing a job.. 1014
Deleting a job... 1014
Disabling a job... 1015
Enabling a job.. 1016
Stopping a job.. 1016
Pending Jobs field descriptions.. 1017
Completed Jobs field descriptions.. 1019
Job Scheduling-View Job field descriptions... 1021
Job Scheduling-Edit Job field descriptions.. 1022
Job Scheduling-On Demand Job field descriptions... 1024
Disable Confirmation field descriptions.. 1024
Stop Confirmation field descriptions... 1026
Delete Confirmation field descriptions.. 1027
Chapter 21: Templates.. 1028
Template management... 1028
Template versioning... 1028
Filtering templates... 1028
Upgrading a template... 1029

Adding CM Agent template 1030
Editing CM Agent template 1030
Viewing CM Agent template 1031
Deleting CM Agent template 1031
Duplicating CM Agent template 1031
Adding CM Endpoint templates 1032
Editing CM Endpoint templates 1032
Viewing CM Endpoint templates 1033
Deleting CM Endpoint templates 1033
Duplicating CM Endpoint templates 1034
Assigning permissions for CM templates 1034
    Adding subscriber templates 1035
Editing subscriber templates 1036
Viewing subscriber templates 1037
Deleting subscriber templates 1037
Duplicating subscriber templates 1037
Viewing associated subscribers 1038
Templates List 1038
Add Agent Template field descriptions 1041
Subscriber Messaging Templates field descriptions 1048
Subscriber CMM Templates field descriptions 1051
Subscriber MM Templates field descriptions 1053
Managing IP Office Endpoint template 1056
    Adding an IP Office endpoint template 1056
    Viewing an IP Office endpoint template 1057
    Editing an IP Office endpoint template 1057
    Duplicating an IP Office endpoint template 1058
    Deleting an IP Office endpoint template 1058
    Upgrading IP Office endpoint templates 1059
    IP Office endpoint template field descriptions 1059
Managing IP Office System Configuration template 1060
    Adding an IP Office System Configuration template 1060
    Viewing an IP Office System Configuration template 1061
    Editing an IP Office system configuration template 1061
    Deleting an IP Office system configuration template 1062
    Applying an IP Office system configuration template on an IP Office device 1062
    IP Office System Configuration template field descriptions 1063
    Manage audio files 1063
    Uploading an audio file 1064
    Converting an .WAV audio file to a .C11 audio file 1064
    Deleting an audio file 1065
    Manage Audio field descriptions 1065
Managing UCM and Application Server system configuration templates 1066

Adding a UCM and Application Server Configuration template.. 1066
Viewing a UCM and Application Server Configuration template...................................... 1067
Editing a UCM and Application Server Configuration template.. 1067
Deleting a UCM and Application Server Configuration template..................................... 1068
Applying a UCM and Application Server Configuration template..................................... 1069
UCM and Application Server Templates field descriptions... 1070
Managing VMPro system configuration templates.. 1070
Adding a VMPro System Configuration template... 1070
Viewing a VMPro System Configuration template.. 1071
Editing a VMPro System Configuration template.. 1071
Deleting a VMPro System Configuration template.. 1072
Applying a VMPro System Configuration template on a device.. 1072
Duplicating a VMPro System Configuration template... 1073
VMPro System Configuration Templates field descriptions.. 1074
Managing VMPro call flow templates.. 1074
Adding a VMPro Call Flow template.. 1074
Viewing a VMPro Call Flow template... 1075
Editing a VMPro Call Flow template.. 1075
Deleting a VMPro Call Flow template.. 1076
Applying a VMPro Call Flow template on a device.. 1076
Duplicating a VMPro Call Flow template.. 1077
VMPro Call Flow Templates field descriptions.. 1077
Chapter 22: Security.. 1079
Managing certificates... 1079
Trust Management.. 1079
Certificate generation and certificate management capabilities in System Manager.......... 1079
Setting the enrollment password... 1083
Managing trusted certificates... 1084
Managing identity certificates.. 1088
Retrieving the System Manager CA certificate... 1092
Certificate Authorities.. 1093
Enrollment Password field descriptions.. 1093
Trusted Certificates field descriptions... 1093
Add Trusted Certificate field descriptions.. 1094
View Trust Certificate field descriptions.. 1096
Delete Trusted Certificate Confirmation field descriptions.. 1096
Generating certificates from System Manager.. 1097
External SSL configurations in System Manager.. 1102
Configuring DTLS for CS 1000.. 1107
Configuring SIP TLS for CS 1000.. 1108
External authentication... 1108
External authentication.. 1108
Editing the authentication scheme... 1109

Provision the authentication servers.... 1110
Provisioning the LDAP server.... 1110
Provisioning the RADIUS server.... 1110
Provisioning the Kerberos server.... 1111
Provision LDAP/Radius/Kerberos server field descriptions.... 1112
SAML authentication.... 1113
Active sessions.... 1118
Viewing active sessions.... 1118
Terminating Single Sign-On sessions.... 1118
Chapter 23: Managing tenants.... 1120
Multi Tenancy.... 1120
Enabling Multi Tenancy.... 1121
Creating a tenant.... 1121
Assigning the tenant administrator to the tenant.... 1125
Unassigning the tenant administrator.... 1125
Viewing the tenant.... 1126
Modifying the tenant.... 1126
Deleting a tenant.... 1127
Multi Tenancy for Avaya SIP AST endpoints.... 1128
Multi Tenancy for Communication Manager objects.... 1128
Notes on Multi Tenancy for Communication Manager.... 1129
Tenant Management field descriptions.... 1132
Create Tenant field descriptions.... 1132
Chapter 24: Shutting down System Manager.... 1137
Overview.... 1137
Shutting down System Manager from the Web console.... 1138
Chapter 25: Solution deployment and upgrade.... 1139
Solution Deployment Manager.... 1139
Solution Deployment Manager overview.... 1139
Solution Deployment Manager options.... 1140
Solution Deployment Manager client.... 1141
Solution Deployment Manager.... 1145
Solution Deployment Manager configuration settings 1148
User settings.... 1148
Establishing PLDS connection to Avaya.... 1148
Establishing the connection to an alternate source.... 1149
User Settings field descriptions.... 1151
Software library management.... 1153
Software library.... 1153
Configuring external server as a remote software library for upgrades.... 1154
Creating a software library.... 1160
Editing a software library.... 1161
Viewing a software library.... 1161

Deleting a software library.......... 1161
Software library field descriptions.......... 1162
Viewing a file in the software library.......... 1164
Uploading a file to the software library.......... 1164
Deleting a file from the software library.......... 1165
Software library files field descriptions.......... 1166
System requirements for the external server.......... 1167
Solution Deployment Manager upgrades and updates.......... 1167
Refreshing elements.......... 1167
Analyzing software.......... 1168
Downloading the software.......... 1169
File Download Manager field descriptions.......... 1170
Performing the preupgrade check.......... 1171
Preupgrade Configuration field descriptions.......... 1171
Virtual machine management.......... 1173
Virtual machine management.......... 1173
Managing the location.......... 1173
Managing the host.......... 1179
Downloading the OVA file to System Manager.......... 1186
Managing the virtual machine.......... 1186
Monitoring a host and virtual machine.......... 1200
Managing vCenter.......... 1201
Upgrading Avaya Aura® applications.......... 1204
Upgrade Management overview.......... 1204
Avaya Aura® applications upgrade.......... 1205
Upgrade target release selection.......... 1206
Upgrading Avaya Aura® applications.......... 1207
System Manager upgrade management.......... 1219
Upgrading System Manager on a different server by using Solution Deployment Manager client.......... 1219
Upgrading System Manager on the same server by using Solution Deployment Manager client.......... 1221
Installing service packs and software patches on System Manager by using the Solution Deployment Manager client.......... 1223
Upgrade Management field descriptions.......... 1224
Add Element field descriptions.......... 1224
Edit Elements field descriptions.......... 1225
Upgrade Management field descriptions.......... 1226
Install on Same ESXi field descriptions.......... 1230
Upgrade job status.......... 1231
Upgrade job status.......... 1231
Viewing the **Upgrade** job status.......... 1231
Deleting the **Upgrade** jobs.......... 1231
Upgrade Job Status field descriptions.......... 1232

Upgrades to Communication Manager Release 6.3.100 1232
Communication Manager upgrades 1232
Checklist for upgrading Communication Manager to Release 6.3.100 1234
Getting inventory 1236
Analyze software 1237
Analyzing the software 1238
Downloading the software 1238
Performing a preupgrade check 1240
Preupgrade checks 1241
Preupgrade checklist for Linux® Operating System upgrades 1242
Pre-upgrade checklist for System Platform upgrades 1242
Hardware requirement checks during a preupgrade check 1243
Preupgrade status 1244
Upgrading Communication Manager 6.0, 6.1, or 6.2 to 6.3 1244
Upgrading Communication Manager 5.2.1 1257
Server support for Communication Manager Release 5.2.1 to 6.3.100 upgrades 1271
Upgrading TN boards 1272
Upgrading media gateways and media modules 1273
Downloading a file 1274
Upgrading Communication Manager 5.x 1275
Upgrading Communication Manager 5.x 1275
Updating Communication Manager 1276
Updating the SAMP/MPC firmware 1276
Protocol matrix for upgrades 1277

Chapter 26: Communication Manager Notify Sync 1279
Overview of the CM notify sync feature 1279
Downloading the System Manager certificate 1280
Downloading the pem file to Communication Manager 1281
Adding a trusted certificate to Communication Manager 1282
Configuring notify sync on Communication Manager 1283
Configure two-way TLS 1285
Adding the Communication Manager certificate to the System Manager trust 1285
Enabling two-way TLS in System Manager 1286

Chapter 27: Changing the IP address and FQDN in System Manager 1288
Verifying the deployment of extension packs 1288
Impact of change in FQDN and IP address on the Geographic Redundancy feature 1288
SSO login to remote machine fails 1289
Reimporting the SSO cookie domain value 1289
Changing the IP address or FQDN in System Manager 1290
Changing IP address or FQDN of managed elements on System Manager 1290
Changing the System Manager IP address in managed elements 1291
Changing the IP address and FQDN on the System Manager servers in Geographic Redundancy 1291

Change in IP address and FQDN on the primary and secondary System Manager servers 1291
Changing the IP address and FQDN on the primary System Manager when the secondary is in the standby or active mode...... 1292
Changing the IP address and FQDN on the primary System Manager server when the secondary is nonoperational...... 1293
Changing the IP address and FQDN on the secondary System Manager server when the secondary is in the standby or active mode...... 1294
Changing the IP address and FQDN on the secondary System Manager server when the primary is nonoperational...... 1295
Changing network parameters on System Manager running on VMware...... 1296
Changing the IP address, FQDN, DNS, Gateway, or Netmask address from CLI 1296
changeIPFQDN command...... 1297
System Manager command line interface operations...... 1298
Chapter 28: Configuring the date and time...... 1301
Verifying changes to the date and time configuration...... 1301
Configuring System Manager logs for Syslog server...... 1301
Changing date and time on System Manager running on VMware...... 1302
Configuring the NTP server...... 1302
Configuring the time zone...... 1302
Appendix A: Firewall implementation in System Manager...... 1303
Firewall basics...... 1303
Firewall implementation in System Manager...... 1303
Appendix B: Communication Manager reports available through System Manager... 1305
List reports...... 1305
Display reports...... 1310
List reports available in Avaya Aura® System Manager 7.0...... 1315
Status reports available in Avaya Aura® System Manager 7.0...... 1319
Commands that does not generates CSV reports...... 1321

Chapter 1: Introduction

Purpose

This document provides procedures for configuring Avaya Aura® System Manager and the Avaya Aura® applications and systems that System Manager manages.

Intended audience

The primary audience for this document is anyone who is involved with configuring, troubleshooting, maintaining, and verifying System Manager at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

Document changes since last issue

The following changes are made to this document since the last issue:

- Added the new and enhanced features in System Manager Release 7.0
- Added support for centralized Solution Deployment Manager.
- The following sections in Solution Deployment Manager:
    - Adding, editing, and deleting a location.
    - Adding, editing, and deleting an ESXI host.
    - Mapping the ESXi host to an unknown location.
    - Adding an ESXi host in vCenter.
- Added support to the following for Solution Deployment Manager client:
    - Deploying Avaya Aura® applications.
    - Upgrading System Manager.
    - Installing software patches for System Manager.

- Added support for adding a virtual machine to the host, starting, stopping, and restarting a virtual machine.
- View the status, stop, and delete the following upgrade-related jobs:
  - Get inventory
  - Analyze
  - Preupgrade
  - Upgrade
- Added support for the Solution Deployment Manager client.
- Added section Cleaning up the CS 1000 and CallPilot communication profiles.
- **November 2017:** Added section Supported ciphers, key exchange algorithms, and mac algorithms.

Related resources

Documentation

The following table lists the documents related to System Manager. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		
Avaya Aura® System Manager Overview and Specification	Understand high-level product features and functionality.	Customers and sales, services, and support personnel
Implementation		
Deploying Avaya Aura® System Manager in Virtualized Environment	Deploy the Avaya Aura® System Manager virtual application.	Implementation personnel
Installing the Dell™ PowerEdge™ R610 server, 03-603793	Install the Dell™ PowerEdge™ R610 server.	Implementation personnel
Installing the HP ProLiant DL360 G7 server, 03-603799	Install the HP ProLiant DL360 G7 server.	Implementation personnel
Installing the Dell™ PowerEdge™ R620 server	Install the Dell™ PowerEdge™ R620 server.	Implementation personnel
Installing the HP ProLiant DL360p G8 server	Install the HP ProLiant DL360p G8 server.	Implementation personnel

Table continues…

Title	Description	Audience
Maintenance and Troubleshooting		
Upgrading Avaya Aura® System Manager in Virtualized Environment	Upgrade the Avaya Aura® System Manager virtual application to Release 7.0.	System administrators and IT personnel
Avaya Aura® System Manager Fault Management and monitoring using SNMP	Monitor System Manager using SNMP.	System administrators and IT personnel
Troubleshooting Avaya Aura® System Manager	Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators and IT personnel

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title	Type
2007V/W	What is New in Avaya Aura® Release 7.0	AvayaLive™ Engage Theory
2008V/W	What is New in Avaya Aura® Application Enablement Services 7.0	AvayaLive™ Engage Theory
2009V/W	What is New in Avaya Aura® Communication Manager 7.0	AvayaLive™ Engage Theory
2010V/W	What is New in Avaya Aura® Presence Services 7.0	AvayaLive™ Engage Theory
2011/V/W	What is New in Avaya Aura® Session Manager Release 7.0 and Avaya Aura® System Manager Release 7.0	AvayaLive™ Engage Theory
2012V	Migrating and Upgrading to Avaya Aura® Platform 7.0	AvayaLive™ Engage Theory
2013V	Avaya Aura® Release 7.0 Solution Management	AvayaLive™ Engage Theory
1A00234E	Avaya Aura® Fundamental Technology	AvayaLive™ Engage Theory
1A00236E	Knowledge Access: Avaya Aura® Session Manager and Avaya Aura® System Manager Fundamentals	AvayaLive™ Engage Theory
5U00106W	Avaya Aura® System Manager Overview	WBT Level 1
4U00040E	Knowledge Access: Avaya Aura® Session Manager and System Manager Implementation	ALE License

Table continues…

Course code	Course title	Type
5U00050E	Knowledge Access: Avaya Aura® Session Manager and System Manager Support	ALE License
5U00095V	Avaya Aura® System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 1
5U00097I	Avaya Aura® Session Manager and System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 2
3102	Avaya Aura® Session Manager and System Manager Implementation and Maintenance Exam	Exam (Questions)
5U00103W	Avaya Aura® System Manager 6.2 Delta Overview	WBT Level 1

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on the System Manager software. For detailed terms and conditions, see the sales agreement or other applicable documentation. Additionally, for the standard warranty description of Avaya and the details of support, see **Help & Policies** > **Policies & Legal** > **Maintenance and Warranty Information** on the Avaya Support website at http://support.avaya.com. For additional information, see **Help & Policies** > **Policies & Legal** > **License Terms**.

For more details on the hardware maintenance for supported products, see http://portal.avaya.com/ptlWeb/services/SV0452.

Chapter 2: System Manager overview

System Manager is a central management system that delivers a set of shared management services and provides common console for Avaya Aura® applications and systems.

System Manager includes the following shared management services:

Service	Description
Solution Deployment Manager	Provides features for: • Deploy Avaya Aura® applications • Upgrade and migrate Avaya Aura® applications • Download Avaya Aura® applications • Install service packs, feature packs, and software patches for the following Avaya Aura® applications: - Communication Manager and associated devices, such as gateways, media modules, and TN boards. - Session Manager - Branch Session Manager - Utility Services - Appliance Virtualization Platform. The ESXi host running on Avaya-provided appliance. Provides features for Solution Deployment Managerclient: • Deploy Avaya Aura® applications. • Upgrade System Manager. • Install software patches for System Manager.
Users	Provides features to administer users, shared address, public contact list, and system presence access control list information. You can: • Associate the user profiles with groups, roles, and communication profiles. • Create a contact list. • Add an address and private contacts for the user.
User Provisioning Rules	Provides features to create rules called user provisioning rules. When the administrator creates the user using the user provisioning rule, the system

Table continues…

Service	Description
	populates the user attributes from the rule. The administrator requires to provide minimal information.
Bulk import and export	Provides features for bulk import and export of user profiles and global settings.
Directory synchronization	Provides features for bidirectional synchronization of user attributes from System Manager to the LDAP directory server.
Elements	Provides features by individual components of System Manager. Some links also provide access to generic features of System Manager, most of the links provide access to features provided by different components of System Manager.
Events	Provides features for administering alarms and logs generated by System Manager and other components of System Manager. Serviceability agent sends alarms and logs to SAL Gateway and System Manager, which in turn forwards the alarms and logs to the Avaya Data Center. You can view and change the status of alarms. You can view logs and harvest logs for System Manager and the components, and manage loggers and appender.
Geographic Redundancy	Provides features for handling scenarios when the primary System Manager server fails or the data network fragments. In such scenario, the system manages and administers elements such as Avaya Aura® Session Manager and Avaya Aura® Communication Manager, across the customer enterprise using the secondary System Manager server.
Groups and Roles	Provides features for administering groups and roles. You can create and manage groups, roles, and permissions.
Licenses	Provides features for administering licenses for individual components of Avaya Aura® Unified Communication System.
Security	Provides features for configuring the certificate authority.
System Manager data	Provides features for: • Backing up and restoring System Manager configuration data. • Monitoring and scheduling jobs. • Replicating data from remote nodes. • Configuring data retention settings and profiles for various services that System Manager provides.
Tenant Management	Provides features for: • Creating a tenant. • Editing tenant details. • Duplicating an existing tenant. • Deleting a tenant.

Related links

New in this release on page 31

New in this release

Avaya Aura® System Manager Release 7.0 supports the following new features and enhancements:

- Avaya offers the following:
    - Avaya-provided appliance: System Manager Release 7.0 with the Solution Deployment Manager service runs on an Avaya-provided appliance. Avaya-provided appliance contains server hardware and Appliance Virtualization Platform. Appliance Virtualization Platform contains the ESXi hypervisor and the application OVA.

      From Release 7.0, Avaya Aura® does not support templates.

      The new Common Server Release 2 servers that Avaya offers contain preinstalled Appliance Virtualization Platform. For the new S8300D or S8300E server installation, Appliance Virtualization Platform is installed at the customer site. In this offer, System Manager is a mandatory application.

      Release 7.0 does not support deploying or upgrading Avaya Aura® application to System Platform.
    - Virtualized Environment: Customers provide Virtualized Environment with a standard ESXi environment on which customers can deploy the System Manager and other Avaya Aura® virtual applications that Avaya provides.
- Solution Deployment Manager, a centralized capability to:
    - Deploy Avaya Aura® applications that System Manager supports
    - Upgrade and migrate Avaya Aura® applications, such as Communication Manager, Communication Manager Messaging, Utility Services, Session Manager, and Branch Session Manager to Release 7.0
    - Install service packs and software patches of Avaya Aura® applications
- The Solution Deployment Manager client that can be installed on the computer
- The Solution Deployment Manager client:
    - Deploy System Manager and other Avaya Aura® applications
    - Upgrade System Manager
    - Install System Manager software patches
- Support for the following web browsers:
    - Microsoft Internet Explorer Release 9.x, 10.x, and 11.x
    - Mozilla Firefox Release 36, 37, and 38

      Note:

      System Manager does not support Firefox releases earlier than 36.
- Virtual machine management:
    - Add an ESXi and Appliance Virtualization Platform host

    - Create and edit a location
    - Create and edit a virtual machine
    - Start, stop, and restart virtual machines
    - Map the ESXi host to an unknown location
    - Monitor CPU and memory usage of hosts and virtual machines
- View and delete the following upgrade-related jobs:
    - Refresh elements
    - Analyze
    - Pre-Upgrade check
    - Upgrade
    - Commit
    - Rollback
    - Uninstall
- Communication Manager 6.3.100 support that includes discovery, inventory, upgrade, update, and new MIBS.

    Note:

    For upgrades to Communication Manager 6.3.100, customer must reconfigure the SNMP alarming on the upgraded system.
- User Management enhancements: User Management interface displays administration fields that apply to administering tasks for applications that the customer solution supports. For example, if a customer solution contains only one Communication Manager, Session Manager, and Communication Manager Messaging, you cannot select more than one server. If a customer solution does not contain Conferencing servers, the Conferencing communication profile is unavailable for the administrator.
- Security enhancements: Integration of System Manager Release 6.3.8 Certificate Authority Generation Utility in System Manager Release 7.0.

    Supports SRVname in the **SubjectAltName** field. When you select this option, the system includes the service name in the certificate.
- SIP users and devices enhancements:
    - Scale increased to support 250000 SIP users from 125000 users
    - Scale increased to support 350000 SIP Endpoint devices from 150000 devices
    - Scale increased to support 28 instances of Session Manager from 12 instances of Session Manager
- Directory synchronization enhancements: LDAP synchronization of Active Directory administrator groups with System Manager administrator roles. The capability includes system roles and custom roles on System Manager.

- Bulk import and export enhancements:
  - Import and export of the CM Agent profile data of the user by using Excel and XML files.
  - Import and export of the Work Assignment profile by using Excel and XML files.
- Out of Band Management: The ability to separate management and nonmanagement network traffic across two physically or logically separated connections or both. With Out of Band Management, customers can keep the public type networking traffic away from the management interface.

  The example of System Manager management network traffic is the database replication with Session Manager.

  The example of System Manager nonmanagement or public network traffic is the client devices obtaining certificates through SCEP.
- Backup and restore on the SolarWinds (Windows) server.

Related links

System Manager overview on page 29
Out of Band Management in System Manager on page 33
New in the Communication Manager element on page 34
Infrastructure and serviceability updates on page 35
System Manager security enhancements on page 36

Out of Band Management in System Manager

Out of Band Management is two physically or logically separated network connections or both that connects to a private management network of the customer. The network connection provides secure management and administration of Avaya products. With Out of Band Management, you can separate the management network and data network traffic to System Manager.

System Manager provides the following network interfaces:

- The regular eth0 interface that was present in releases earlier than System Manager , is called the Management interface or Out of Band Management interface. The IP address is called as the Management IP address. The Management interface is mandatory for configuration.

  The following are the examples of System Manager Management network traffic:
  - Database replication with Session Manager
  - Element management. For example, Session Manager, Communication Manager, and Engagement Development Platform.
  - User management
  - Solution deployment, upgrades, and software patch install
- If Out of Band Management is enabled, then the public interface is configured with Public IP address and used for the nonmanagement traffic. This is an optional configuration.

The following are the examples of System Manager nonmanagement or public network traffic:

- End-user self-provisioning
- Client devices getting certificates through SCEP
- Tenant Management

Out of Band Management configuration persists across System Manager upgrades, updates, and restarts.

For configuring Out of Band Management in System Manager, System Manager must be installed on an Appliance Virtualization Platform host that is configured with Out of Band Management. Out of Band Management is enabled during the deployment of Appliance Virtualization Platform.

Out of Band Management in a Geographic Redundancy setup

When you configure Geographic Redundancy, provide Management network details only. Validation fails if you configure Geographic Redundancy with Public network details. In Geographic Redundancy setup, you do not disable or enable Out of Band Management on both primary and secondary System Manager virtual machine. You can enable Out of Band Management on the primary System Manager virtual machine and disable Out of Band Management on the secondary System Manager virtual machine, and vice versa.

Restoring System Manager backup

While restoring backup on System Manager with different Out of Band Management network details, the restore operation fails at validation phase.

Tenant Management on Out of Band Management-enabled System Manager

By default, the Multi Tenancy feature is disabled on System Manager when Out of Band Management is enabled. You must enable Multi Tenancy on Out of Band Management-enabled System Manager for the Tenant Management administrator to manage tenant users.

Related links

New in this release on page 31

New in the Communication Manager element

Managing Communication Manager

You can add buttons to Communication Manager SIP endpoints from **Endpoints** > **Manage Endpoints** on System Manager. You can configure the following on SIP endpoints:

- Triple Ringer type for the Call Pickup button
- Service Observe button
- Enable Listen-only and Coach option on Service Observe button
- Add VOA repeat button
- Add and remote agent skills
- Enable reachability for the domain control SIP stations
- Create single administration for dual registration

- Enable automatic call routing

Managing Media Server

You can manage the Media Serverin the following ways:

- Adding Media Server
- Viewing Media Server
- Editing Media Server
- Deleting Media Server

Communication Manager status and performance reports

With the reports feature, you can gather predefined detailed measurement, performance, and status data for Communication Manager attributes. You can use the new performance-based reports for serviceability, maintenance, and troubleshooting of Communication Manager.

About 140 predefined list and display Communication Manager performance measurement and status reports are added to System Manager 7.0

With the new List and Display Measurement and Status Reports, customers using ASA, MSA, or FPM report feature can have the same services and capabilities after migration to System Manager.

Related links

New in this release on page 31

Infrastructure and serviceability updates

While upgrading to Avaya Aura® System Manager7.x, you can also upgrade the following third-party applications:

- Move System Manager and standalone WebLM from Oracle JRE to Open JDK
- Update to CentOS 6.5
- Update to PostgreSQL 9.3.4
- Update the supported browsers
- Update standalone WebLM version of Tomcat Server to 8.0.x

The output of the `swversion` command displays the version of software that is running on the System Manager server.

Depending on the application and the customer solution, the User management page displays only the administration fields that are applicable.

Related links

New in this release on page 31

System Manager security enhancements

System Manager 7.0 enhanced its security as follows:

- System Manager 6.3.8 Certificate Authority Generation Utility integration with System Manager7.0: The CLI-based CA Generation utility to support customers who want to update the certificates from SHA1 and RSA 1024 to SHA2 and RSA 2048. However, if the administrator wants to generate a new SHA2 CA, then the trust with the older elements breaks. The administrator must reestablish the trust with the new CA.
- Support for SRVname in the **SubjectAltName** field: The Support SRVname option includes the service name in the certificate when you select the check box. By default, the **Support SRVname** check box is clear.

Related links

New in this release on page 31

Log on to System Manager

Turning off the compatibility mode

About this task

You might not be able to view the status of some operations on the webpages using Microsoft Internet Explorer because Internet Explorer imposes a time-out limit for the server to return the data. To correct this problem, you must install the patch for Internet Explorer from the Microsoft website at http://support.microsoft.com/kb/181050%20.

If the compatibility mode is turned on, some System Manager features might not work in Internet Explorer version 8 onwards. Therefore, you must turn off the compatibility mode.

Procedure

1. On the menu, click **Tools** > **Compatibility View Setting**.
2. In the Compatibility View Settings dialog box, clear all check boxes.
3. Ensure that the **Websites you've added to Compatibility View** field does not contain the address of the System Manager website.

Related links

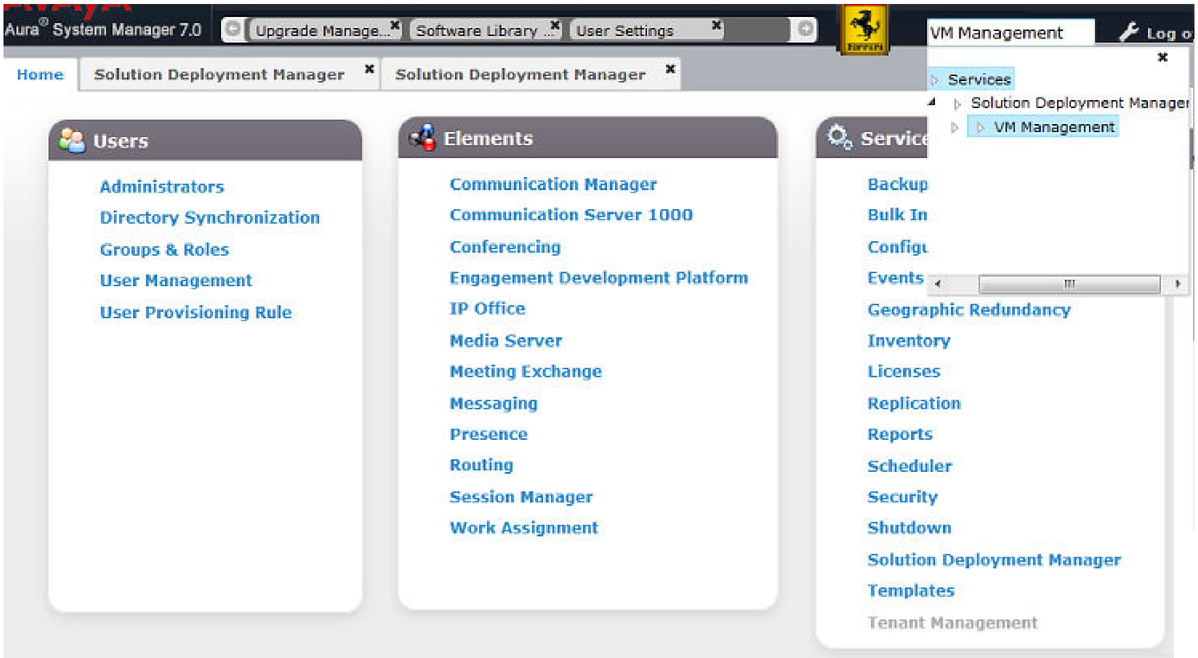
System Manager overview on page 29

System Manager web console

System Manager provides centralized access to all Avaya Aura® elements through a browser-based Avaya management console with Single Sign-on.

The System Manager web console provides the following:

- Corporate logo: You can add a logo on the web console.
- **Settings** icon (🔧): You can navigate to **Help**, **About**, and **Change Password** links.
- User Preference: You can add a page as your preference by using the plus sign (+) in the top-right corner. The web console displays the link to the page on System Manager. You can delete the user preferences.
- Quick Navigator: You can type the name of the link that you want to search. The web console displays all related links with the search text in the top-right corner of the page. You can click a link to navigate to the specific page.
- A message on the web console that prompts you to restart the System Manager virtual machine after a patch installation if the kernel is upgraded.



The Administrators link opens on the same System Manager window in a separate tab.

Related links

System Manager overview on page 29

Logging on to the System Manager web console

Before you begin

Obtain a user account to log on to the System Manager web console. If you do not have a user account, go to the Avaya Support website at https://support.avaya.com to create your account.

About this task

The System Manager web console is the main interface of Avaya Aura® System Manager. You must log on to System Manager web console to perform any task. The System Manager home page displays the navigation menu that provides access to shared services to perform various operations that System Manager supports. The tasks that you can perform depend on the role that you are assigned with.

Important:

On the System Manager web console, to navigate to the previous page, do not use the back arrow on the upper-left corner of the browser. If you click the back arrow, the system might not return to the previous page and might display an error.

Procedure

1. On the web browser, enter the System Manager URL `https://<Fully Qualified Domain Name>/SMGR`.
2. In the **User ID** field, type the user name.
3. In the **Password** field, type the password.
4. Click **Log On**.

   The system validates the user name and password with the System Manager user account.

   - If the user name and password match, the system displays the System Manager home page with the System Manager <*version_number*>.
   - If the user name and password does not match, System Manager displays an error message and prompts you to enter the user name and password again.

Related links

System Manager overview on page 29

Logon information for users with user name *admin*

This logon information applies only to users with the user name, admin.

- After installation, when you log on to System Manager for the first time, enter `admin123` as the default password.

  The system displays the Forced Change Password page. The Forced Change Password page does not contain the **Cancel** button. You must change the password when you log on to the system by using the default password.

- After an upgrade, when you log on to System Manager, you must reset the password.
- If you gain access to System Manager using the IP address and you log on to the system as admin for the first time, click **Change Password** to change the password.

Note:

The password must contain a combination of alphanumeric and special characters. For more information about the password strength policy, see Password strength policy enforcement.

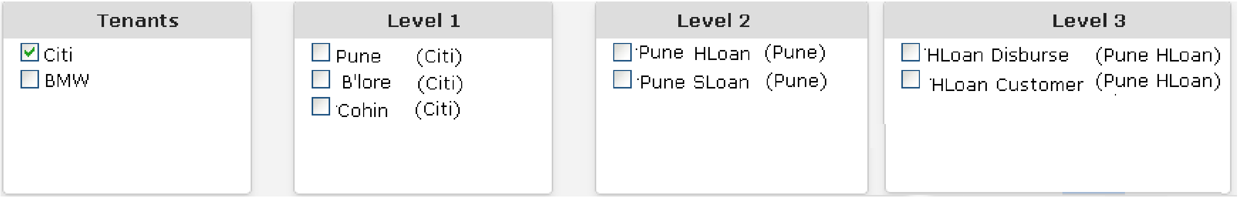
Related links

System Manager overview on page 29
Password strength policy enforcement on page 41

Tenant Management web console

From System Manager web console, the user with tenant administrator permissions can perform the following:

- View all tenants in the Tenants panel for which the tenant administrator has permissions. By default, the system selects the first tenant in the list.

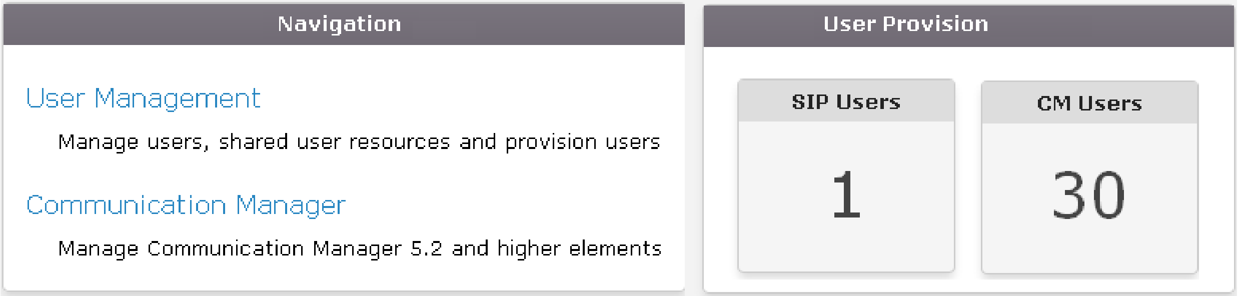


Tenants	Level 1	Level 2	Level 3
☑ Citi	□ Pune (Citi)	□ Pune HLoan (Pune)	□ HLoan Disburse (Pune HLoan)
□ BMW	□ B'lore (Citi)	□ Pune SLoan (Pune)	□ HLoan Customer (Pune HLoan)
	□ Cohin (Citi)		

- View all child levels of the selected item in the subsequent panel.
  - When the tenant administrator selects an item, the system:
    - Selects all parent items of the selected item.
    - Displays the child levels of the selected item in the subsequent panel.
  - When the tenant administrator clears all selections in a panel, the system displays the default selection.

  Note:

  Select at least one tenant. If you do not select a tenant, the system displays a message.
- Gain access to:
  - User Management
  - Communication Manager. Only if the role has permissions to Communication Manager.



Navigation

User Management

Manage users, shared user resources and provision users

Communication Manager

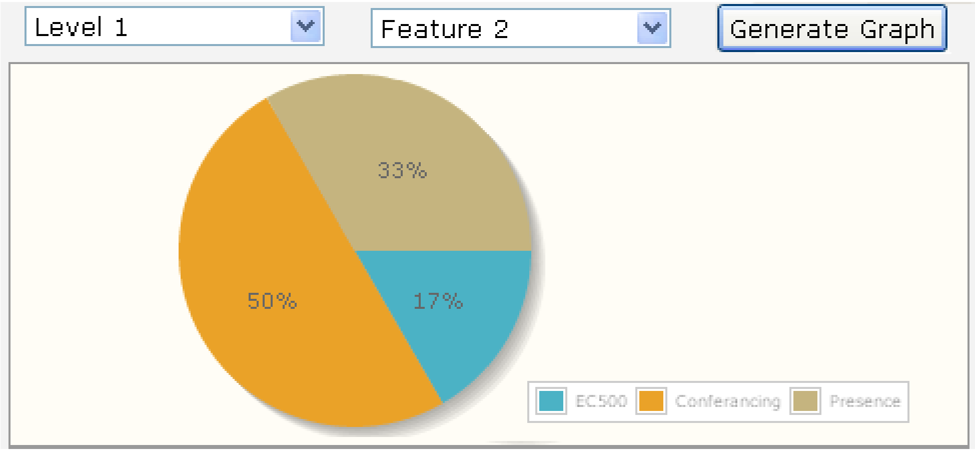
Manage Communication Manager 5.2 and higher elements

User Provision

SIP Users	CM Users
1	30

- View the **User Provision** section that displays the number of SIP users and H.323 users to which the tenant administrator has permissions.
- Select the organizational hierarchy of the tenant and features in the **Graph** section and, generate graphs.

  The features include EC500, Presence, Conferencing, H.323 users, and SIP users. The system generates Pie charts based on the user selection. If the tenant administrator does not select a level from the Organization level field, the system generates graphs based on items selected in the panels.



Related links

System Manager overview on page 29

Multi Tenancy on page 1120

Password and security policies for all administrators

Password aging policy enforcement

The password aging policy has the following time-based password thresholds:

- Minimum password age
- Password expiration warning
- Password expiration

The system administrator configures the password threshold in days.

Password threshold	Result of the expiry of the password aging policy threshold
Minimum password age	You cannot change the password until the minimum password age is reached. For example, you cannot change the password within 3 days after the last change was made.
Password expiration warning	The system sends a password expiration warning when the password is about to expire and before the password expires.
Password expiration period	The system prompts you to change the password after the threshold for the password expires and before the threshold to disable the account. The password remains locked until the system administrator resets the password.

Related links

System Manager overview on page 29

Password strength policy enforcement

The password strength policy that the system administrator defines enforces the following constraints:

- Passwords must be 6 to 25 characters long. The default character length is eight.
- Passwords must contain a combination of the following characters: a-z,A-Z,0-9,{}|()<>,/.=[]^_@!$%&-+":?`\;
- Passwords do not require a minimum character type. However, the default is one lowercase character and one uppercase character, one numeric character, and one special character. The sum cannot exceed the minimum total length.
- Password must not contain a character repeated more than twice consecutively.
- Passwords must not be your user ID, in forward or reverse order.

When you enable the password strength policy, if the password does not meet the password strength policy, the system rejects the password.

You can can disable the password strength policy.

Related links

System Manager overview on page 29

Password history policy enforcement

The password history policy verifies that a password is new. The blocked passwords can range from 1 to 99. The default is six.

Related links

System Manager overview on page 29

Password lockout policy enforcement

The lockout policy provides a limit on the number of unsuccessful attempts that you can make to access System Manager. The system locks System Manager for use after a specified number of logon attempts. By default, if you make consecutive attempts within a 10-minute period, the system locks you out for 2 minutes after five unsuccessful attempts.

Related links

System Manager overview on page 29

Inactive session termination policy

By default, the system suspends a user session after 30 minutes of inactivity. When the session becomes inactive, to access System Manager, you must log on to System Manager again.

Related links

System Manager overview on page 29

Change Password field descriptions

Use this page to change the password for your account.

Name	Description
Current password	The existing password.
New password	The new password that you must set.
Confirm new password	The new password that you have set.

Button	Description
Save	Changes the password.

Table continues…

Button	Description
Cancel	Cancels the change password operation and closes the Change Password page.

Related links

System Manager overview on page 29

Logon warning banner

System Manager provides the text for the logon warning banner that a system administrator can change.

Related links

System Manager overview on page 29

Editing password policies

About this task

Only an administrator can edit the password settings.

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Security** > **Policies**.
3. In the **Password Policy** section, click **Edit**.
4. On the Password Policy page, edit the required fields.
5. Click **Save**.

   To undo your changes and return to the previous page, click **Cancel**.

   ❗ **Important:**

   The system displays a message about the invalid logon in the following scenarios:

   - If you use a disabled account to log on.
   - If the password is invalid.
   - If you have exceeded the maximum number of failed logon attempts limit.
   - If the password expires.

   For more information on password policies, contact the system administrator.

Related links

System Manager overview on page 29
Password policies field descriptions on page 45

Editing Session Properties

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Security** > **Policies**.
3. On the Policies page, in the Session Properties section, click **Edit**.
4. On the Session Properties page, edit the required fields.
5. Click **Save**.

Related links

System Manager overview on page 29
Session Properties field descriptions on page 47

Security settings

System Manager provides a customizable logon banner that appears when a user logs on to the system. Customers who have security policies that require the network equipment to display a specific message to users when users log on by using the customizable banner.

Related links

System Manager overview on page 29

Editing the logon warning banner

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Security** > **Policies**.
3. On the Policies page, in the **Security Settings** section, click **Edit**.
4. On the Security Settings page, edit the text as required in the Logon Warning Banner text area.

   Note:

   You can enter a maximum number of 2500 characters.
5. Click **Save**.

Related links

System Manager overview on page 29

Customized interface

System Manager provides the feature to add a logo to the System Manager web interface. Organizations can customize the logo without removing the Avaya logo.

Related links

System Manager overview on page 29

Adding the corporate logo

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Security** > **Policies**.
3. On the Policies page, in the **Customized Interface** section, click **Edit**.
4. On the Customized Interface page, in the **Upload File** section, click **Browse** and select an image file that you want to upload.

   The system supports PNG, GIF, and JPEG image file formats. The image dimensions must be 100x51 pixels.
5. In the **Change Image ALT Attribute** section, type the alternate text that you want the system to display.
6. Click **Save**.

   System Manager web console displays the corporate logo on the upper-right corner of the page.

Related links

System Manager overview on page 29
Customized Interface field descriptions on page 48

Password policies field descriptions

This page is applicable only for users with the user name admin.

Aging section

Field	Description
Enforce password aging policies	The option to enforce the aging policies.
Enable expired password change	The option to change password after it expires.

Table continues…

Field	Description
Expiration period	The maximum allowable days to maintain the password. The default is 90 days. You can type a value from 1 to 365.
Expiration warning	The warning message that must be sent to the user when the password is about to expire. You can type a value from 1 to 15. The default is 7.
Minimum age	The minimum allowable days for password age. You can type a number from 0 to 7. The default is 3. Ensure that the expiration period is greater than the minimum password age.

History section

Field	Description
History	The option to enforce policies against previously used passwords.
Previous passwords blocked	The number of passwords the system maintains in the history. You cannot set your password to the old values. The default is 6.

Strength section

Field	Description
Strength	The option to enforce password content standards.
Minimum Total Length	The minimum number of characters that you can use in the password. The default value is 8. Set the password with 6-25 characters.
Minimum by character Type: Lower case	The minimum number of lowercase characters required in the password. The default value is 1.
Minimum by character Type: Upper case	The minimum number of uppercase characters required in the password. The default value is 1.
Minimum by character Type: Numeric case	The minimum number of numeric characters required in the password. The default value is 1.
Minimum by character Type: Special case	The minimum number of special characters required in the password. The default value is 1.

Lockout section

Name	Description
Lockout	The option to enforce lockout after failed login attempts.
Consecutive Invalid Login Attempts	The number of failed attempts before lockout. Type a value from 1 through 20. The default is 3.

Table continues…

Name	Description
Interval for Consecutive Invalid Login Attempts	The time interval in minutes between invalid login attempts. Type a value from 0 through 120. The default is 10 minutes.
Lockout Time	The number of minutes that the account must be locked after invalid login attempts. Type a value from 0 through 120. The default is 2 minutes.

Button	Description
Save	Saves all the entries on the Edit Password Policies page.
Cancel	Ignores your changes and returns to the previous page.

Related links

System Manager overview on page 29

Session Properties field descriptions

Name	Description
Maximum Session Time	The maximum time in minutes a session can remain active. The valid values are 10 through 1440.
Maximum Idle Time	The maximum time in minutes a session can remain idle. The valid values are 10 through 1440. **Note:** • It is mandatory to set the session idle time out to 10 minutes before you run a security scan against System Manager by using tools like Nessus or IBM AppScan. • The maximum idle time must not exceed the maximum session time.

Button	Description
Save	Saves the changes on the Session Properties page.
Cancel	Ignores your changes and returns to the previous page.

Related links

System Manager overview on page 29

Customized Interface field descriptions

Upload file

Button	Description
Browse	Displays the File Upload dialog box where you navigate to the image file. **Note:** The system supports PNG, GIF, and JPEG file formats. The dimensions of the image must be 100x51 pixels.

Change Image ALT Attribute

Field	Description
Image ALT Attribute	The alternate text for the image that you uploaded. **Note:** The text must be up to 20 characters.

Button	Description
Save	Saves the image on the server and displays the image on System Manager web console.
Cancel	Ignores your changes and returns to the previous page.

Related links

System Manager overview on page 29

Chapter 3: Directory synchronization

Directory synchronization overview

System Manager integrates with a number of Lightweight Directory Access Protocol (LDAP) directory servers to provide the following functions:

- Synchronization of users from the LDAP directory server to System Manager User Management.
- Bidirectional synchronization of the selected user attributes from System Manager to the LDAP directory server.

LDAP supports the following directory servers for synchronization:

- Active Directory 2003
- Active Directory 2008
- Active Directory 2012
- OpenLDAP 2.4.21
- IBM Domino 7.0
- Novell eDirectory 8.8
- SunOne Directory/Java System Directory 6.3

From the System Manager web console, you can run the directory synchronization engine as an on-demand job. You can also schedule the data synchronization to and from the enterprise directory. During synchronization of information to the enterprise directory server, System Manager modifies the user data that is stored in the LDAP directory server.

From the System Manager web console, you can configure bidirectional attribute mapping through the Directory Synchronization user interface. The bidirectional synchronization does not synchronize the user in the LDAP directory synchronization that is created from the System Manager web console and the System Manager bulk import utility. The bidirectional synchronization only synchronizes the attributes for the user that you synchronized from the LDAP directory server.

You can perform LDAP synchronization of Active Directory administrator roles with System Manager administrator roles. The capability includes system roles and custom roles on System Manager.

Synchronization by using the user provisioning rule

You can synchronize the communication data, such as extensions, Messaging mail box, and telephone numbers, by using the user provisioning rule. You can map the user provisioning rule to more than one LDAP attribute. However, you cannot map the user provisioning rule to the same LDAP attribute twice.

Results of synchronization from the LDAP directory server to System Manager

You can expect the following results when you run the directory synchronization job or when the system runs the scheduled job.

Action	Provided	Expected result
Create a new user in the LDAP directory server.	Add the user in the filter criteria.	The system synchronizes the user in System Manager.
Update the user attributes in the LDAP directory server.	The system adds the attributes in the mappings for the data source.	The system updates the user attributes in System Manager.
Change the filter criteria.	Remove the user from the filter criteria, and select the **Allow Deletion** check box.	The system permanently deletes the user from System Manager.
Delete a user in the LDAP directory server.	Select the **Allow Deletion** check box for the data source , and leave the filter criteria unchanged.	The system permanently deletes the user from System Manager.

Results of synchronization from System Manager to the LDAP directory server

You can expect the following results when you run the directory synchronization job or when the system runs the scheduled job.

Action	Provided	Expected result
Update the user attributes that are synchronized from LDAP directory server in System Manager.	The system adds the attributes in the mappings for that datasource, and the mapping synchronizes from System Manager to the LDAP directory server.	The system updates the user attributes in the LDAP directory server.

Limitations in the synchronization of the LDAP directory server

You can expect the following results when you run the directory synchronization job or when the system runs the scheduled job.

Table 1: Synchronization from the LDAP directory server to System Manager

Action	Expected result
Synchronize users from multiple LDAP directory servers.	The system creates different datasources for each directory server. The system supports the authentication of two directory servers, the RADIUS server and the KERBEROS server, at a given point of time.
Modify the user attributes that the LDAP directory server synchronizes.	If you add the attributes in mappings for the datasource, the system overwrites the attributes from the synchronization job.

Table 2: Synchronization from System Manager to the LDAP directory server

Action	Expected result
Create a user in System Manager from the User Management interface or by using the bulk import operation.	The system does not synchronize the user in the LDAP directory server.
Update the user attributes synchronized from the LDAP directory server in System Manager.	If you add the attributes in mappings for the datasource, the system updates the attributes in the LDAP directory server. You can synchronize only optional attributes from System Manager to the LDAP directory server.
Delete users in System Manager.	The system does not delete the user from the LDAP directory server. The Directory Synchronization feature does not support the soft deletion or permanent deletion of the user from the LDAP directory server. The system synchronizes the user in System Manager even after you permanently delete the user.

Adding the synchronization datasource

Procedure

1. On the System Manager web console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.

3. On the User Synchronization page, click the **Synchronization Datasources** tab.
4. Click **New**.
5. On the New User Synchronization Datasource page, complete the fields in the **Directory Parameters** section.
6. Click **Test Connection**.

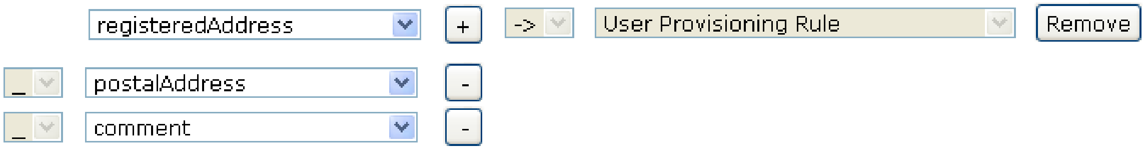
   If the connection fails, the system displays an external directory error message.

   If the connection is successful, the system displays the status icon. Click the status icon to view the message. Continue with the next step to map attributes in System Manager to LDAP attributes.

   The system displays five mandatory attributes of System Manager that are read-only values.
7. To add more attributes, click **Add Mapping**.

   You can use an appropriate LDAP attribute to synchronize in System Manager. If the LDAP attributes that you select are invalid, the synchronization fails.
8. To add the user provisioning rule attribute, perform the following:
   1. Click **Add Mapping**, and select **User Provisioning Rule** from System Manager.

      You cannot add the User Provisioning Rule attribute more than one time. After you select **User Provisioning Rule**, the system displays the User Provisioning Rule attribute as read-only.
   2. Select an LDAP attribute that you map to the user provisioning rule.

   3. To add more than one LDAP attribute, click plus (+).

      You can map more than one LDAP attribute to the user provisioning rule attribute. When you map more than one attribute, the system appends the second and third attributes to the first LDAP attribute. For example, asia_pune_maint.
9. Click **Save**.

   Note:

   - For bidirectional synchronization of data in the LDAP directory with System Manager, select the two-way arrow icon in the **Attribute Parameters** section.
   - The user provisioning rule data synchronization is unidirectional from the LDAP directory server to System Manager.
   - In System Manager, you cannot create a user in Active Directory. With bidirectional synchronization, you can only edit the existing user in Active Directory.

During attribute mapping, the right arrow indicates that the system synchronizes from the LDAP server to System Manager. The left arrow indicates that the system synchronizes from System Manager to the LDAP server.

Related links

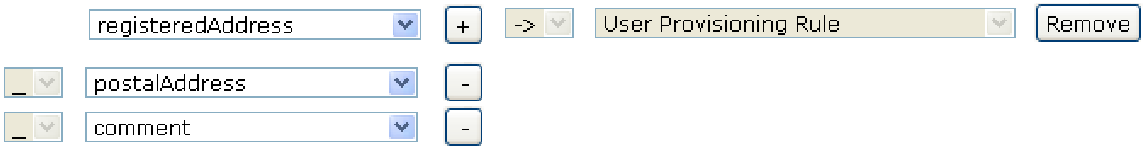
User synchronization datasource field descriptions on page 54
Results of using the user provisioning rule on page 177

Editing the synchronization datasource

Procedure

1. On the System Manager web console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Synchronization Datasources** tab and click the record that you must edit.
4. Click **Edit**.
5. On the Edit Synchronization Datasource page, change the required fields.
6. To modify the user provisioning rule attribute:
    a. To add an LDAP attribute, click the plus (+).

    You can map more than one LDAP attribute to the user provisioning rule attribute. When you map more than one attribute, the system appends the second and third attributes to the first LDAP attribute. For example, asia_pune_maint.

    You cannot add the User Provisioning Rule attribute more than one time. After you click **User Provisioning Rule**, the system displays the User Provisioning Rule attribute as read-only.

    b. To remove the LDAP attribute, click the minus (-).
7. Click **Save**.

Related links

User synchronization datasource field descriptions on page 54
Results of using the user provisioning rule on page 177

Deleting a synchronization datasource

Procedure

1. On the System Manager web console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Synchronization Datasources** tab and click a record to delete.
4. Click **Delete**.

   ✱ **Note:**

   If you synchronize a user by using the datasource that you selected for deletion, the delete operation fails. The system display the message `Data Source <Datasource Name> cannot be deleted as at least one enterprise CsUser references it.`

User synchronization datasource field descriptions

Directory Parameters

Field	Example values	Description
Datasource Name	Win2K8ADA	The name to identify an active directory. You might require the name later to create a synchronization job.
Host	148.147.163.131	The IP address or the host name of the directory server that you synchronize users with.
Principal	CN=Administrator,CN=Users,DC=pansv8,DC=platform,DC=avaya,DC=com	The user name of the active directory that has permissions to create or update users.
Password	<password>	The password to connect to the active directory.
Port	389	The port number of the active directory The default port is 389 for a non-SSL connection and 636 for an SSL connection.
Base Distinguished Name	CN=Users,DC=pansv8,DC=platform,DC=avaya,DC=com	An element that works with the search scope or the hierarchy from where you synchronize the users.
LDAP User Schema	inetOrgPerson	The schema that defines object classes by a list of attributes where the values are mandatory or optional. The schema might differ depending on your Active Directory. The default value is inetOrgPerson.

Table continues…

Field	Example values	Description
Search Filter	(cn=Alex*)	The field that provides a mechanism to define the criteria for matching entries in an LDAP search operation. For more information about Search filter, see http://msdn.microsoft.com/en-us/library/windows/desktop/aa746475(v=vs.85).aspx.
Use SSL	False when you clear the check box	The option to use SSL to connect to Active Directory. The default port for an SSL connection is 636. **Important:** When you add the certificate, you must select the **Import using TLS** option. For more information about setting up the SSL connection, see Adding trusted certificates.
Allow Deletions	False when you clear the check box	The option to delete a synchronized user that is already removed from Active Directory.
Test Connection	-	The option to verify your LDAP connection. Test the connection before you map attributes.

Attribute Parameters

When you click **Test Connection** and after the test is complete, the system displays the LDAP attributes that you can administer.

When you remove the following attributes from the mapping page, the system does not remove the communication profile handle of the user:

- email
- otherEmail
- Microsoft Exchange Handle
- Microsoft SIP Handle
- IBM Sametime Handle

LDAP Attribute	System Manager Attribute	Description
objectGUID	sourceUserKey	The attribute that uniquely defines a user.
userPrincipalName	loginName **Note:** If you are using Microsoft Active Directory for external authentication with System Manager, the attribute userPrincipalName of the	The attribute that defines the login name in System Manager.

Table continues…

<table>
<tr><th>LDAP Attribute</th><th>System Manager Attribute</th><th>Description</th></tr>
<tr><td></td><td>user in the external server must contain a valid value.</td><td></td></tr>
<tr><td><b>sn</b></td><td>surname</td><td>The attribute that defines the last name of the user.</td></tr>
<tr><td><b>givenName</b></td><td>givenName</td><td>The attribute that defines the given name.</td></tr>
<tr><td><b>displayName</b></td><td>displayName</td><td>The attribute that defines the display name.</td></tr>
<tr><td><b>middleName</b></td><td>middleName</td><td>The attribute that defines the middle name.</td></tr>
<tr><td><b>mail</b></td><td>email</td><td>The attribute that defines the communication profile handle.</td></tr>
<tr><td><b>postalCode</b></td><td>postalCode</td><td>The attribute that defines the postal code of the user. The system creates the address of the user, Registered_User_Address.</td></tr>
<tr><td><b>streetAddress</b></td><td>streetAddress</td><td>The attribute that defines the postal code of the user. The system creates the address for the user with a name.</td></tr>
<tr><td><b>preferredLanguage</b></td><td>preferredLanguage</td><td>The preferred language of the user. The application supports only G13 languages.
Mapping of the LDAP attribute to preferredLanguage must be in the LanguageCode_CountryCode format.
The following list gives the format for the G13 languages that the preferredLanguage attribute supports:
<table>
<tr><th>Language</th><th>Supported format</th></tr>
<tr><td>English (United States)</td><td>en_US</td></tr>
<tr><td>Chinese (Simplified)</td><td>zh_CN</td></tr>
<tr><td>Japanese (Japan)</td><td>ja_JP</td></tr>
</table>
<i>Table continues…</i></td></tr>
</table>

<table>
<tr><th>LDAP Attribute</th><th>System Manager Attribute</th><th>Description</th></tr>
<tr><td></td><td></td><td><table>
<tr><th>Language</th><th>Supported format</th></tr>
<tr><td>Korean (Korea)</td><td>ko_KR</td></tr>
<tr><td>French (France)</td><td>fr_FR</td></tr>
<tr><td>German (Germany)</td><td>de_DE</td></tr>
<tr><td>Italian (Italy)</td><td>it_IT</td></tr>
<tr><td>Russian (Russia)</td><td>ru_RU</td></tr>
<tr><td>English (United Kingdom)</td><td>en_GB</td></tr>
<tr><td>Spanish (Mexico)</td><td>es_MX</td></tr>
<tr><td>Portugese (Brazil)</td><td>pt_BR</td></tr>
<tr><td>French (Canada)</td><td>fr_CA</td></tr>
<tr><td>English (Canada)</td><td>en_CA</td></tr>
</table></td></tr>
<tr><td><b>mail</b></td><td>otherEmail</td><td>The attribute for the secondary email of the user.</td></tr>
<tr><td><b>roomNumber</b></td><td>room</td><td>The room number of the user. The system creates the address of the user, Registered_User_Address.</td></tr>
<tr><td><b>co</b></td><td>country</td><td>The country of the user. The system creates the address of the user, Registered_User_Address.</td></tr>
<tr><td><b>otherTelephone</b></td><td>otherBusinessPhone</td><td>The secondary business telephone number of the user, Registered_User_Address address.</td></tr>
<tr><td><b>facsimileTelephoneNumber</b></td><td>fax</td><td>The fax number of the user, Registered_User_Address address.</td></tr>
<tr><td><b>homePhone</b></td><td>homePhone</td><td>The residential phone number of the user, Registered_User_Address.</td></tr>
</table>

Table continues…

LDAP Attribute	System Manager Attribute	Description
otherHomePhone	otherHomePhone	The secondary residential phone number of the user, Registered_User_Address.
mobile	mobilePhone	The mobile phone number of the user, Registered_User_Address.
otherMobilePhone	otherMobilePhone	The secondary mobile phone number of the user, Registered_User_Address.
pager	pager	The pager number of the user, Registered_User_Address address.
otherPager	otherPager	The secondary pager number of the user, Registered_User_Address.
givenName	preferredGivenName	The preferred given name of the user.
organization	organization	The organization to which the user belongs.
department	department	The department to which the user belongs.
employeeID	employeeNo	The employee ID of the user.
st	stateOrProvince	The state or the province of the user. The system creates the address of the user, Registered_User_Address.
l	localityName	The locality of the user. The system creates the address for the user, Registered_User_Address.
displayName	localizedName	The localized name of the user in different languages. **Note:** Map the LDAP attribute to localizedName in the format:Locale.Name. For example, if the locale is English and the user name is Alex, the value for **displayName** must be en.Alex.
displayNamePrintable	endpointDisplayName	The full text name of the user represented in ASCII. The attribute supports displays that

Table continues…

LDAP Attribute	System Manager Attribute	Description
		cannot handle localized text, for example, some endpoints.
msExchHouseIdentifier	Microsoft Exchange Handle	The Microsoft Exchange communication address of the user for communication with Microsoft SMTP Server.
o	Microsoft SIP Handle	The Microsoft SIP communication address of the user that supports SIP-based communication.
manager	IBM Sametime Handle	The IBM Sametime communication address of the user that supports IBM Sametime. The format must be of type DN=IBMHandle.
l	User Provisioning Rule ✱ **Note:** If you map the telephone number (Avaya E164 handle) and UPR in datasource and the LDAP attribute values change in LDAP, during next synchronization, the system updates only the Avaya E164 handle. The system does not update the Communication Manager extension or SIP handle that is configured in UPR.	The user provisioning rule. You can map the user provisioning rule to more than one LDAP attribute. The system joins the value of multiple LDAP attributes by an underscore (_) to map the value in System Manager. You cannot map the same LDAP attribute more than once. The user provisioning rule data synchronizes from the LDAP directory server to System Manager only.
telephoneNumber	Phone Number	The attribute that the system maps to the Avaya E164 handle. The value for the extension is the last N digit value that is set in the **Use Phone Number last ..... digits for Extension** field on the User Provisioning Rule page. The synchronization is bidirectional.
extensionName	Mailbox Number	The Messaging mailbox number. The synchronization is bidirectional.
telexNumber	CS 1000 Extension	The extension on CS 1000.

Table continues…

LDAP Attribute	System Manager Attribute	Description
		The data synchronizes from System Manager to the LDAP directory server.
primaryTelexNumber	Communication Manager Extension	The extension on Communication Manager. The data synchronizes from System Manager to the LDAP directory server.
msDS-PhoneticLastName	surnameascii	The last name of the user in ASCII.
msDS-PhoneticFirstName	givennameascii	The first name of the user in ASCII.
msDS-PhoneticDisplayName	endPointDisplayName	The display name of the user in ASCII as displayed on the endpoint.

Button	Description
Save	Adds a new datasource or saves the changes that you made on the page.
Cancel	Cancels your action and displays the previous page.

Related links

Editing the synchronization datasource on page 53

Creating the user synchronization job

Procedure

1. On the System Manager web console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Active Synchronization Jobs** tab.
4. Click **Create New Job**.
5. On the New User Synchronization Job page, select the datasource from which you want to synchronize.
6. Perform one of the following:
    a. Click **Run Job** to run the job immediately.
    b. Select the **Schedule job for future execution** check box to schedule the job at a later time.

    You can delete a job that is scheduled to run in the future.

Note:

Every 7 seconds, the system fetches the job status and the number of users synchronized on the **Active Synchronization Job** tab. Therefore, you might not immediately see the status of the active synchronization job that is running.

Related links

User active synchronization job field descriptions on page 62

Scheduling a user synchronization job

Procedure

1. On the System Manager web console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Active Synchronization Jobs** tab.
4. Click **Create New Job**.
5. Perform the following:
    a. On the New User Synchronization Job page, in the **Datasource Name** field, enter a datasource for which you want to schedule a job.
    b. Select the **Schedule job for future execution** check box.
    c. In the **Date** field, enter the date when you want to run the job.
    d. In the **Time** field, enter the time when you want to run the job.
    e. In the **Time Zone**, enter the time zone.
    f. Select the **Repeat Job Execution** check box to repeat the job
    g. Select the recurring interval in minutes, hours, days, weeks, or months.
6. Click **Schedule job for future execution**.

Deleting a user synchronization job

Procedure

1. On the System Manager web console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Synchronization Job History** tab and select the job that you want to delete.
4. Click **Delete Job**.

    Without any confirmation, the system deletes the job.

Note:

You can delete a job that is scheduled to run in the future.

User active synchronization job field descriptions

Field	Description
Datasource Name	The name of the datasource
Schedule job for future execution	The option to schedule a user synchronization job
Date	The date on which you want to schedule the job
Time	The time when you want to schedule the job
Time Zone	The time zone closest to your location

Button	Description
Run Job	Runs the user synchronization job that you specified.
Schedule job for future execution	Schedules a user synchronization job. The system displays the button only when you select the **Schedule job for future execution** check box.
Cancel	Cancels the synchronization and displays the previous page.

Synchronization job history

The **Synchronization Job History** tab displays the history of jobs created for user synchronization and the result of each job execution. You can delete any entry from the list of user synchronization job by using the **Delete Job** link.

Related links

Synchronization job history field descriptions on page 62

Synchronization job history field descriptions

Field	Description
Name	The datasource name for which the user synchronization job was executed.

Table continues…

Field	Description
Start Time	The start time of a user synchronization job.
End Time	The time when a user synchronization job was completed.
Status	The status of the user synchronization job.
Job Result	The result of running a job. To view the results of the user synchronization, click the **View Job Summary** link. The system displays the results on the Synchronization Job Summary page.
Action	The **Delete Job** link that you use to delete the results of the user synchronization job.

Icon	Description
🔄	Refreshes the information on the **Synchronization Job History** tab.

Viewing Job Summary

Procedure

1. On the System Manager web console, click **Users** > **Directory Synchronization**.
2. In the left navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Synchronization Job History** tab.
4. In the **Job Result** column, click the **View Job Summary** link.

Related links

Viewing Job Summary field descriptions on page 63

Viewing Job Summary field descriptions

Field	Description
Datasource Name	The datasource name for which the user synchronization job was run.
End Time	The time when the user synchronization job was completed.
Job Results	The results of running the user synchronization job.

Table continues…

Field	Description
Added	The number of users added to the system as a result of running the job. For a nonzero count, the system displays an expand sign (+) or collapse sign (-). You can click the sign to show or hide the details of user entries.
Modified	The number of users modified as a result of running the job. For a nonzero count, the system displays an expand or collapse sign. You can click the sign to show or hide the details of modified user entries.
Deleted	The number of users deleted as a result of running the job. For a nonzero count, the system displays an expand or collapse sign. You can click the sign to show or hide the details of deleted user entries.
Unchanged	The number of users that remained unchanged after running the job.
Failed	The number of user records that the system failed to synchronize because of errors. For a nonzero count, the system displays an expand or collapse sign. You can click the sign to show or hide the details of user entries for which the synchronization failed.
Total records processed	The total number of user records that the system processed while the job is in progress.

Button	Description
Back	Displays the previous page.

Chapter 4: Geographic Redundancy

Geographic Redundancy overview

Avaya Aura® provides System Manager Geographic Redundancy, a resiliency feature that handles scenarios where the primary System Manager server fails or the data network partially loses connectivity. In such scenarios, the system manages and administers products such as Avaya Aura® Session Manager and Avaya Aura® Communication Manager across the customer enterprise using the secondary System Manager server.

For customers who need highly fault-tolerant deployments, System Manager supports System Manager Geographic Redundancy deployments that can provide the Active-Standby mode of resiliency.

The following table lists some of the key differences between Geographic Redundancy and High Availability (HA) solutions:

Geographic Redundancy	HA
Addresses sudden, site-wide disasters	Addresses server outages due to network card, hard disk, electrical, or application failure
Distributed across WAN	Deployed within a LAN
Manual	Automated

You must install System Manager on both the standalone servers with separate IP addresses and configure Geographic Redundancy. If a managed product that supports the Geographic Redundancy feature loses connectivity to the primary System Manager server, the secondary System Manager server provides the complete System Manager functionality. However, you must manually activate the secondary System Manager server.

Note:

Only the system administrator can perform Geographic Redundancy-related operations.

You must reconfigure the elements that do not support Geographic Redundancy so that the elements can communicate with the secondary System Manager server to receive configuration information. For more information about configuring elements that do not support Geographic Redundancy, see *Geographic Redundancy-unaware elements overview*.

During the installation of GR-unaware elements such as Presence Server, you must specify if you want to enable the Geographic Redundancy feature on the element.

Out of Band Management in a Geographic Redundancy setup

When you configure Geographic Redundancy, provide Management network details only. Validation fails if you configure Geographic Redundancy with Public network details. In Geographic Redundancy setup, you do not disable or enable Out of Band Management on both primary and secondary System Manager virtual machine. You can enable Out of Band Management on the primary System Manager virtual machine and disable Out of Band Management on the secondary System Manager virtual machine, and vice versa.

Related links

Geographic Redundancy-unaware elements overview on page 88

Geographic Redundancy-unaware elements overview on page 88

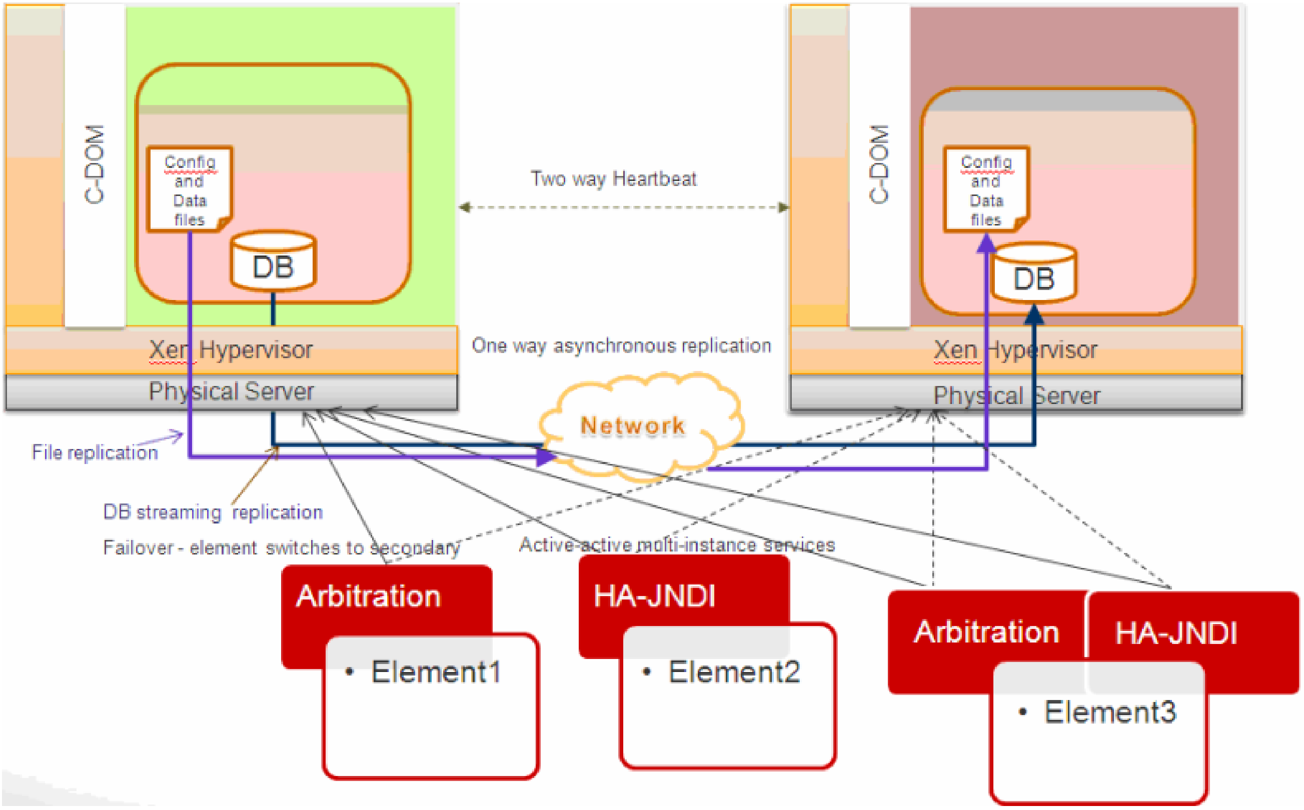
Licensing in Geographic Redundancy

In Geographic Redundancy, the system replicates the license file on the secondary System Manager server that you installed on the primary System Manager server. When you activate the secondary System Manager server, the same license file works on the secondary System Manager server.

In Geographic Redundancy, you must generate the license file by using the host ID of primary System Manager.

Architecture and deployment diagrams for Geographic Redundancy

The following diagram illustrates the interaction between System Manager Geographic Redundancy and the elements that System Manager manages, such as Avaya Aura® Session Manager and Communication Manager.



Geographic Redundancy terminology

Primary System Manager server

The first or the master System Manager server in a Geographic Redundancy setup that serves all system management requests.

Secondary System Manager server

The System Manager server that functions as a backup to the primary System Manager server in a Geographic Redundancy setup. The secondary System Manager server provides the full System Manager functionality when the system fails to connect to the primary System Manager server.

Active System Manager server

The mode of operation of the System Manager server where the server provides the full System Manager functionality.

Standby System Manager server

The mode of operation of the System Manager server where the server serves only authentication and authorization requests. In the standby mode of operation, the system supports limited Geographic Redundancy configuration, the inventory service.

Standalone System Manager server

The single System Manager server deployed in an enterprise that provides full System Manager functionality. The standalone server operates independently and does not contain a backup server.

Element

An element is an instance of an Avaya Aura® network entity that System Manager manages. For example, a Session Manager server or a Communication Manager server.

The elements can be of the following types:

- Active-Active: The elements leverage the services of the primary and the secondary System Manager servers. The system functions in this mode when the enterprise network splits.
- Active-Standby: The elements communicate with the active System Manager server. The mode is also called Active-Standby Auto. In the normal operation scenario, the primary System Manager server is active and the secondary System Manager server is in the standby mode. The primary System Manager server continues to manage elements until the primary System Manager server becomes unavailable. If the primary System Manager server fails and the administrator activates the secondary System Manager server, the elements automatically switch to the secondary System Manager server.
- Active-Standby: The elements function similar to the Active-Standby mode, except that you must manually select the elements from System Manager web console by using **More Options** > **Manage** or **More Options** > **UnManage** provided on the **Services** > **Inventory** > **Manage Elements** page. The mode is also called Active-Standby Manual.

Geographic Redundancy-aware element

An element that supports Geographic Redundancy, such as Avaya Aura® Session Manager Release 6.3.

Geographic Redundancy-unaware element

An element that does not support Geographic Redundancy, such as Avaya Aura® Session Manager release earlier than 6.3.

Geographic Redundancy operational modes

- The normal operation mode. Also called the Sunny Day scenario. A System Manager Geographic Redundancy scenario where the primary System Manager server runs in the active mode while the secondary System Manager server runs in the standby mode providing limited set of services. In the normal operation mode, the primary System Manager server manages all elements and provides the complete System Manager functionality.
- Primary nonoperational mode. Also called the Rainy Day scenario. The primary System Manager server fails or loses connectivity to all elements that the system manages. The administrator activates the secondary System Manager server to make the secondary System Manager server manage all elements in the system.
- Split network. A System Manager Geographic Redundancy scenario when the primary and secondary System Manager servers run in the active mode but cannot communicate with each other due to a network connectivity outage or when some elements cannot communicate with one System Manager and both primary and secondary System Manager servers can communicate with each other.

Failover

Failover is the process of activating the secondary System Manager server when the primary System Manager server becomes nonoperational due to server outage or loses connectivity to the elements that the server manages.

Failback

Failback is the process of making the primary System Manager server operational by restoring the primary System Manager server by using the primary or secondary System Manager data.

Geographic Redundancy replication

The Geographic Redundancy feature provides the following replication mechanisms to ensure consistency of data between the primary and the secondary System Manager servers:

- Database replication
- File replication
- LDAP (Directory) replication

The primary System Manager server continuously replicates the data with the secondary System Manager server. If the system does not replicate the data for a specific period of time that is configured in **Services** > **Configurations** > **Settings** > **SMGR** > **HealthMonitor**, the primary and the secondary System Manager servers raise alarms.

Prerequisites for servers on Appliance Virtualization Platform in the Geographic Redundancy setup

In a Geographic Redundancy setup, ensure that the two standalone running on Appliance Virtualization Platform that you designate as primary and secondary servers meet the following requirements:

- Must contain the same hardware such as Dell™ PowerEdge™ R620 server.
- Must have the same hardware configuration, for example, the same processor.
- Must contain the same version of the Avaya Virtualization Platform software that includes software packs.

  Note:

  System Manager does not support the mixed Virtualized Environment and Appliance Virtualization Platform environment. For example, the primary System Manager on Appliance Virtualization Platform and the secondary System Manager on VMware ESXi.

- Must contain the same profile for primary and secondary System Manager Geographic Redundancy virtual machines. For example, if the primary System Manager contains Profile 1, the secondary System Manager must also contain Profile 1.
- Must contain the same version of the System Manager software that includes service pack and software patches.
- Must contain the same parent domain names for two System Manager systems. For example, smgr.abc.com and smgr.xyz.com are invalid domain names because the parent domain names abc and xyz are different.
- Must be able to communicate with each other over the network using the IP address and FQDN.
- Must have synchronized network time.
- Must use DNS to ensure that the name resolution is automatic. Otherwise, you must resolve the IP address and the host name in the `/etc/hosts` file on the primary and secondary System Manager servers.
- Must ensure that the required ports are open to support the Geographic Redundancy feature. For port usage information, see *Avaya Port Matrix: Avaya Aura® System Manager* on the Avaya Support website at http://support.avaya.com/.
- Must ensure that the minimum data pipe between the primary and the secondary System Manager server is T1. T1 provides 1.544 Mbps.
- Must ensure that the network latency is less than 500 ms.

Prerequisites for System Manager on VMware in the Geographic Redundancy setup

In a Geographic Redundancy-enabled system running on VMware, ensure that System Manager that you designate as primary and secondary systems meet the following requirements:

- Must be on VMware environment.

  Note:

  System Manager does not support the mixed VMware and Appliance Virtualization Platform environment. For example, the primary System Manager on Appliance Virtualization Platform and the secondary System Manager on VMware ESXi.
- Must contain the same profile for primary and secondary System Manager Geographic Redundancy virtual machines. For example, if the primary System Manager contains Profile 1, the secondary System Manager must also contain Profile 1.
- Must contain the same version of the System Manager software that includes service pack and software patches.

- Must contain the same parent domain names for two System Manager systems. For example, smgr.abc.com and smgr.xyz.com are invalid domain names because the parent domain names abc and xyz are different.
- Must be able to communicate with each other over the network using the IP address and FQDN.
- Must have synchronized network time.
- Must use DNS to ensure that the name resolution is automatic. Otherwise, you must resolve the IP address and the host name in the `/etc/hosts` file on the primary and secondary System Manager servers.
- Must ensure that the required ports are open to support the Geographic Redundancy feature. For port usage information, see *Avaya Port Matrix: Avaya Aura® System Manager* on the Avaya Support website at http://support.avaya.com/.
- Must ensure that the network latency is less than 500 ms.
- Must ensure that the minimum data pipe between the primary and the secondary System Manager server is T1. T1 provides 1.544 Mbps.

Key tasks for Geographic Redundancy

Prerequisites

Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.

Key tasks

Only the system administrator can perform Geographic Redundancy-related operations.

- Configure Geographic Redundancy.

  Configure Geographic Redundancy to handle the situation when the primary System Manager server fails or when the managed element loses connectivity to the primary System Manager server.

  Important:

  During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

- Enable the Geographic Redundancy replication between the two servers.

  Enable the Geographic Redundancy replication in the following scenarios:

  - After you configure the two standalone System Manager servers for Geographic Redundancy, you must enable the Geographic Redundancy replication between the two servers to ensure that the secondary System Manager server contains the latest copy of the data that is available on the primary System Manager server.

  - During the system maintenance or during the upgrades, Geographic Redundancy replication is disabled. You must enable the replication after the maintenance activity is complete and you configure Geographic Redundancy on the system.

    Note:

    If the heartbeat between the two System Manager servers, in which the Geographic Redundancy replication is enabled, stops because of network connectivity failure or because of the failure of one of the server, the system automatically disables the Geographic Redundancy replication within a preconfigured time. The default is 5 minutes. If the primary and secondary System Manager servers are running and if the network connectivity between the two servers fails, the system triggers auto-disable on both servers. If one of the two servers becomes nonoperational, the system triggers auto-disable on the server that is operational.

  - After the primary System Manager server recovers from failure.

  Important:

  During the bulk activities such as import, export, and full synchronization of Communication Manager, the system might disable the Geographic Redundancy replication for reasons, such as the size of the data involved in the bulk activity and the bandwidth between the primary and the secondary System Manager server. After you complete the bulk activity, enable the Geographic Redundancy replication if the replication is disabled.

- Disable the Geographic Redundancy replication between the two servers.

  Disable the Geographic Redundancy replication before you start the maintenance activities such as upgrades, installation of software patches or hot fixes. If the primary and the secondary System Manager servers disconnect from each other for more than the threshold period, the system automatically disables the Geographic Redundancy replication. The default threshold period is 5 minutes.

- Activate the secondary System Manager server.

  Activate the secondary System Manager server in the following scenarios:

  - The primary System Manager becomes nonoperational.
  - The enterprise network splits.

- Deactivate the secondary System Manager server.

  Deactivate the secondary System Manager server in the following situations:

  - The primary System Manager server becomes available.
  - The element network restores from the split.

- Restore the primary System Manager server.

  After you activate the secondary System Manager server, to return to the active-standby mode, you must restore the primary System Manager server. You can choose to restore from the primary System Manager or the secondary System Manager server.

  Note:

  The system does not merge the data from the primary and secondary server.

- Reconfigure Geographic Redundancy.

You can reconfigure Geographic Redundancy when the secondary System Manager is in the standby mode or active mode. The reconfiguration process copies the data from the primary System Manager server to the secondary System Manager server.

- Convert the primary System Manager server to the standalone server.

  Perform this procedure to convert the primary System Manager server in the Geographic Redundancy-enabled system to a standalone server or if you have to configure a new secondary server.

For detailed instructions to complete each task, see the relevant section in this document.

Configuring Geographical Redundancy

Before you begin

- For the new installation of System Manager, ensure that you change the default password for the system administrator user.
- Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.

About this task

For resiliency, from the pair of standalone System Manager servers, you can configure Geographic Redundancy.

Important:

- During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.
- After the Geographic Redundancy configuration is complete, the credentials used for logging in to the secondary System Manager becomes identical to the login credentials of the primary System Manager.

Procedure

1. Log on to the System Manager web console of the standalone server that you require to designate as the secondary server and perform the following:
   a. On the System Manager web console, click **Services** > **Geographic Redundancy**.
   b. Click **Configure**.
   c. In the dialog box, provide the details of the primary System Manager server in the following fields:
      - **Primary Server Username**

        Enter the system administrator user name that you use to log on to the primary System Manager server.

- **Primary Server Password**

  Enter the system administrator password that you use to log on to the primary System Manager server.

- **Primary Server IP**
- **Primary Server FQDN**

d. Click **OK**.

The configuration process takes about 30 minutes. However, the duration might vary depending on the size of the data on the primary System Manager server,

✱ **Note:**

As the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

The server that you configured becomes the secondary server and the other standalone server becomes the primary System Manager server.

2. To view the status of the Geographic Redundancy configuration during the restart of the two application servers, perform one of the following:

- Log on to the web console of the primary System Manager server and perform the following steps:

  a. On the System Manager web console, click **Services** > **Geographic Redundancy**.

  b. Refresh the GR Health page.

  If **Enable** is available, the configuration is complete.

  ✱ **Note:**

  Log off and log on to the primary System Manager server to view the updated status of GR Health.

- Log in to the secondary System Manager server as system administrator by using the command line interface and perform the following steps:

  a. Type `tail -f /home/ucmdeploy/quantum/autoReconfig.log`.

  The system displays the progress during the restart of the two application servers. When the second application server restart completes, the system displays the following messages:

```
          SMGR  ::  operationStatus=success

          SMGR  ::  Quantum has been successfully configured
as a secondary.
```

Next steps

On the web console of the primary System Manager server, enable the Geographic Redundancy replication.

Related links

Enabling the Geographic Redundancy replication on page 75
Geographic Redundancy field descriptions on page 85
Prerequisites for servers on Appliance Virtualization Platform in the Geographic Redundancy setup on page 69
Prerequisites for System Manager on VMware in the Geographic Redundancy setup on page 70
Enabling the Geographic Redundancy replication on page 75
Geographic Redundancy field descriptions on page 85
Prerequisites for servers on Appliance Virtualization Platform in the Geographic Redundancy setup on page 69
Prerequisites for System Manager on VMware in the Geographic Redundancy setup on page 70

Enabling the Geographic Redundancy replication

Enable the Geographic Redundancy replication between the two servers to ensure that the data gets continuously replicated between the primary and secondary System Manager servers.

Before you begin

Log on to the System Manager web console of the primary server.

About this task

Important:

During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Enable Replication**.

   The system displays the progress information in the **Enable GR Status** section.

   Note:

   As the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

   If the enabling process is successful, the system displays the Geographic Redundancy replication status as `Enabled`. If the process fails, the system displays an error message with the replication status as `Failed` on the primary the System Manager web console. The primary server remains in the failed state while the secondary server rolls back to the previous state. Verify if the system has raised an alarm for a temporary network connectivity failure. Retry when the network connectivity is restored. If the problem persists, contact Avaya service personnel.

Related links

Disabling the Geographic Redundancy replication on page 76
Geographic Redundancy field descriptions on page 85
Disabling the Geographic Redundancy replication on page 76
Geographic Redundancy field descriptions on page 85

Disabling the Geographic Redundancy replication

Before you begin

Log on to the System Manager web console of the primary server.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Disable Replication**.
3. In the dialog box, click **Yes**.

   The system displays the progress information in the **Disable GR Status** section.

   If the disabling process is successful, the system displays the Geographic Redundancy replication status as `Disabled`. The system stops replicating the data from the primary and secondary System Manager server. If the disabling process fails, the system displays an error message on the web console of the primary System Manager.

Related links

Enabling the Geographic Redundancy replication on page 75
Geographic Redundancy field descriptions on page 85
Enabling the Geographic Redundancy replication on page 75
Geographic Redundancy field descriptions on page 85

Activating the secondary System Manager server

Before you begin

Log on to the System Manager web console of the secondary server.

About this task

Note:

- When you activate the secondary System Manager server, the system stops replicating the data from the primary System Manager server to the secondary System Manager server. During activation, you cannot gain access to the web console of the secondary System Manager server for some time.
- In the same browser instance, do not open the primary and secondary System Manager server in different tabs. The system might display an unknown error after the activation, deactivation, or recovery is complete. You can ignore this error message.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Activate Secondary Server**.

   The system displays the Geographic Redundancy (GR) Health Current status dialog box.
3. In the Select the reason for activation, choose one of the following options:
   - **Primary Down**: When the primary System Manager server becomes nonoperational, the server hardware is faulty and unusable or the application server fails to recover.
   - **Network Split**: When the enterprise network splits and servers fail to communicate with each other.
   - **Maintenance**: When the maintenance activities such as backup, restore, upgrade, and shutdown are in progress.
   - **Other**: Any other reason where the primary System Manager server becomes unusable and needs the secondary System Manager server to become operational.
4. Click **Yes**.

   The system displays the initialization of the activation process.
5. Click **Yes**.

   The activation process takes about 15–20 minutes to complete.

   If the activation process fails, the system displays an error message on secondary the System Manager web console and rolls back to the previous state. If the activation process is successful, the secondary System Manager server changes to the active mode and provides complete System Manager functionality.

   Note:

   As the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

Related links

Deactivating the secondary System Manager server on page 78

Geographic Redundancy field descriptions on page 85

Deactivating the secondary System Manager server on page 78

Geographic Redundancy field descriptions on page 85

Deactivating the secondary System Manager server

Before you begin

Log on to the System Manager web console of the secondary server.

About this task

✱ **Note:**

In the same browser instance, do not open the primary and secondary System Manager server in different tabs. The system might display an unknown error after the activation, deactivation, or recovery is complete. You can ignore this error message.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Deactivate Secondary Server**.

   The system displays the Deactivate Secondary Server dialog box and the progress while performing the deactivation process.
3. Click **OK**.

   If the deactivation process is complete, the secondary System Manager server goes to the standby mode. If the deactivation process fails, the system displays an error message on the secondary System Manager web console and the server remains in the active mode.

Next steps

Restore primary System Manager. For instructions, see Restoring the primary System Manager server.

Related links

Activating the secondary System Manager server on page 76
Geographic Redundancy field descriptions on page 85
Activating the secondary System Manager server on page 76
Geographic Redundancy field descriptions on page 85

Restoring the primary System Manager server

Before you begin

Log on to the System Manager web console of the primary server.

About this task

You can restore the data when the secondary System Manager server is active or in the standby mode. However, for minimum system nonfunctional time during data restoration or an emergency or both, you can restore the data when the secondary System Manager server is active.

Important:

After you restore the system with the secondary System Manager data, if you want to revert to the primary System Manager data, you can restore to the primary System Manager data using the procedure in Step 4. However, you must restore to the primary System Manager data, before you enable the Geographic Redundancy replication. After you enable the Geographic Redundancy replication, you cannot restore to the primary System Manager server data.

In the same browser instance, do not open the primary and secondary System Manager server in different tabs. The system might display an unknown error after the activation, deactivation, or recovery operation is complete. You can ignore this error message.

Procedure

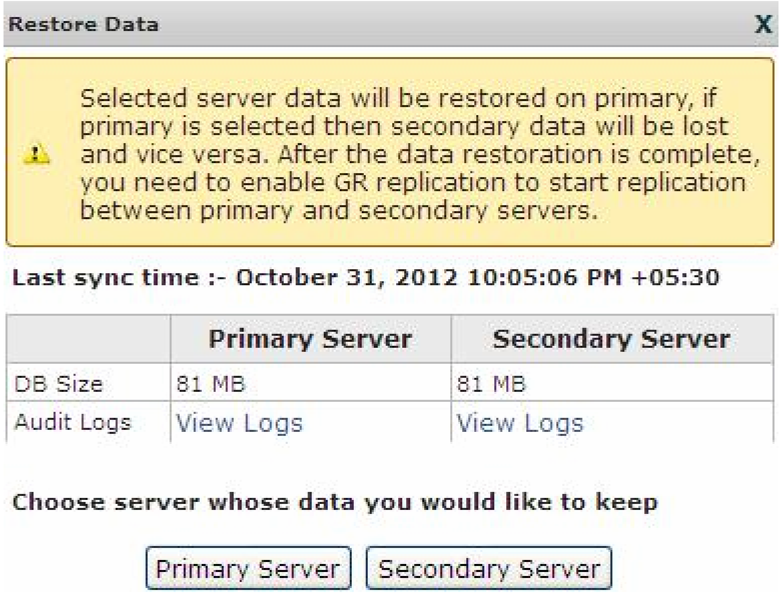
1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Restore Data**.
3. On the Restore GR dialog box, select a server whose data you want to retain:
   - **Primary Server**

     The system keeps the primary System Manager server data. The data on the secondary System Manager server is lost.

     Select the secondary System Manager server if the secondary System Manager server data changes significantly during the interval between activation and deactivation and the administrator wants to retain those changes even after restoring the data using **Restore Data**.
   - **Secondary Server**

     The system restores the data from the secondary server on the primary System Manager server. the System Manager web console is unavailable for some time. The time that the system takes to restore depends on the network speed and the size of the data that the system must restore.

     After the system recovery, select the secondary System Manager server if the secondary System Manager server data changes significantly during the interval between the system recovery and the deactivation and if you want to retain the changes from the secondary System Manager server after restoring the data by using **Restore Data**.



Restore Data

Selected server data will be restored on primary, if primary is selected then secondary data will be lost and vice versa. After the data restoration is complete, you need to enable GR replication to start replication between primary and secondary servers.

Last sync time :- October 31, 2012 10:05:06 PM +05:30

	Primary Server	Secondary Server
DB Size	81 MB	81 MB
Audit Logs	View Logs	View Logs

Choose server whose data you would like to keep

The system displays the Restore Status dialog box.

The system displays the restore operation status and the status of the primary and the secondary System Manager server.

Important:

After you restore the data, all changes that you make on the secondary System Manager server that is active will not be available on the primary System Manager server.

4. If you later decide to revert to the database of the primary System Manager server, perform the following steps after the restore is complete:

   a. Using the command line interface, log in to System Manager of the primary server as root.

   b. Change to the `$MGMT_HOME/geo/bin` directory.

   c. Type `sh backupandrestore.sh recovery secondaryIP secondaryFQDN`.

      When the script completes, System Manager restarts and contains the data from the primary System Manager server that was available before you restored with the secondary System Manager data.

      Note:

      - To restore with the secondary System Manager server data again, activate and deactivate the secondary System Manager server.
      - As the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

Next steps

After the data restoration is complete, verify the data and deactivate the secondary System Manager server if the server is active during the restoration process.

Enable the Geographic Redundancy replication to synchronize the primary and secondary System Manager servers.

Related links

Enabling the Geographic Redundancy replication on page 75
Deactivating the secondary System Manager server on page 78
Geographic Redundancy field descriptions on page 85
Enabling the Geographic Redundancy replication on page 75
Deactivating the secondary System Manager server on page 78
Geographic Redundancy field descriptions on page 85

Reconfiguring Geographic Redundancy

Before you begin

- Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.
- Log on to System Manager web console of the secondary server.

About this task

For resiliency, from the pair of standalone System Manager servers, you can configure Geographic Redundancy.

Important:

During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Click **Reconfigure**.
3. In the dialog box, provide the details of the primary System Manager server in the following fields:
    - **Primary Server Username**

      Enter the admin user name that you use to log on to the primary System Manager server.
    - **Primary Server Password**

      Enter the admin password that you use to log on to the primary System Manager server.
    - **Primary Server IP**
    - **Primary Server FQDN**

4. Click **OK**.

   Note:

   As the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

   The server that you configured becomes the secondary server and the other standalone server becomes the primary System Manager server.

5. To view the status of the Geographic Redundancy configuration during the restart of the two application servers, perform one of the following:

   - Log on to the web console of the primary System Manager server and perform the following steps:

     a. On the System Manager web console, click **Services** > **Geographic Redundancy**.

     b. Refresh the GR Health page.

        If **Enable** is available, the configuration is complete.

        Note:

        Log off and log on to the primary System Manager server to view the updated status of GR Health.

   - Log in to the secondary System Manager server as system administrator by using the command line interface and perform the following steps:

     a. Type `tail -f /home/ucmdeploy/quantum/autoReconfig.log`.

        The system displays the progress during the restart of the two application servers. When the second application server restart completes, the system displays the following messages:

```
           SMGR  ::  operationStatus=success

           SMGR  ::  Quantum has been successfully configured
as a secondary.
```

Next steps

On the primary the System Manager web console, enable the Geographic Redundancy replication.

Related links

Prerequisites for servers on Appliance Virtualization Platform in the Geographic Redundancy setup on page 69
Prerequisites for System Manager on VMware in the Geographic Redundancy setup on page 70
Prerequisites for servers on Appliance Virtualization Platform in the Geographic Redundancy setup on page 69
Prerequisites for System Manager on VMware in the Geographic Redundancy setup on page 70

Converting the primary System Manager server to the standalone server

Before you begin

- Log on to the System Manager web console of the primary server.
- Disable the Geographic Redundancy replication if you have not already disabled.

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy**.
2. Select the primary System Manager server, and click **Convert To Standalone**.

   The system displays a dialog box.
3. Click **OK**.

   If the conversion is successful, the system displays `Converted to Standalone successfully` and converts the primary System Manager server to a standalone server.

   The system displays the status of the server as `Unconfigured` on the Manage Elements page. The administrator can configure the server when required.

Related links

Enabling the Geographic Redundancy replication on page 75
Geographic Redundancy field descriptions on page 85
Enabling the Geographic Redundancy replication on page 75
Geographic Redundancy field descriptions on page 85

About the Health Monitoring service

Using the Health Monitoring service, you can monitor the status of the following:

- Database replication
- File replication
- LDAP replication
- System health check
- Application server

The system checks the condition of services on both the primary and secondary System Manager servers.

You can configure the following parameters from **Services** > **Configurations** > **Settings** > **SMGR** > **HealthMonitor** of the System Manager web console:

- Health monitoring interval

- The number of days the health monitoring data must be retained
- The number of successive retries before an alarm is raised

You can configure the timeout interval for health monitoring in the `MonitorConfig.properties` file from System Manager CLI. The properties file is available in the `$MGMT_HOME/SystemMonitor/res/` location. The default timeout interval is 15 seconds.

The health monitoring includes the overall status of the replication, and the detailed health metric such as the time and size of the data that the secondary System Manager server lags in replication behind the primary System Manager server.

You can view the heartbeat status and the health monitoring details in the graphical format for different services from **View Heartbeat Status** from **Services** > **Geographic Redundancy** > **GR Health** on System Manager web console.

Related links

Configuring the timeout interval for health monitoring on page 84
View Profile:HealthMonitor field descriptions on page 815
Edit Profile:HealthMonitor field descriptions on page 816
GR Health field descriptions on page 86

Configuring the timeout interval for health monitoring on page 84
View Profile:HealthMonitor field descriptions on page 815
Edit Profile:HealthMonitor field descriptions on page 816
GR Health field descriptions on page 86

Configuring the timeout interval for health monitoring

Procedure

1. Log in to System Manager CLI.
2. From the `$MGMT_HOME/SystemMonitor/res` location, open the `MonitorConfig.properties` file.
3. In the properties file, change the value for the ServiceTimeOutInterval property.

   The default is 15 seconds.
4. Type `service systemMonitor restart` to restart the service.

   The changes takes effect.

Geographic Redundancy field descriptions

The Geographic Redundancy and the GR Health pages remain blank on a standalone server or until you configure a secondary System Manager.

Primary Server Details

The system displays the IP address and the FQDN of the primary System Manager server.

Name	Description
Convert to Standalone	Converts to a standalone server. The system displays the **Convert to Standalone** button only when the replication is disabled.
Configure	Configures Geographic Redundancy. The system displays the **Configure** button only on the standalone System Manager server.
Reconfigure	Configures Geographic Redundancy. The system displays the **Reconfigure** button only on the secondary System Manager server.

Secondary Server Configured

You can use the **Enable Replication**, **Disable Replication**, and **Restore Data** buttons only from the primary System Manager server.

Button	Description
Enable Replication	Continuously replicates the data between the primary and the secondary System Manager server. The system displays the **Enable Replication** button after the following events: • State of Geographic Redundancy is Disable. • Geographic Redundancy configuration. • Restoration of the primary Geographic Redundancy server is complete.
Disable Replication	Stops replicating the data between the primary and the secondary System Manager server. The system displays the **Disable Replication** button when the state of Geographic Redundancy is Enable.
Restore Data	Recovers the server after the failback. The system displays the **Restore Data** button when the secondary System Manager server is deactivated.

Field name	Description
IP	Displays the IP address of the secondary System Manager server.
FQDN	Displays FQDN of the secondary System Manager server.
Replication Status	Displays the status of replication. The values are Disabled and Enabled.
Last Action	Displays the last action that you performed on the secondary System Manager server.
Last Action Status	Displays the status of the last action that you performed on the secondary System Manager server.

GR Health field descriptions

The information available on the GR Health page is read-only.

The Geographic Redundancy and the GR Health pages remain blank on a standalone server or until you configure a secondary System Manager.

GR Health

Name	Description
GR Health Status	Displays the health status of the monitored services. The page displays: • 🟥, if the monitored service stops. • ✓, if the monitored service is running. • ✗, if the monitored service fails to run.
Activate Secondary Server	Click to make the secondary server provide full System Manager functionality when the primary System Manager server fails or the data network splits. **Note:** • The system displays **Activate Secondary Server** only on the secondary System Manager server. • The system displays the **Activate Secondary Server** or the **Deactivate Secondary Server** button on the page.

Table continues…

Name	Description
Deactivate Secondary Server	Click to make the primary System Manager resume operation. You use this option when the primary System Manager server restores operation or recovers from a network failure. ✱ **Note:** The system displays **Deactivate Secondary Server** only on the secondary System Manager server.
Service Name	Displays the name of the service for which the system provides the status of the health.
View Detail	Click **View Graph**. • For database and directory replication, the system displays the graph for default interval. If no graph is present for the default interval, using the calendar, you can set the period for which you require to check the health status, and click **Generate** to view health details in a graph. For database replication, the system displays graphs for time lag and the size lag. For directory replication, the system displays graph for time lag only. • For file replication, the system displays the last replication time and the size of the lag.

HeartBeat status

Click **View Heartbeat Status** to view the details. The system displays the GR Heartbeat page.

Name	Description
Service Name	The name of the monitored service. The services are: • **System Health**: The heartbeat status indicates if the primary or the secondary System Manager server can communicate with the peer System Manager server over the network. • **Database Replication**: The heartbeat status indicates if the data stored in the System Manager database is getting replicated between the primary and the secondary System Manager server. • **Application System Health**: The heartbeat status indicates if the application server of primary or secondary System Manager can query the application server of the peer System Manager.

Table continues…

Name	Description
	• **File Replication**: The heartbeat status indicates if the configuration files are getting replicated between the primary and the secondary System Manager server. • **Directory Replication**: The heartbeat status indicates if the data stored in the internal LDAP server is getting replicated in the respective System Manager server.
Last Successful Heartbeat Time	The last time the heartbeat was successful for the monitored service.
Last Missed Heartbeat Time	The last time when the monitored service missed the heartbeat.
View Details	The **View Graph** link to view the health status of the monitored service over a period of time. To configure the time period, click **Edit Dates**. The graph displays the status in 0 and 1. • 0 indicates that the monitored service is either stopped or failed at that point of time • 1 indicates that the monitored service is running at that point of time.

Configuring the GR-unaware elements to work with System Manager

Geographic Redundancy-unaware elements overview

Geographic Redundancy-unaware (GR-unaware) elements are elements that cannot support the System Manager Geographic Redundancy feature. GR-unaware elements might be legacy elements, that is, prior to Release 6.3, which are already present in the field or elements that have not yet leveraged the Geographic Redundancy feature.

You must manually activate the secondary System Manager server to manage the elements when:

- The primary System Manager server fails.
- The network fails to isolate one of the System Manager systems or one or more adopter elements or both.

This scenario is called the primary nonoperational scenario or rainy day scenario.

This document provides the procedures required in a primary nonoperational scenario to reconfigure the GR-unaware elements in the system. After the reconfiguration is complete, the elements can communicate with the secondary System Manager server to receive management or configuration information. This document also describes the functioning of GR-unaware elements with System Manager in general and the secondary System Manager server in particular.

Note:

The system does not replicate the `/etc/hosts` file of the primary System Manager server to the secondary System Manager server. If you have elements that depend on the entries present in the `/etc/hosts` file of the primary server, you must make the appropriate entries during the failover process.

Related links

Geographic Redundancy terminology on page 67
Geographic Redundancy terminology on page 67

Elements Geographic Redundancy manageability status matrix

The following table provides the status of managing the elements from the System Manager Geographic Redundancy perspective:

Element	Version	Geographic Redundancy-enable status	Notes
Avaya Aura® Session Manager	6.3	Active-Standby (Auto)	
	6.2 and earlier	GR-unaware	
Communication Manager	6.2 and earlier	Active-Standby (Manual)	
CS 1000	7.5	Active-Active	
Meeting Exchange	6.2	GR-unaware	
Conferencing	7.0	GR-unaware	
Presence Server	6.1.4	GR-unaware	
CallPilot	5.0	GR-unaware	
Messaging	Avaya Aura® Messaging 6.0, 6.1, and 6.2	GR-unaware	
	Modular Messaging 5.0, 5.1, and 5.2		
	CMM 5.2, 6.0, and 6.2		
IP Office	6.2	GR-unaware	
M3K Gateway	3.0	GR-unaware	
Visualization, Performance and Fault Manager	3.0	Active-Active	
Application Enablement Services	6.2	GR-unaware	
Call Center Elite	6.2	GR-unaware	

Table continues…

Element	Version	Geographic Redundancy-enable status	Notes
One-X Client Enablement Services	6.2	GR-unaware	
One-X Client Attendant	4.0	GR-unaware	
Avaya one-X® Agent	2.5	GR-unaware	
Avaya Aura® Contact Center	6.3	Active-Active	

Configuring various elements to change to the secondary System Manager

Introduction

The sections describe how to reconfigure various GR-unaware elements that the secondary System Manager server manages when the server is activated during outages for an extended period of time, typically for more than 4 hours.

For outages that are less than 4 hours and that occur due to a primary System Manager server failure or a partial network breakdown, do not activate the secondary System Manager server.

If you perform the failover, the recovery process might take a few hours, depending on the data size and whether the recovery is done using the primary or secondary System Manager data.

Session Manager 6.3 configuration

Session Manager 6.3 elements are GR-aware.

In the normal operation mode, all Session Manager 6.3 elements communicate with the primary System Manager server for provisioned and configuration data.

You can configure both the primary and the secondary System Manager servers as unique trap destinations on each element. During a failover, the primary System Manager server becomes nonoperational, and you must manually activate the secondary System Manager server. Subsequently, all Geographic Redundancy-aware Session Manager elements automatically switch to the secondary System Manager server by using the Arbiter process of Session Manager.

In the primary nonoperational mode, each Session Manager element continues to interact with the primary System Manager server until the element receives an Activation notification from the secondary System Manager server. After the Session Manager element receives a secondary Activation notification, the element switches to the primary nonoperational mode.

In the primary nonoperational mode, the Session Manager element continuously polls the two System Manager servers to determine the current states.

The Session Manager element continues to communicate with the current managing System Manager server until there is a network disconnect or fragmentation. If there is a disconnect, for example, because of a network split, the Session Manager element switches to System Manager that is reachable within the network if that System Manager is in the activated state.

Note:

From the web console of the active System Manager, you can override the automatic switching of Session Manager by using the Manage option.

Session Manager elements support only Manage operation. These elements do not support the Geographic Redundancy UnManage operation.

Related links

Configuring Session Manager Release 6.2 and earlier during GR failover on page 91
Configuring Session Manager Release 6.2 and earlier during failback on page 91
Problems in managing Session Manager 6.1 or 6.2 using System Manager 6.2 on page 92

Configuring Session Manager Release 6.2 and earlier during GR failover

Session Manager 6.2 or earlier releases are GR-unaware elements.

About this task

During a failover, perform this procedure to configure the Session Manager elements to switch to the activated secondary System Manager server:

Procedure

1. Log in to Session Manager as `cust` or `service`.
2. Run the `ChangeManagementIP` script with the secondary System Manager IP address or FQDN as the target.
3. Stop Session Manager.

   Session Manager registers as a DRS node with the secondary System Manager server.
4. Start Session Manager.

   The Session Manager element is marked for repair and gets DRS initial load from the secondary System Manager server.

   The system overwrites the existing data of the element with the current data in the secondary System Manager database.

Related links

Session Manager 6.3 configuration on page 90

Configuring Session Manager Release 6.2 and earlier during failback

During the failback when the primary System Manager server is back online after an outage or failure and ready to serve the devices, you must perform the restore operation. During the restore operation, you can retain the primary or the secondary System Manager database.

About this task

⚠ **Caution:**

The following procedure impairs service. Therefore, schedule the restore operation outside of service hours.

When the primary System Manager server is functional, to switch back the System Manager elements earlier than Release 6.3 to the primary System Manager server and resume normal operational behavior, perform the following procedure.

Procedure

1. Log in to Session Manager as `cust` or `service`.
2. At the prompt, perform the following:
   a. Enter `cd /opt/Avaya/bin`.
   b. Enter `ChangeManagementIP` and provide the IP address or FQDN of the secondary System Manager server as the target.

   The command changes the configuration on the element. The system prompts for the enrollment password of the primary System Manager server.
3. Stop Session Manager.

   Session Manager registers as a DRS node with the primary System Manager server.
4. Start Session Manager.

   The Session Manager element is marked for repair and gets DRS initial load from the primary System Manager server.

   The system overwrites the existing data of the element with the current data in the primary System Manager server.

Next steps

After the recovery operation is complete, enable the Geographic Redundancy replication on System Manager web console.

Related links

Session Manager 6.3 configuration on page 90

Problems in managing Session Manager 6.1 or 6.2 using System Manager 6.2

Do not manage Session Manager 6.2 or 6.1 using System Manager 6.2. If you deploy SIP Endpoints, ensure that this configuration is not a long-term configuration as some functionality is lost in the configuration.

Users cannot successfully complete certain Personal Profile Manager (PPM) operations if the SIP phone is registered to a System Manager 6.1 or 6.2 that is getting service from System Manager 6.3. For example:

- Add a contact to the contact list.

- Update a contact on the contact list.
- Delete a contact from the contact list.
- Change and save the phone volume settings.
- Change and save specific phone settings using the **Home** > **Settings** menu on the phone, for example, from the 96x1 SIP phone.
- Save the phone identity and update the time of the latest PPM login in the database.

The system internally saves the phone settings and the volume settings operations in the phone, but the settings are lost when you reboot the phone. To retain the settings, the user must log out and log in again. Ensure that another user does not log in to the same phone before the original user logs in back.

Related links

Session Manager 6.3 configuration on page 90

Communication Manager configuration

Configuring Communication Manager during GR failover

Communication Manager is GR-unaware, regardless of the software release.

About this task

When the primary System Manager server has failed and the secondary System Manager server is activated, the replication is disabled.

Perform this procedure to configure the Communication Manager elements to switch to the secondary System Manager server.

Procedure

1. Log on to the web console of the secondary System Manager server.
2. In the left navigation pane, click **Services** > **Inventory** > **Manage Elements**. The system displays the status of Communication Manager as Unmanaged. You cannot administer the Communication Manager elements that System Manager does not manage.
3. Select the Communication Manager elements that you can manage or administer.
4. Click **More Actions** > **Manage**.
5. Click **Inventory** > **Synchronization** > **Communication Manager**.
6. Select the newly managed Communication Manager elements.

   Ensure that the system displays the Communication Manager state as Managed.
7. Select Initialize data for selected devices, and click **Now**.

   The secondary System Manager server retrieves all data from Communication Manager and is now ready to administer and manage Communication Manager.

Note:

You must perform the Communication Manager synchronization only if Communication Manager is not synchronized with the secondary System Manager server, which happens if the secondary System Manager server is not synchronized with the primary server due to a split network. If you are unsure whether Communication Manager is synchronized with the current System Manager, follow the Synchronization steps.

Configuring Communication Manager during GR failback

About this task

Perform the Geographic Redundancy failback operation to resume normal operational behavior.

Procedure

1. Log on to the web console of the primary System Manager server.
2. Deactivate the secondary System Manager server.

   In this state, the heartbeat mechanism between the primary and secondary System Manager servers resumes as in a normal operation scenario, but the Geographic Redundancy replication between the System Manager servers is disabled.
3. Perform the recovery operation and retain the primary or the secondary database of System Manager. During recovery, you can select one of the following databases:
   - The database of the primary System Manager server.
     - The primary System Manager server resumes the state that the server was in before becoming nonfunctional.
     - You cannot see the administration that is performed while the secondary System Manager server manages the devices on the primary System Manager server. Inconsistency in data between Communication Manager and the primary System Manager database is likely. Therefore, run the initialize data job of Communication Manager. If you fail to initialize data, the data between Communication Manager and the primary System Manager server remains inconsistent.
   - The database of the secondary System Manager server.
     - The system overwrites the data in the primary System Manager server.
     - The system restores all the administration or changes done while the secondary server was serving the devices to the primary System Manager server.
     - The primary System Manager server displays the status of all Communication Manager servers that the secondary System Manager manages as UnManaged.

       To manage the Communication Manager servers, navigate to **Home** > **Services** > **Inventory** > **Manage Elements** on the primary System Manager server and click **More Actions** > **Manage**.

Next steps

Enable the Geographic Redundancy replication on System Manager web console.

Communication Manager configuration when the primary System Manager server is nonoperational

In the primary nonoperational scenario, you might reach some of the Communication Manager elements from only one of System Manager servers.

Configuring Communication Manager during GR failover when only the primary server is reachable

Communication Manager Release 6.2 and later have a feature to notify all the changes made outside System Manager, for example, using ASA and MSA to the configured System Manager. To leverage the notify feature in System Manager Geographic Redundancy, configure Communication Manager with the IP addresses of the primary and the secondary System Manager server in the notification list.

About this task

For Communication Manager elements that you can reach only from the secondary System Manager server, perform the following procedure to configure Communication Manager elements to change to the secondary System Manager server.

Note:

Perform the same procedure during failback by reversing the roles of the primary and secondary System Manager servers.

Procedure

1. Log on to the web console of the primary System Manager server.
2. In the left navigation pane, click **Services** > **Inventory** > **Manage Elements**.

   The system displays the status of Communication Manager as Unmanaged. You cannot administer Communication Manager elements that System Manager does not manage.
3. Select Communication Manager elements that the secondary System Manager server must manage.
4. Click **More Actions** > **Manage**.
5. Log on to the web console of the secondary System Manager server.
6. In the left navigation pane, click **Services** > **Inventory** > **Manage Elements**.

   The system displays the status of Communication Manager as Unmanaged. You cannot administer the Communication Manager elements that System Manager does not manage.
7. Select Communication Manager elements that you must change to the secondary System Manager server.
8. Click **More Actions** > **Manage**.
9. Click **Inventory** > **Synchronization** > **Communication Manager**.

   Perform Step 10 only if Communication Manager is not synchronized with the secondary System Manager server. This can happen if the secondary System Manager server is not synchronized with the primary System Manager server due to reasons such as the nonoperational state of the primary or split network.

10. Select the newly managed Communication Manager elements.

    Ensure that the system displays the manageability status of Communication Manager as Managed.

11. Select Initialize data for selected devices, and click **Now**.

    The secondary System Manager server retrieves all data from Communication Manager and is now ready to administer and manage Communication Manager.

    Note:

    To find the difference between data on the primary and secondary System Manager servers during failback, use **Services** > **Geographic Redundancy** > **Restore Data**. The Restore Data dialog box displays comparative data between the primary and secondary System Manager servers when the primary System Manager server is nonoperational. This includes the number of elements that were managed by the primary and secondary System Manager servers, the number of entities modified on the primary and secondary System Manager servers, and the link to the audit logs. With the comparative data, you can decide whether to use secondary or primary System Manager data during failback.

CS 1000 configuration

CS 1000 elements are Active-Active GR-aware. The GR-aware CS 1000 elements are configured to interact with both primary and secondary System Manager servers. The element communicates with System Manager servers for Authentication and Authorization (A&A) related operations. Typically, the element leverages A&A services from the System Manager server that is closest to the element regardless of whether the server is in the primary or secondary mode. The secondary System Manager can serve A&A requests in both standby and active modes.

CS 1000 server deployments are of two types:

- VxWorks-based servers
- Linux-based servers

Related links

Configuring CS 1000 SNMP alarms on page 96
Configuring VxWorks-based CS 1000 servers on page 97
Configuring Linux-based CS 1000 servers on page 97
Limitations to the CS 1000 and CallPilot functionality support on System Manager on page 98

Configuring CS 1000 SNMP alarms

Procedure

1. Get the port number for the CS 1000 SNMP profile.

   For more information, see TrapListener service. The default port is 10162.

2. Configure CS 1000 SNMP alarms on the CS 1000 element by using the port number that you received.

   For more information, see *Fault Management - SNMP Avaya Communication Server 1000*, NN43001-719.

3. Manage alarms on System Manager.

   For more information, see Manage alarms.

Related links

CS 1000 configuration on page 96
Alarming on page 909
TrapListener service on page 948
Alarming on page 909
TrapListener service on page 948

Configuring VxWorks-based CS 1000 servers

Procedure

Run the following commands to register the information on CS 1000 servers:

```
Register UCMSecurity System
join secDomain
```

Related links

CS 1000 configuration on page 96

Configuring Linux-based CS 1000 servers

System Manager Geographic Redundancy deployment does not support some of the CS 1000 functionality. For more information, see Limitations to the CS 1000 and CallPilot functionality support on System Manager.

Procedure

1. On the Security Configuration page, click **Full security configuration** and **Security Configuration**.

   The system displays the FQDN validation page.

2. Confirm that the (TLAN) IP address and FQDN values are correct, and click **Next**.

   The system displays the Select server type page.

3. Click **Member server** and click **Next**.

   The system displays the Enter server information page.

4. Enter the (TLAN) IP address of the primary security server, and click **Next**.

   The system displays the Verify primary security server fingerprint page.

5. Verify that the FQDN and fingerprint information for the primary security server is valid, and enter the following details in appropriate fields:
   - The primary security server user ID, that is, a UCM user ID with System Administrator role.
   - The primary security server password of the user.
6. Click **Next**.

   The system displays the Enter certificate information page.
7. Enter information in appropriate fields.
8. Click **Finish**.

   The system displays the Security Configuration Progress page.
9. To complete the configuration process, click **Restart**. to restart the web server.

   The Security Configuration Progress page confirms that the server is restarting.

   The restart process might take up to 5 minutes to complete. You can then establish a new session and log on with your security administrator credentials. The registration process requires configuration of the primary System Manager information on the element. The secondary server information is provided to the element when the element registers with the primary server.

Related links

CS 1000 configuration on page 96

Limitations to the CS 1000 and CallPilot functionality support on System Manager

System Manager server state		CS 1000 and CallPilot functionality support available	
Primary server	**Secondary server**	**From the primary server**	**From the secondary server**
Active, reachable from the secondary server	Standby	• Authentication (SSO) • Authorization (RBAC) • Trust Management • Starting of Remote Element Managers • Alarm Management (Display CS 1000 alarms) • Log Harvesting • Audit Log Collection • IPSec Manager • SNMP Manager	• Authentication (SSO) • Authorization (RBAC) • Starting of Remote Element Managers

Table continues…

System Manager server state		CS 1000 and CallPilot functionality support available	
Primary server	**Secondary server**	**From the primary server**	**From the secondary server**
		• Corporate Directory • Registration of the new CS 1000 member • User Management of CS 1000 and CallPilot elements • Starting of Deployment Manager • Starting of Patch Manager	
Nonoperational	Standby	The primary server is nonoperational. Therefore, no functionality is available from the primary server.	• Authentication (SSO) • Authorization (RBAC) • Starting of Remote Element Managers
Nonoperational	Active	The primary server is nonoperational. Therefore, no functionality is available from the primary server.	• Authentication (SSO) • Authorization (RBAC) • Starting of Remote Element Managers • Alarm Management (Display CS 1000 Alarms) • Audit Log Collection

Related links

CS 1000 configuration on page 96

Meeting Exchange configuration

Meeting Exchange elements are GR-unaware. All communications except for WebLM are initiated from System Manager to Meeting Exchange. For licensing, a WebLM client on Meeting Exchange initiates communication with System Manager. For Meeting Exchange configuration, the data on System Manager is stored in the form of a Binary Large Object (BLOB) and synchronized with the element by using a scheduler job that runs every minute. The Meeting Exchange element is registered with System Manager. As these entities are replicated from the primary to the secondary server, information about the Meeting Exchange elements is present with the secondary System Manager server as well. You do not have to explicitly establish trust between the Meeting Exchange element and System Manager.

Related links

Element configuration on page 100

License management on page 100

Element configuration

In the failover scenario, you can perform all Meeting Exchange configuration changes from the activate secondary System Manager server. The system synchronizes the changes with the Meeting Exchange element by using Scheduler job. You do not require to make changes on the Meeting Exchange element in this case.

Related links

Meeting Exchange configuration on page 99

License management

To provision licensing from the secondary server, reassociate the Meeting Exchange element with the secondary server. To reassociate the Meeting Exchange element, remove the Meeting Exchange entry from **Services** > **Inventory** > **Manage Elements** of the secondary System Manager server and add the entry back again.

Related links

Meeting Exchange configuration on page 99

Presence Server configuration

Presence Server 6.2.x and earlier elements are GR-unaware. During failover, configure the Presence Server elements manually to switch to the secondary System Manager. Presence Server elements are registered in System Manager from **Services** > **Inventory**. All Presence Server configuration data is replicated from the primary to the secondary System Manager server.

Related links

Configuring Presence Server on page 100

Configuring Presence Server

About this task

Perform this procedure to switch Presence Server elements to the secondary server:

Procedure

1. Create a backup of the Presence Server data after the failover to be invoked manually by an operator after the failover of System Manager.
2. Run the `changeSMGRFQDN.sh` script on Presence Server element to change Presence Server System Manager configuration from the primary System Manager to secondary System Manager.

The script changes all configurations on the Presence Server element but does not affect Presence Server entries or configuration on System Manager. Presence Server calls InitTM to establish trust with the secondary System Manager. The element is re-registered on the secondary System Manager. The element is registered in DRS and **Services** > **Inventory**. As part of the registration, Presence Server element is added in `/etc/hosts` of the secondary System Manager. DRS marks the element for repair and sends the initial load of data to the element. Data on System Manager overwrites data on Presence Server element.

3. Log out or log in to the endpoints on failover.
4. Create a backup of Presence Server element after System Manager failover to ensure that the new configuration data is backed up.
5. To ensure continued serviceability support during primary nonoperational scenarios, configure Presence Server elements with both the primary and secondary System Manager servers as trap destinations.

   For instructions to configure trap destinations on Presence Server element, see *Administering Avaya Aura® Presence Services*.

Related links

Presence Server configuration on page 100

CallPilot configuration

CallPilot elements are GR-unaware. All communication with CallPilot is always initiated from System Manager. CallPilot does not store the IP address or FQDN of System Manager. In other words, System Manager points to CallPilot, but CallPilot does not point to System Manager. Use the Quantum UI to add the CallPilot element to System Manager. The system stores the element information in Elements tables through the UDDI interface and replicates to the secondary System Manager. The system provisions the System Manager data to the CallPilot element through the CallPilot adapter integrated with UPM. During a failover or an Active-Active scenario, CallPilot elements can be serviced using any of the active System Manager. The secondary System Manager must have CallPilot certificates. CallPilot certificates are imported in the primary System Manager server. The system replicates the certifications to the secondary server using file replication.

System Manager Geographic Redundancy deployment does not support some CallPilot functionality. For more information, see Limitations to the CS 1000 and CallPilot functionality support on System Manager.

Related links

Limitations to the CS 1000 and CallPilot functionality support on System Manager on page 98
Limitations to the CS 1000 and CallPilot functionality support on System Manager on page 98

Messaging configuration

Messaging elements are GR-unaware. However, the Messaging element manager is GR-aware. Messaging includes Avaya Aura® Messaging, Modular Messaging, and Communication Manager Messaging.

Related links

Configuring Messaging in the normal operational mode on page 102
Configuring Messaging when the primary System Manager server is nonoperational on page 103
Configuring Messaging during GR failback on page 103
Configuring Messaging during split network on page 104

Configuring Messaging in the normal operational mode

Before you begin

- Add both the primary and secondary servers as Trusted Servers in the Messaging system.
- Update the **Login**, **Password**, and **Confirm Password** fields with the appropriate trusted server defined on the Messaging system.

Procedure

1. Log on to the primary System Manager server.
2. On the System Manager web console, click **Services** > **Inventory**.
3. In the left navigation pane, click **Manage Elements**.
4. On the Manage Elements page, click **New** and add the Messaging system.
5. Provide the name and IP address of the Messaging system.
6. On the **Attributes** tab, fill the **Login**, **Password**, and **Confirm Password** fields with the corresponding name and password of the Messaging trusted server.
7. Click **Inventory** > **Synchronization** > **Messaging System**. Select the required Messaging element, and click **Now**.
8. Perform one of the following:
    - If synchronization is successful, perform the administration task on Messaging.
    - If synchronization fails, check the login details for Messaging.
9. Log on to the secondary System Manager server.
10. On the System Manager web console, click **Services** > **Inventory**.
11. In the left navigation pane, click **Manage Elements**.
12. Ensure that the Messaging system that has been added is visible on the Manage Elements page.

Related links

Messaging configuration on page 102

Configuring Messaging when the primary System Manager server is nonoperational

Perform this procedure to switch the Messagingsystem to the secondary System Manager when the primary System Manager server fails.

Before you begin

- Add both the primary and secondary servers as Trusted Servers in the Messaging system.
- Update the **Login**, **Password**, and **Confirm Password** fields with the appropriate trusted server defined on the Messaging system.

Procedure

1. Log on to the Messaging system that System Manager manages.
2. Add the secondary System Manager server as Trusted Servers in the Messaging system.
3. Log on to the secondary System Manager server.
4. On the System Manager web console, click **Services** > **Inventory**.
5. In the left navigation pane, click **Manage Elements**.
6. On the Manage Elements page, select the Messaging system that you want to change to the secondary System Manager server.
7. Click **Edit**.
8. On the **Attributes** tab, fill the **Login**, **Password**, and **Confirm Password** fields with the corresponding name and password of the Messaging trusted server.
9. Click **Commit**.
10. Click **Inventory** > **Synchronization** > **Messaging System**, and select the required Messaging element.
11. Click **Now**.

    The secondary System Manager server retrieves all data from Messaging and is now ready to administer and manage Messaging.

Related links

Messaging configuration on page 102

Configuring Messaging during GR failback

Before you begin

Complete the GR failback from the database of the primary System Manager server.

Procedure

1. Log on to the primary System Manager server.

   If the trusted server entry for the primary System Manager server is already present in Messaging, perform from the Step 3 e.

2. **(Optional)** Remove the secondary System Manager server as the trusted server in the Messaging system.
3. If you select the database of the secondary System Manager server to recover the data, perform the following steps:
    a. On the web console of the primary System Manager server, click **Services** > **Inventory**.
    b. In the left navigation pane, click **Manage Elements**.
    c. Select the Messaging element that you must change to the primary System Manager server.
    d. Click **Edit**.
    e. On the Manage Elements page, navigate to the **Attributes** tab and update the **Login**, **Password**, and **Confirm Password** fields with the corresponding name and password of the Messaging trusted service.
    f. Click **Commit** to apply the changes.
    g. Click **Inventory** > **Synchronization** > **Messaging System**.
    h. Select the required Messaging element, and click **Now**.

       The primary System Manager server retrieves all data from Messaging and is now ready to administer and manage Messaging.

Related links

Messaging configuration on page 102

Configuring Messaging during split network

About this task

Do not activate primary and secondary System Manager servers except during scenarios such as the primary System Manager server is nonoperational. When the primary System Manager server is nonoperational, not all elements are reachable from either System Manager servers.

Perform the procedure on the primary System Manager server. You cannot administer Messaging on the secondary System Manager server in the standby mode.

Procedure

1. Log on to the primary System Manager server and the System Manager server and verify that the system displays the replication status as disabled.
2. Add System Manager as the trusted server in the Messaging system.

   If the server is already added as the trusted server, update the login and password details of Messaging for both System Manager servers.
3. Click **Services** > **Inventory**.
4. In the left navigation pane, click **Synchronization** > **Messaging System**.
5. Select the Messaging element and click **Now**.

6. Perform one of the following:
    - If the synchronization is successful on both System Manager servers, perform the administration task for Messaging on both System Manager servers.
    - If the synchronization fails, check the login details for Messaging.

      While performing administrative tasks on Messaging, the system displays a warning message that the changes can result data inconsistency.
7. To perform administration tasks only on the primary System Manager server, remove the trusted server entry of the secondary System Manager server from Messaging.

Related links

Messaging configuration on page 102

Avaya Aura® Conferencing configuration

Avaya Aura®Conferencing elements are GR-unaware.During a failover or split network, you must manually configure to point the Avaya Aura® Conferencing element to the secondary System Manager server.

The following components of Avaya Aura® Conferencing are integrated with System Manager:

- License Management
- Trust Management
- User Management
- Logs
- Single Sign-On
- Role based access control
- Alarms

Related links

Configuring Avaya Aura Conferencing to be managed by System Manager on page 105
License management on page 107
Trust management on page 107
Single Sign-On and Role Based Access Control on page 108
User management on page 108
Logs on page 108
Alarms on page 108

Configuring Avaya Aura® Conferencing to be managed by System Manager

Before you begin

From System Manager, get the information for the community string and the Trap Listener port number.

About this task

For the Avaya Aura® Conferencing components to function, configure the IP address and FQDN of the active System Manager in the Element Manager console of Avaya Aura® Conferencing.

Procedure

1. On the web browser, type `http://<IP address>:12120`.

   where *IP address* is the logical IP address of the server that is running the Element Manager Internal OAM Service.

2. Press `Enter`.

   The system displays a webpage with the IP address that you entered and the **Launch Element Manager Console** link.

3. Click **Launch Element Manager Console**.
4. In the navigation pane of **Element Manager Console**, select **Addresses**.
5. In the Addresses window, click **Add (+)**.
6. In the Add IPv4 Address dialog box, complete the following fields:
   - **Logical Name**: Type SMGRAddress.
   - **IPv4 Address**: Type the IP address of the primary System Manager.
7. Click **Apply**.
8. Repeat Step 3 through Step 5 on the secondary System Manager, and enter a logical name and IP address.
9. In the navigation pane, click **External Nodes**.
10. In the External Nodes window, click **Add (+)**.
11. In the Add External Nodes dialog box, complete the following fields:
    - **Name**: Type SMGRNode.
    - **IPv4 Address**: Select SMGRAddress from the list.
12. Click **Apply**.
13. Repeat Step 8 through Step 10 for the secondary System Manager, and enter a name.

    Select the logical name that you entered in Step 6.

14. In the navigation pane, click **OAM Profiles** > **OSS Servers**.
15. Click **Add (+)**.
16. In the Add OSS Server dialog box, complete the following fields:
    - **Name**: Type a name, for example, SmgrOssServer.
    - **Node**: Select SmgrExtNode from the list.
    - **Use External OAM Network**: Do not select this check box.

17. Click **Apply**.
18. Repeat Step 12 through Step 15 for the secondary System Manager, and enter a name.

    Select the node entered in Step 11.
19. In the navigation pane, click **OAM Profiles** > **SNMP Managers**.
20. Click **Add (+)**.
21. In the Add SNMP Manager dialog box, complete the following fields:
    - **Name**: Type a name, for example, SmgrSnmpManager.
    - **Community**: Type the community string as obtained from System Manager.
    - **Servers**: Select the server name you created in Step 14, for example, SmgrOssServer.
    - **Trap Port**: Type the Trap Listener port number as obtained from System Manager.
22. Click **Apply**.
23. Repeat Step 17 through Step 20 for the secondary System Manager, and enter a name, the community string, and the trap port.

    Select the server name that you entered in Step 16.
24. Restart Element Manager through SSH to the server.

Related links

Avaya Aura Conferencing configuration on page 105

License management

Avaya Aura® Conferencing license key is installed on System Manager for forwarding license requests to the Avaya WebLM server residing on System Manager. For initial setup with the primary or active System Manager, follow the procedure in *Deploying Avaya Aura® Conferencing*. During a failover in a System Manager Geographic Redundancy setup, for license management to work, reconfigure the IP address and FQDN to match the IP address and FQDN of the active System Manager.

Related links

Avaya Aura Conferencing configuration on page 105

Trust management

For the initial setup, follow the procedures in *Deploying Avaya Aura® Conferencing*. Because the same root Certificate Authority exists on the primary and the secondary System Manager, you can use the same end-identity certificate for both System Manager servers. During a failover in a System Manager Geographic Redundancy setup, for trust management to work, reconfigure the IP address and FQDN to match the IP address and FQDN of the active System Manager.

Related links

Avaya Aura Conferencing configuration on page 105

Single Sign-On and Role Based Access Control

For the initial setup, follow the procedures in *Deploying Avaya Aura® Conferencing*. In a System Manager Geographic Redundancy setup, all elements in the inventory, such as Avaya Aura® Conferencing Element Manager and Avaya Aura® Conferencing Provisioning Client, admin users and passwords, Role Based Access Control (RBAC) attributes replicate between the primary and secondary System Manager. For Single Sign-On (SSO) and RBAC to function during a failover, reconfigure the IP address and FQDN to the IP address and FQDN of the active System Manager.

Related links

Avaya Aura Conferencing configuration on page 105

User management

For the initial setup, follow the procedures in *Deploying Avaya Aura® Conferencing*. In a System Manager Geographic Redundancy setup, all elements in the inventory, user profiles, and user data in the System Manager database replicate between the primary and secondary System Manager. During a failover in System Manager Geographic Redundancy setup, Single Sign-On or RBAC must work for user management. Reconfigure the IP address and FQDN to match with the IP address and FQDN of the active System Manager.

Related links

Avaya Aura Conferencing configuration on page 105

Logs

For the initial setup, follow the log forwarding procedures in *Deploying Avaya Aura® Conferencing*. In a System Manager Geographic Redundancy setup, send the logs to the active System Manager. In a GR-enabled System Manager pair, the enrollment password is the same for the primary and active System Manager servers. During a failover in a System Manager Geographic Redundancy setup, for log forwarding to the active System Manager, run the logAgent script again with the IP address or FQDN of the active System Manager, the same https System Manager port, and the same enrollment password.

Related links

Avaya Aura Conferencing configuration on page 105

Alarms

For the initial setup, follow the alarm forwarding procedures in *Deploying Avaya Aura® Conferencing*. You can configure Avaya Aura® Conferencing to use two SNMP managers and hence two alarm destinations. See section 5.8.2 for configuring primary and secondary System Manager servers as two trap destinations.

Related links

Avaya Aura Conferencing configuration on page 105

IP Office configuration

IP Office elements are GR-unaware. During failover, split network, or failback, perform the procedures from this section to ensure data integrity and proper administration of IP Office from System Manager. As the System Manager certificates contain an entry of the secondary System Manager in the **SAN** field, the same trust continues to work between the secondary System Manager and the IP Office element.

❗ **Important:**

The System Manager lock is maintained on the IP Office device to ensure that changes are not provisioned on the device outside System Manager. You can only make configuration changes on IP Office after removing the System Manager lock. For more information, see *Implementing IP Office*.

Related links

Configuring IP Office in normal operational mode with SCEP enabled on page 109
Configuring IP Office in normal operational mode with SCEP disabled on page 110
IP Office configuration when the primary System Manager is nonfunctional on page 110
IP Office configuration in the Active-Active scenario on page 111
Alarms on page 111
User management on page 111

Configuring IP Office in normal operational mode with SCEP enabled

Procedure

1. Log on to the web console of the primary System Manager server.
2. On the System Manager web console, click **Services** > **Inventory**.
3. In the left navigation pane, click **Manage Elements**.
4. Click **New**.
5. On the Add IP Office page, provide the name, the IP address, and the valid user name and password for IP Office.
6. On the System Manager web console, click **Services** > **Security**.
7. In the left navigation pane, click **Certificates** > **Authority**.
8. Click **RA Functions** > **Add End Entity** and add IP Office as an entity and specify all required details.
9. On the IP Office device, open the security settings and perform the following:
    a. Set SCEP to **active**.
    b. Specify the correct IP address of System Manager and the certificate name that you added on System Manager.
    c. Set the received certificates check to **High**.

10. Verify that the system receives the SCEP requests from the device at the specified interval using system monitor for the IP Office device.

    The primary System Manager server is now ready to administer and manage the IP Office device.
11. On the web console of the primary System Manager, click **Services** > **Inventory**.
12. In the left navigation pane, click **Manage Elements**.
13. Log on to the web console of the secondary System Manager and click **Services** > **Inventory**.
14. In the left navigation pane, click **Manage Elements**.

    The Manage Elements page displays the IP Office devices that you added on the primary System Manager.

Related links

IP Office configuration on page 109

Configuring IP Office in normal operational mode with SCEP disabled

Procedure

1. Log on to the web console of the primary System Manager server.
2. On the System Manager web console, click **Services** > **Inventory**.
3. In the left navigation pane, click **Manage Elements**.
4. Click **New**.
5. On the Add IP Office page, provide the name, the IP address, and the valid user name and password for IP Office.
6. Click **Commit**.

   The primary System Manager server is now ready to administer and manage the IP Office device.
7. Log on to the web console of the secondary System Manager, and click **Services** > **Inventory**.
8. In the left navigation pane, click **Manage Elements**.

   The Manage Elements page displays the IP Office devices that you added on the primary System Manager.

Related links

IP Office configuration on page 109

IP Office configuration when the primary System Manager is nonfunctional

If the primary System Manager server is nonfunctional, the secondary System Manager server can administer and manage the IP Office device without any additional steps on the secondary System Manager.

Related links

IP Office configuration on page 109

IP Office configuration in the Active-Active scenario

If the primary System Manager server is nonfunctional, the secondary System Manager server can administer and manage the IP Office device without any additional steps on the secondary System Manager.

If the IP Office element can communicate with both System Manager servers, you can administer IP Office from both System Manager servers. The data from the two servers conflict. During recovery, you must select the database of only one System Manager, and the changes in the other database are lost.

Manage the IP Office elements from only one System Manager even in the Active-Active scenario so that you can select this database for recovery when the communication between the two System Manager servers is reestablished. For more information about managing IP Office from System Manager, see *Implementing the Avaya IP Office for an Aura Configuration*.

Note:

For configuring the trap destination, SCEP details, and WebLM server in a single step, run the Initial Installation Utility of Native B5800 Manager.

You can also use the installation utility to change the configuration on IP Office for the System Manager failover scenarios. As the System Manager certificates contain an entry of the secondary System Manager in the **SAN** field, the same trust continues to work between the secondary System Manager and IP Office.

Related links

IP Office configuration on page 109

Alarms

To ensure serviceability support in primary System Manager nonoperational scenarios, forward the alarms or traps from the IP Office elements to both the primary and secondary System Manager servers. Configure the IP Office device with IPs of both primary and secondary System Manager servers as a trap destination.

Related links

IP Office configuration on page 109

User management

IP Office elements are registered with System Manager in **Inventory** > **Manage Elements**. The inventory data is replicated from the primary System Manager to the secondary System Manager. When the secondary System Manager server is activated after failover, you can use the IP Office element for user provisioning from the secondary System Manager without any changes to the IP Office device.

Related links

IP Office configuration on page 109

Visualization, Performance, and Fault Manager

Visualization, Performance, and Fault Manager (VPFM) is Active-Active Geographic Redundancy-aware. VPFM is configured to communicate with primary and secondary System Manager servers. VPFM communicates with System Manager servers for Authentication and Authorization (A&A) operations, such as SSO and RBAC. Usually, the element leverages A&A services from the System Manager server which is closest to the element regardless of whether the server is in the primary or the secondary mode. The secondary System Manager can serve A&A requests in both the standby and active modes.

VPFM leverages System Manager for Common Service Client (SMGR-CS Client) that provides adopters with off-box SSO and RBAC solution that works with System Manager.

Application Enablement Services

Application Enablement Services (AES) uses the licensing feature of System Manager. When System Manager fails, you must reconfigure the WebLM client on AES to point to the correct System Manager for using Licensing Service.

You can configure AES to integrate with centralized System Manager WebLM.

Avaya Aura® Contact Center

Avaya Aura® Contact Center (AACC) is Active-Active GR-aware. AACC elements are configured to communicate with primary and secondary System Manager servers. The element communicates with System Manager servers for Authentication and Authorization (A&A) operations such as Single Sign-On (SSO) and Role Based Access Control (RBAC). Usually, the element leverages A&A services from the System Manager server that is closest to the element regardless of whether System Manager is in the primary or the secondary mode. The secondary System Manager can serve A&A requests in the standby and active modes.

Avaya Multimedia Messaging configuration

Avaya Multimedia Messaging is GR-unaware. During the failover of the primary System Manager, you must configure the Avaya Multimedia Messaging server manually to use the secondary System Manager server.

For procedures to configure the System Manager connection details on the Avaya Multimedia Messaging server, see *Deploying Avaya Multimedia Messaging*. The document is available on the support site at https://support.avaya.com.

Replacing System Manager servers

Replacement of System Manager servers

From the pair of System Manager servers that are configured with Geographic Redundancy, you might have to replace the primary System Manager server with a new primary System Manager server or move existing primary System Manager server to a different location. The following sections list the scenarios when you must replace the primary System Manager server and the key tasks involved in the replacement procedure.

Moving the existing primary System Manager server to a different location

Procedure

1. Disable the Geographic Redundancy replication.
2. Shut down the System Manager server, and relocate the server to a new location.
3. **(Optional)** Activate the secondary System Manager server.

   You activate the secondary server to ensure zero down time. If you do not activate the secondary server, do not perform Step 7 and Step 8.
4. Start the primary System Manager server.
5. If the primary System Manager server uses a different IP or FQDN or both, change the IP address, FQDN, or both on the primary System Manager server.

   For instructions to change the IP address or FQDN, see Changing the IP address and FQDN in System Manager.
6. Connect the primary System Manager server to the network.
7. Deactivate the secondary System Manager server if you already activated in Step 3.
8. Restore the data.
9. Enable the Geographic Redundancy replication.

Related links

Enabling the Geographic Redundancy replication on page 75

Restoring the primary System Manager server on page 78

Deactivating the secondary System Manager server on page 78
Disabling the Geographic Redundancy replication on page 76
Activating the secondary System Manager server on page 76
Enabling the Geographic Redundancy replication on page 75
Restoring the primary System Manager server on page 78
Deactivating the secondary System Manager server on page 78
Disabling the Geographic Redundancy replication on page 76
Activating the secondary System Manager server on page 76

Restoring the primary System Manager server using the old primary server backup data

About this task

When the primary System Manager server or the site fails, you can restore the primary System Manager server using the backup data from the old primary server.

Procedure

1. **(Optional)** Activate the secondary System Manager server.

   Activate the secondary server to ensure zero down time. If you do not activate the secondary server, do not perform Step 6 and Step 7.

2. On the new server, install the System Manager template that you later designate as primary server by using the cold standby procedure.

   For instructions to change over to the cold standby server, see *Upgrading Avaya Aura® System Manager on VMware in Virtualized Environment*.

3. If you must to use a different IP address or FQDN or both on the new primary System Manager server, change the IP address, FQDN, or both on the primary System Manager server. For more information, see Changing the IP address and FQDN in System Manager.

4. Connect the primary System Manager server to the network if not already connected to the network.

5. Deactivate the secondary System Manager server.

6. Restore the data.

7. Enable the Geographic Redundancy replication if not already enabled.

Related links

Enabling the Geographic Redundancy replication on page 75
Deactivating the secondary System Manager server on page 78
Disabling the Geographic Redundancy replication on page 76
Activating the secondary System Manager server on page 76
Recovering the primary System Manager server from disaster on page 116

Enabling the Geographic Redundancy replication on page 75
Deactivating the secondary System Manager server on page 78
Disabling the Geographic Redundancy replication on page 76
Activating the secondary System Manager server on page 76
Recovering the primary System Manager server from disaster on page 116

Restoring the primary System Manager server using the data on the secondary System Manager server

When the primary System Manager server or the site fails, you can restore the primary System Manager server using the data on the secondary System Manager server.

Procedure

1. Activate the secondary System Manager server if you have not already activated.
2. Create a backup of the secondary System Manager server.
3. On the new server, install the System Manager template and perform the following steps:
    a. Log on to the System Manager web console of the standalone server that you installed, and change the admin password.

       Ensure that the server meets the requirements for the Geographic Redundancy setup.

    b. Recover System Manager from disaster.
4. Deactivate the secondary System Manager server.
5. Restore the data.
6. Enable the Geographic Redundancy replication.

Related links

Enabling the Geographic Redundancy replication on page 75
Deactivating the secondary System Manager server on page 78
Disabling the Geographic Redundancy replication on page 76
Activating the secondary System Manager server on page 76
Recovering the primary System Manager server from disaster on page 116

Enabling the Geographic Redundancy replication on page 75
Deactivating the secondary System Manager server on page 78
Disabling the Geographic Redundancy replication on page 76
Activating the secondary System Manager server on page 76
Recovering the primary System Manager server from disaster on page 116

Replacing the secondary System Manager server on the site

About this task

From the pair of System Manager servers that are configured with Geographic Redundancy, you might have to replace the secondary System Manager server with a new secondary System Manager server or move existing secondary System Manager server to a different location. The reasons might be the following:

- Secondary System Manager failure
- Site failure
- Movement of the secondary to a different location.

Procedure

1. Create a backup of the primary System Manager server.
2. On System Manager web console, click **Services** > **Replication** and verify that the system synchronized all elements to the primary System Manager server the data replication is working.
3. On the new server, install the System Manager template. For instructions, see *Implementing Avaya Aura® System Manager*.
4. Convert the primary System Manager server to standalone server.
5. On System Manager web console, click **Services** > **Replication** and verify that the system synchronized all elements to the primary System Manager server the data replication is working.
6. Log on to System Manager web console of the standalone System Manager server that you installed and change the password.
7. Configure Geographic Redundancy.
8. Enable the Geographic Redundancy replication if you have not already enabled.

Related links

Enabling the Geographic Redundancy replication on page 75
Configuring Geographical Redundancy on page 73
Converting the primary System Manager server to the standalone server on page 83
Enabling the Geographic Redundancy replication on page 75
Configuring Geographical Redundancy on page 73
Converting the primary System Manager server to the standalone server on page 83

Recovering the primary System Manager server from disaster

Perform the system recovery process when the primary System Manager server becomes unavailable and when you do not have a backup to restore on the new System Manager server.

Before you begin

- For fresh installation of System Manager, change the default password for the system administrator user.
- Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.

About this task

Important:

During the system recovery of Geographic Redundancy, the active secondary System Manager server copies the data between the secondary System Manager server to the primary System Manager server. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

Procedure

1. Activate the secondary System Manager server.
2. Create a backup of the secondary System Manager server.
3. View and verify the virtual FQDN that is configured on the secondary System Manager server by using one of the following:
    - From the virtual FQDN configured in the System Manager certificate, perform one of the following:
        - On Firefox, click the 🔒 icon on the address bar of the browser. Click **More Information** > **View Certificate** > **Details**. In the **Certificate Details** area, click **Certificate** > **Extensions** > **Certificate Subject Alt Name**. The system displays two values for **DNS Name**. The first entry is the virtual FQDN.
        - On Internet Explorer, click **Certificate Error** next to the address bar and click **View Certificates** > **Details** > **Subject Alternative Name**. The first entry for **DNS Name** is the virtual FQDN.
    - From the command line interface, log in to the secondary System Manager server, and check the virtualFQDN property value in the `$MGMT_HOME/infra/conf/smgr-properties.properties` file.
4. On the new server, install the System Manager template that you later designate as primary server with the same virtual FQDN that you obtained in Step 3.
5. Log on to the web console of the new System Manager server to change the default password.
6. Log in to the command line interface of the newly created primary System Manager as root, and perform the following:
    a. Perform one of the following:
        - For Releases 6.3.1 and 6.3.0, type `sh $MGMT_HOME/geo/bin/rundisasterrecovery.sh <peer fqdn> <peer ip> <peerNodesmgrUserId> <peerNodesmgrPassword>`.

- For Release 6.3.2 and later, type `sh $MGMT_HOME/geo/bin/rundisasterrecovery.sh —FQDN <secondary fqdn> —IP <secondary IP> —ID <secondary System Manager web console system admin user name> —PASS <secondary System Manager Web console system admin password>`.

For example, **`$MGMT_HOME/geo/bin/rundisasterrecovery.sh -FQDN psvdbf24.dr.sdr.com -IP 144.235.244.244 -ID systemadmin -PASS T3mp123@`**.

The recovery process starts and takes about 40 minutes. The command runs in the background and the system creates nohup logs in the directory from where you run the **`rundisasterrecovery.sh`** command, which you can tail.

b. Type one of the following:

- `tail -f $AVAYA_LOG/mgmt/geo/disasterRecoveryScript.log`
- `tail -f nohup.out`

7. To quit the **`tail`** command, press `Control+C`.

   When the recovery process is complete, the system displays the message `Disaster Recovery has completed JBoss will be restarted, may take up to 15 minutes`. The system configures System Manager servers as a Geographic Redundancy pair with the secondary data on the primary System Manager server.

8. Deactivate the secondary System Manager server.
9. Restore the data from the primary System Manager server.
10. Enable the Geographic Redundancy replication.

    The system starts working in the normal operational mode.

Related links

Enabling the Geographic Redundancy replication on page 75
Restoring the primary System Manager server on page 78
Deactivating the secondary System Manager server on page 78
Activating the secondary System Manager server on page 76
Prerequisites for servers on Appliance Virtualization Platform in the Geographic Redundancy setup on page 69
Prerequisites for System Manager on VMware in the Geographic Redundancy setup on page 70

Enabling the Geographic Redundancy replication on page 75
Restoring the primary System Manager server on page 78
Deactivating the secondary System Manager server on page 78
Activating the secondary System Manager server on page 76
Prerequisites for servers on Appliance Virtualization Platform in the Geographic Redundancy setup on page 69
Prerequisites for System Manager on VMware in the Geographic Redundancy setup on page 70

Chapter 5: Managing groups and roles for resources

Managing groups

Group management

Group and Lookup Service (GLS) is a shared service that provides group administration and lookup service for managed resources. GLS encapsulates the mechanisms for creating, changing, searching, and deleting groups and group memberships. Use GLS to group resources in ways that work best for the business, such as organizing resources by location, organization, and function.

On the System Manager web console, with GLS, you can assign different roles to administrators and allow administrators to perform only limited tasks on group of resources. For example, you can create a user group so that only an authorized user can manage the user group.

GLS supports group administration for the following common resources:

- Shared across elements, such as roles and users
- Unshared element-specific resources

GLS contains a repository of groups and memberships from System Manager and other applications that use the GLS service. GLS synchronizes the resources with other Avaya applications and services that manage these resources. GLS maintains resource IDs and their group memberships. With GLS, you can search for one or more resources based on their attribute values and get resource attributes for one or more resources.

With GLS, you can perform the following operations:

- Create groups.
- View and change groups.
- Create duplicate groups by copying properties of existing groups.
- Move groups across hierarchies.
- Assign and remove resources for groups.
- Delete groups.
- Synchronize groups.

As a shared service, GLS reduces the time and effort involved by defining reusable groups of managed resources that more than one application or service requires. For example, you can use the group of resources to assign permissions through Role Based Access Control (RBAC).

Viewing groups

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group Management page, select a group and perform one of the following:
   - If the group is a selection-based group, click **View**.
   - If the group is a query-based group, perform the following:
     a. Click **View**.
     b. On the View Group page, click **Execute Query**.

   The system displays the View Group page with the details of the group and the resources assigned to the group.

Related links

View Group field descriptions on page 131
View Group field descriptions on page 131

Creating groups

About this task

You can create up to 300 groups.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group Management page, perform one of the following:
   - Click **New** to create a group.
   - Select a group and click **New** to create a subgroup within a group.
4. On the New Group page, enter the name, type, group membership, and a description of the group.
5. Click **Commit**.

   The system creates the new group.

Related links

New Group field descriptions on page 129
New Group field descriptions on page 129

Modifying groups

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group Management page, select a group.
4. Click **Edit** or **View** > **Edit**.
5. On the Edit Group page, enter the appropriate information.
6. Click **Commit** to save the changes to the database.

Related links

Edit Group field descriptions on page 132
Edit Group field descriptions on page 132

Creating duplicate groups

About this task

You can create a duplicate group by copying the properties of an existing group. When you create a duplicate group, the system copies all the information, except the hierarchy, from the existing group to the new group.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group Management page, select a group.
4. Click **Duplicate**.
5. On the Duplicate Group page, perform one of the following:
   - Click **Root** to create a duplicate group at the root level.
   - Select a group and click **Selected Group** to create a duplicate group within another group.

   The system displays a copy of the parent group on the Group Management page.
6. Click the plus sign (**+**) to view the subgroups in a group.

Related links

[Duplicate Group field descriptions](#) on page 134
[Duplicate Group field descriptions](#) on page 134

Deleting groups

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group Management page, select the groups that you want to delete.
4. Click **Delete**.
5. On the Delete Group confirmation page, click **Delete**.

   The system confirms the successful deletion of groups and displays the details of groups that the system failed to delete.

   The system does not delete the resources.

Related links

[Delete Group Confirmation field descriptions](#) on page 134
[Delete Group Confirmation field descriptions](#) on page 134

Moving groups

About this task

You can move a group from one hierarchy to another.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group Management page, select a group.
4. Click **More Actions** > **Move**.
5. On the Move Group page, perform one of the following:
   - To move a group to the root level, click **Root**.
   - To move a group to a different group or subgroup, select the target group or subgroup, and click **Selected group**.
6. To view the subgroups in a group, click the plus sign (**+**).

Related links

[Move Group field descriptions](#) on page 135

Move Group field descriptions on page 135

Synchronizing resources for a resource type

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group Management page, click **More Actions** > **Sync**.
4. On the Resource Synchronization page, in the **Type** field, select the type of resources.
5. Click **Sync**.

Related links

Resource Synchronization field descriptions on page 136
Resource Synchronization field descriptions on page 136

Assigning resources to a group

About this task

You can assign only resources of the type that is configured for the group. The type of resource that you can assign to a group is set when you create a group. For example, if the type of resource is set to Users, you can assign only user types to the group. If the type is set to ALL, you can assign all types of resource to the group.

Note:

In System Manager, the users that you add to a group can only manage the resources that are assigned to the group and cannot add new users.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group Management page, click **New**.
4. Enter the name of the group, and select a group type.
5. Perform one of the following:
   - To assign a resource to a new group, click **Assign Resources**.
   - To assign a resource to an existing group, perform one of the following:
     - Click **Edit** > **Assign Resources**.
     - Click **View** > **Edit** > **Assign Resources**.
6. On the Resources page, select a resource.

The Resources page displays all resources available in the application. You cannot select the resources that are assigned to a group.

You can also search for a resource by using **Advance Search**.

7. Click **Add To Group**.

   The system adds the selected resources to the group.

Related links

Resources field descriptions on page 139
Resources field descriptions on page 139

Searching for resources

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, perform one of the following:
   - Click **Groups**.
   - Click **Resources** and continue with Step 4.
3. On the Group Management page, perform one of the following:
   - Click **New** > **Assign Resources**.
   - Select a group and click **Edit** > **Assign Resources**.
   - Select a group and click **View** > **Edit** > **Assign Resources**.
4. On the Resources page, click **Advanced Search**.
5. In the **Criteria** area, perform the following:
   a. In the **Type** field, select the resource type.
   b. In the **Resource Attributes** area, select the attribute name, the matching operator, and the search string from the appropriate fields.
6. To add more than one search condition, click the plus sign (**+**).

   Click the minus sign (-) to delete a search condition. You can delete a search condition only if you have more than one search condition.
7. In the drop-down field, click **And** or **Or**.

   The system displays this option only when you use the plus sign (+) to add a search condition.
8. Click **Search**.

   The **Resources** section displays the resources that match the search criteria. If no resources match the search criteria, the **Resource** section displays the message `No records are found`.

Searching for groups

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group Management page, click **Advanced Search**.
4. In the **Resource Attributes** section, select the attribute name, the matching operator, and the search string from the appropriate fields.
5. To add more than one search condition, click the plus sign (**+**).

   Click the minus sign (**-**) to delete a search condition. You can delete a search condition only if you have more than one search condition.
6. In the drop-down field, select **And** or **Or**.

   The system displays this option when you use the plus sign (**+**) to add a search condition.
7. Click **Search**.

Related links

Resources field descriptions on page 139
Resources field descriptions on page 139

Filtering groups

About this task

You can apply filter to the following fields:

- **Name**
- **Type**
- **Hierarchy**

You can filter groups by a single column or multiple columns.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. On the Group Management page, click **Filter: Enable**.
4. In the **Name** field, enter the group name.
5. In the **Type** field, select the resource type.
6. In the **Hierarchy** field, enter the hierarchy level.

When you enter a hierarchy level, the table displays only those groups that you created under that level. For example, to view all groups that you created under root, enter / as the hierarchy level.

7. Click **Apply**.

   The page displays the groups that match the filter criteria.

8. **(Optional)** Perform the following:

   - To hide the column filters, click **Disable**.

     This action does not clear the filter criteria that you have set.

   - To clear the filter criteria, click **Clear**.

Filtering resources

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, perform one of the following:
   - Click **Groups**.
   - Click **Resources** and continue with Step 5.
3. On the Group Management page, select a group to assign a resource to an existing group.
4. Perform one of the following:
   - Click **New** > **Assign Resources**.
   - Click **Edit** > **Assign Resources**.
   - Click **View** > **Edit** > **Assign Resources**.
5. On the Resources page, click **Filter: Enable** and perform the following:
   a. In the **Name** field, enter the resource name.
   b. In the **Type** field, select the resource type.
6. Click **Apply**.
7. **(Optional)** 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 the resources that match the filter criteria.

Removing assigned resources from a group

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Groups**.
3. Perform one of the following:
   - Select the resources, and click **Remove** if you have assigned resources to the group while creating the group.
   - Select a group, and click **Edit** > **Remove**.
   - Select a group, and click **View** > **Edit** > **Remove**.

   The system removes the association of the resource with the group.

Group Management field descriptions

Field	Description
Select check box	The option to select a group.
Name	The name of the group.
Type	The group type based on the resources.
Hierarchy	The position of the group in the hierarchy.
Description	A brief description of the group.

Button	Description
View	Displays the View Group page with details of the selected group.
Edit	Displays the Edit Group page where you change the information of the selected group.
New	Displays the Create Group page where you can create a new group.
Duplicate	Displays the Duplicate Group page where you can duplicate a group to another selected group.
Delete	Deletes the selected groups.
More Actions > **Move**	Displays the Move page where you can move a group to another group.
More Actions > **Sync**	Displays the Resource sync page that you use to synchronize resources of a specific resource type.

Table continues…

Button	Description
Advanced Search	Displays fields where you can specify the criteria for searching a group.
Filter: Enable	Displays fields where you can set the filter criteria. This button is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This button is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters groups based on the criteria.
Select: All	Selects all groups in the table.
Select: None	Clears all check boxes.

Icon	Description
🔄	Refreshes the group information.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link in the upper-right corner of the page.

Field	Description
Criteria	The criteria for search operation. The page displays the following fields: • **Field 1**: The list of criteria to search groups. • **Field 2**: The list of operators for evaluating the expression. This list of operators depends on the criterion that you selected in **Field 1**. • **Field 3**: The value of the search criterion. The Group Management service retrieves and displays the groups that match this value.

Icon	Description
+	Adds a row below **Field 1**, **Field 2**, and **Field 3** to add more search conditions.
-	Deletes the row with the search conditions.

Button	Description
Clear	Clears the search value that you entered in **Field 3**.
Search	Searches the group based on the specified search conditions and displays the results in the **Groups** section.
Close	Cancels the search operation and hides the **Criteria** section.

New Group field descriptions

New Group

Field	Description
Name	The unique name of the group.
Type	The group type based on the resources. The options are: • **<Resource>**: To create a group with members of the same resource type. • **All**: To create a group without any restrictions on the members of the group. ✱ **Note:** You cannot change the group after you create a group.
Group Membership	The group type based on the resources. The options are: • **Query Based**: To create a group that contains resources that match a specific query criteria. Query-based groups can have resources only of a specific type. You can create only resource type query groups. Thus, these groups cannot have subgroups. • **Selection Based**: To create a group that contains resources based on static assignment. The groups can have subgroups. Subgroups and parent group might have members of the same resource type or different resource types. ✱ **Note:** You can create up to 400 members in a group.
Description	A brief description of the group.

Button	Description
Assign Resources	Displays the Resources page where you can search and assign resources to a group. ✱ **Note:** The **Assign Resources** button is available only when you select **Selection Based** for creating group members in the group.

Table continues…

Button	Description
Commit	Creates a new group with the specified configurations.
Cancel	Discards the changes that you made to the Create Group page and displays the Group management page.

Define Query

The page displays the following fields when you select **Query Based** for creating group members:

Field	Description
Name	The name of the resource.
Type	The resource type.
Define Query	Displays the following fields: • **Field 1**: The list of criteria that you can use to search resources. • **Field 2**: The list of operators for evaluating the expression. The list of operators depends on the criterion that you selected in **Field 1**. • **Field 3**: The value corresponding to the search criteria.

Button	Description
+	Adds a search condition row for defining the new search condition.
–	Removes a search condition.
Execute Query	Runs the query and fetches resources matching the search conditions defined in the query. The page displays the resources in the **Results** section. ✱ **Note:** The system displays the **Execute Query** button only when you create a query-based group.

Assigned Resources

The page displays the following fields when you select **Selection Based** for creating group members:

Field	Description
Name	The name of the resource.
Type	The resource type.

Button	Description
Assign Resources	Displays the Resources page that you use to search and assign resources to a group.
Remove	Removes the selected resources from the list of assigned resources.

View Group field descriptions

View Group

Field	Description
Name	The unique name of the group.
Type	The resources that the group contains.
Group Membership	The group type that is based on the resources. The options are: • If the group is selection-based, the system displays the assigned resources. • If the group is query-based, click **Execute Query** to view the assign resources.
Description	A brief description of the group.

Button	Description
Edit	Displays the Edit Group page where you can edit the group information.
Done	Closes the View Group page and displays the Group Management page.

Define Query

The page displays the following fields when you use the **Query Based** option for creating group members:

Field	Description
Define Query	Displays the following fields: • **Field 1**: The list of criteria that you can use to search resources. • **Field 2**: The list of operators for evaluating the expression. The list of operators depends on the criterion that you selected in **Field 1**. • **Field 3**: The value corresponding to the search criteria.

Button	Description
+	Adds a search condition row for defining a new search condition.
–	Removes the search condition.
Execute Query	Runs the query and fetches resources matching the search conditions defined in the query. The page displays the resources in the **Results** section. ✱ **Note:** The system displays the **Execute Query** button only when you create a query-based group.

The page displays the following fields for assigned resources:

Field	Description
Name	The name of the resource
Type	The resource type

Edit Group field descriptions

You can edit a group. However, you cannot edit the following fields:

- **Type**
- **Group Membership**

Edit Group

Field	Description
Name	The unique name of the group.
Type	The group type based on the resources. The options are: • **<Resource>**: To create a group with members of the same resource type. • **All**: To create a group without any restrictions on the members of the group.
Group Membership	The group type based on the resources.The options are: • **Query Based**: To create a group that contains resources that match a specific query criteria. Query-based groups can have resources only of a specific type. You can create only resource type query groups. Thus, these groups cannot have subgroups.

Table continues…

Field	Description
	• **Selection Based**: To create a group that contains resources based on static assignment. The groups can have subgroups. Subgroups and parent group might have members of the same resource type or different resource types. **Note:** You cannot change the group after you create a group.
Description	A brief description of the group.

Button	Description
Commit	Saves the changes in the database.
Cancel	Discards the changes that you made on the Edit Group page and displays the Group Management page.

Define Query

The page displays the following fields when you select **Query Based** for creating group members:

Field	Description
Name	The name of the resource.
Type	The resource type.
Define Query	Displays the following fields: • **Field 1**: The list of criteria that you can use to search resources. • **Field 2**: The list of operators for evaluating the expression. The list of operators depends on the criterion that you selected in **Field 1**. • **Field 3**: The value corresponding to the search criteria.

Button	Description
+	Adds a row for defining a new search condition.
–	Removes the row that defines the search condition.
Execute Query	Runs the query and fetches resources matching the search conditions defined in the query. The page displays the resources in the **Results** section. **Note:** The system displays the **Execute Query** button only when you create a query-based group.

Assigned Resources

The page displays the following fields when you select the **Selection Based** option for creating group members:

Field	Description
Name	The name of the resource
Type	The type of the resource

Button	Description
Assign Resources	Displays the Resources page where you can search and assign resources to a group.
Remove	Removes the selected resources from the list of assigned resources.

Delete Group Confirmation field descriptions

Field	Description
Name	The name of the group
Type	The group type based on the resources
Hierarchy	The position of the group in the hierarchy
Description	A brief description of the group
Subgroup Count	The number of subgroups in the parent group
Resource Count	The number of resources in the group

Button	Description
Delete	Deletes the groups listed in the table.
Cancel	Cancels the delete operation and displays the Group Management page.

Duplicate Group field descriptions

Field	Description
Select	The option to select a group.
Name	The groups under which you can create a copy of the selected group. Usethe plus sign (+) to expand a group.
Type	The group type based on resources.

Table continues…

Field	Description
Dynamic	The status that indicates whether the group uses a query to determine the members or contains static members. The options are: • **true**: Indicates that group membership is not permanent. • **false**: Indicates that the group contains static members.
Description	A brief description of the group.

Button	Description
Root	Creates a copy of the selected group at the root level.
Selected Group	Creates a copy of the group that you selected within the group.
Cancel	Discards the changes and displays the Group Management page.

Move Group field descriptions

Use this page to move a group to another group or to root level.

Name	Description
Select	The option to select a group.
Name	The groups to which you can move the selected group. Use the plus sign (+) to expand a group.
Type	The group type based on resources.
Dynamic	The status that indicates whether the group uses a query to determine the members or contains static members. The options are: • **true**: Indicates that group membership is not permanent. • **false**: Indicates that the group contains static members.
Description	A brief description of the group.

Button	Description
Root	Moves the selected group to the root level.
Selected Group	Moves the selected group to the group that you selected in the **Name** column.

Table continues…

Button	Description
Cancel	Closes the Move Group page and returns to the Group Management page.

Resource Synchronization field descriptions

Field	Description
Type	The resource type

Button	Description
Sync	Synchronizes resources for the selected resource type and displays the Group Management page.
Cancel	Discards the changes that you made to the Resource Synchronization page and displays the Group Management page.

Managing resources

Manage resources

System Manager contains different types of resources such as users and roles. You can view and filter these resources based on the search criteria. You can also add resources of the same or different types in a group.

Accessing resources

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Resources**.

Related links

Resources field descriptions on page 139
Resources field descriptions on page 139

Assigning resources to a new group

About this task

Use this functionality to create a new group and assign resources to the group. You can choose to create the new group at root level or within an existing group.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Resources**.
3. On the Resources page, select a resource from the Resources table or search for a resource using **Advanced Search**.
4. Click **Add To New Group**.
5. Perform one of the following:
   - To add a resource to a new group at root level, perform the following steps:
     a. On the Choose Parent Group page, click **Root**.
     b. On the Create Group page, enter the appropriate information.
     c. Click **Commit**.
   - To add a resource to a new subgroup under a group, perform the following steps:
     a. On the Choose Parent Group page, click a group.

        Note:

        To select a subgroup of a group, click **+** and click the subgroup.

     b. Click **Selected Group**.
     c. On the Create Group page, enter the appropriate information.
     d. Click **Commit**.

        Note:

        The system creates the new group and assigns the selected resources. The system adds the new group within the group that you selected on the Choose Parent Group page.

Related links

Resources field descriptions on page 139
New Group field descriptions on page 129
Resources field descriptions on page 139
New Group field descriptions on page 129

Adding resources to a selected group

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Resources**.
3. Select a resource from the resource table.

   You can also click the **Advanced Search** link to search a resource.
4. Click **Add To Group**.
5. On the Choose Group page, click a group.
6. Click **Selected Group**.

   The Group Management module assigns the selected resources to the selected groups on the Choose Group page.

Related links

Resources field descriptions on page 139
Resources field descriptions on page 139

Searching for resources

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Resources**.
3. On the Resources page, click **Advanced Search**.
4. In the **Criteria** section, in the **Type** field, select a resource type.
5. In the **Resource Attributes** section, perform the following steps:
   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. **(Optional)** To add another search condition, click the plus sign (**+**).

   Click the minus sign (**–**) to delete a search condition. You can delete a search condition only if you have more than one search condition.
7. In the drop-down field, click **AND** or **OR**.

   The system displays this option when you use the plus sign (**+**) to add a search condition.
8. Click **Search**.

The Resources section displays the resources matching the search criteria. If no resources match the search criteria, system displays the message `No records are found`.

Filtering resources

About this task

You can filter and view resources that meet the specified selection 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.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Resources**.
3. On the Resources page, click **Filter: Enable**.
4. Type the resource name in the **ID** field.

   You can apply filter on one column or multiple columns.
5. Select the resource type from the **Type** field.
6. Click **Apply**.

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

   The table displays resources that match the filter criteria.

Resources field descriptions

Resources section

Field	Description
Select	Use this check box to select a record.
ID	The unique name of the resource. Also known as native ID of the resource
Type	The type based on the resources.
View Details	The link displays the attributes and membership details of the selected resources on the same page.

Button	Description
Add to Group	Displays the Choose Group page. Use this page to choose a group in which you want to add the selected resource.
Add to New Group	Displays the Choose Parent Group page. Use this page to add the selected resources to a new group or to a chosen group.
Cancel	Closes the Resources page and take you to the Create Group page.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a resource.
Filter: Enable	Displays fields under the columns **ID** and **Type**. You can use them to set the filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters the resources based on the filter criteria.
Select: All	Select all the resources in the table.
Select: None	Clears the selection for the resources that you selected.
🔄	Refreshes the resource information in the table.

Attributes of Resource section

Field	Description
Name	The name of the attribute.
Value	The value assigned to the attribute for the resource.

Resource is member of following groups section

Field	Description
Name	The unique name of the group.
Type	The group type based on the resources it contains.
Hierarchy	The position of the group in the hierarchy.
Description	A brief description about the group.

Criteria section

Click **Advanced Search** to view this section. The **Advanced Search** link is available at the upper-right corner of the page.

Field	Description
Type	The types based on the resources it contains.

Table continues…

Field	Description
Resource Attributes	Displays the following three fields: • Drop-down 1: The criteria for searching a resource. The options are attributes of resources for the attribute type selected in the **Type** drop-down list. • Drop-down 2: The list of operators for evaluating the expression. The list of operators depends on the type of attribute selected in the Drop-down 1 list. • Field 3 – The value corresponding to the search criteria.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the resources matching the search conditions.
Close	Closes the Criteria section.
Advanced Search	Cancels the search operation and hides the **Criteria** section.

Choose Group field descriptions

Use this page to add resources to the selected groups.

Field	Description
Select	The option to select a group.
Name	The name of the group.
Type	The group type based on the type of resources. The options are: • Groups with members of the same resource type. • All: Groups having members of any resource types.
Dynamic	The status that indicates whether the group uses a query to determine the members or contains static members. The options are: • **true**: Indicates that group membership is not permanent. • **false**: Indicates that the group contains static members.
Description	A brief description of the group.

Button	Description
Expand All	Displays the subgroups of groups in the list.
Collapse All	Hides the subgroups of all expanded groups.
Selected Group	Adds the resource as a member of the group you selected.
Cancel	Closes the Choose Group page and returns to the Resources page.

Choose Parent Group field descriptions

Field	Description
Select	Use this option to select a group.
Name	The name of the group.
Type	The group type based on the type of resources. The options are: • Groups with members of the same resource type. • All: Groups with members of any resource types.
Dynamic	Indicates whether the group uses a query to determine its members or has static members. The options are: • **True**: Indicates that group membership is not permanent. • **False**: Indicates groups with static members.
Description	A brief description of the group.

Button	Description
Expand All	Displays the subgroups of groups listed in the table.
Collapse All	Hides the subgroups of all the expanded groups.
Root	Displays the New Group page. Use this page to create a new group. The selected resource is the member of this group.
Selected Group	Adds the resource as a member of the selected group.
🔄	Refreshes the resource information in the table.
Cancel	Closes the Choose Parent Group page and displays the Resources page.

Managing roles

Role Based Access Control

In System Manager, you require appropriate permissions to perform a task. The administrator grants permissions to users by assigning appropriate roles. Role Based Access Control (RBAC) in System Manager supports the following types of roles:

- Built-in
- Custom

With these roles, you can gain access to various elements with specific permission mappings.

Built-in roles are default roles that authorize users to perform common administrative tasks. You can assign built-in roles to users, but you cannot delete roles or change permission mappings in the built-in roles.

You can perform LDAP synchronization of Active Directory administrator roles with System Manager administrator roles. The capability includes system roles and custom roles on System Manager.

Related links

Custom roles on page 147
Built-in roles on page 143
Custom roles on page 147
Built-in roles on page 143

Built-in roles

Role	Privileges
Auditor	Gives read-only access to logs, configuration information, and audit files. With this role, you cannot run any command.
System Administrator	Gives the super-user privilege. System Administrator is the single all powerful role. Using this role, you can perform operations, such as the following: • Backup and restore • Scheduling jobs • Bulk import and export • Tenant administration • Geographic Redundancy operations • Element and user management • Software upgrade

Table continues…

Role	Privileges
	Note: • The System Administrator role replaces the Network Administrator role. System Manager does not support the Network Administrator role. • The page might not display all privileges that the System Administrator role supports. However, the system maps the permissions by implicit wild card rules.
Avaya Services Administrator	This role is equivalent to the System Administrator role. Depending on the access level that is set in the **E-token Authentication** section on the External Authentication page, System Manager assigns this role to the service personnel who logs in to the system through Etoken.
Avaya Services Maintenance and Support	Gives read-only access to maintenance logs, the capability to run diagnostics, and view the output of diagnostics tools. Using this role, you cannot run any command that might provide access to another host. System Manager assigns the role to the service personnel who logs in to the system through Etoken. The access level for the role depends on the value that is set in the **E-token Authentication** section on the External Authentication page.
Backup Administrator	Gives access to create backups, schedule backups, and restore backups.
Service Provider Administrator template	Gives permissions to: • Configure the solution • Manage the organization hierarchy of tenants. For example, site, department, and team. • Assign elements and resource permissions to the site • Manage end users for the tenant • Manage Tenant Administrators and Site Administrators **Note:** Service Provider Administrator Template is a template role.
Tenant Administrator Template	Gives permissions to: • Manage end users for the tenant • Communication Manager webpages **Note:** Tenant Administrator Template is a template role.
Discovery Admin	Gives permissions to configure the discovery parameters such as SNMP version, SNMP credentials, the subnetworks, and devices that you require to discover. You also have the permissions to schedule and run a discovery operation.

Table continues…

Role	Privileges
End-User	The administrator assigns this role to the telephony users. **Important:** You cannot log in to System Manager with the End-User role.
Communication Manager Admin	Gives you access and permission to perform all activities related to Communication Manager.
Messaging System Admin	Gives you access and permission to perform all activities related to Messaging or mailbox. You cannot perform any tasks related to Communication Manager as a Modular Messaging administrator.
Presence Admin	Gives read-write access to the Presence configuration.
Presence Auditor	Gives read-only access to logs, configuration information, and audit files. Using the Auditor role you cannot run any command that might provide access to another host.
Security Administrator	Gives read-write access to create other logins, create, modify or assign roles, install ASG keys, install licenses, and install PKI certificates and keys.
SIP AS Auditor	Gives read-only access to all SIP Foundation server management functionality.
SIP AS Security Administrator	Gives access to the security features provided by the SIP Foundation server. For example, Security Extension.
SIP AS System Administrator	Gives read and write access to all SIP Foundation server management functionality.
CS1000_Admin1	Gives unrestricted OAM access to most administrative functions and provisioning for all customers on all call servers and related elements. However, the role does not give access to the security and account administration. The role includes basic diagnostic (PDT1) privileges and access to network-level services for deployment, update, and SNMP management for CS 1000 systems. Gives authorization to use all roles on all User Management elements with all permissions. You can access the following elements: • All elements of type: CS 1000 • All elements of type: Deployment Manager • All elements of type: Linux Base • All elements of type: Patching Manager • All elements of type: SNMP Manager As this role gives permissions to All elements of type: Linux Base, you cannot use this role if you only require authorization to manage CS 1000 systems. The administrator must create a custom role for the user who requires to manage CS 1000 systems.
CS1000_Admin2	Provides unrestricted OAM access including security and account administration, and provisioning for all customers on all call server

Table continues…

Role	Privileges
	elements. The role also includes basic diagnostic (PDT1) privileges and access to network-level services for deployment, patching, SNMP, IPsec and SFTP management for CS 1000 systems. You can access the following elements: • All elements of type: CS1000 • All elements of type: Deployment Manager • All elements of type: IPSec Manager • All elements of type: Linux Base • All elements of type: Patching Manager • All elements of type: Secure FTP Token Manager • All elements of type: SNMP Manager As this role gives permissions to All elements of type: Linux Base, you cannot use this role if you only require authorization to manage CS 1000 systems. The administrator must create a custom role for the user who requires to manage CS 1000 systems.
CS1000_CLI_Registrar	Provides permission to register and unregister each CS 1000 elements, such as Call Server, MGC, and Media Card, using the local device OAM CLI. The role has a single permission value to allow or deny a user to register or unregister an element. You can access the following elements: • All elements of type: CS1000 • All elements of type: Linux Base The role does not have CS 1000 security or network level security privileges. The installation and repair technicians specifically require this role.
CS1000_PDT2	Gives full diagnostic and operating system access to all call servers. The role restricts access to administrative functions and customer provisioning data unless combined with another role. You can access All elements of type: CS1000.
MemberRegistrar	Gives limited access. You can register new members to the primary server. You can access the following elements: • All elements of type: IPSec Manager • All elements of type: LinuxBase
Patcher	Gives access to software maintenance functions such as update and maintenance. You can access the following elements: • All elements of type: Linux Base

Table continues…

Role	Privileges
	• All elements of type: Patching Manager
Service Technician	The system assigns the role to the service personnel when the service personnel connects to customer systems through the e-token. The Service Technician role has limited privileges as compared to the Avaya Services Administrator role.

Related links

Custom roles on page 147
Role Based Access Control on page 143
Custom roles on page 147
Role Based Access Control on page 143

Custom roles

On the Roles webpage, you can create a custom role that maps to specific elements of different types and specify customized permissions for the elements.

You can assign the roles that you created to users to perform specific tasks on an element. For example, a custom role that you create for a single element can only perform specific tasks on that element. A permission set defines the tasks that you can perform on the element with this role.

You can also define roles that apply to how elements and element types are hierarchically arranged in user-defined groups. When you map a permission to a group, the system takes that group into account when determining user permissions.

Related links

Built-in roles on page 143
Role Based Access Control on page 143
Built-in roles on page 143
Role Based Access Control on page 143

Viewing user roles

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role.

   In the right pane, the system displays the role name, a description, and the number of users, and also the elements that you can access by using the role.

Related links

Roles field descriptions on page 155

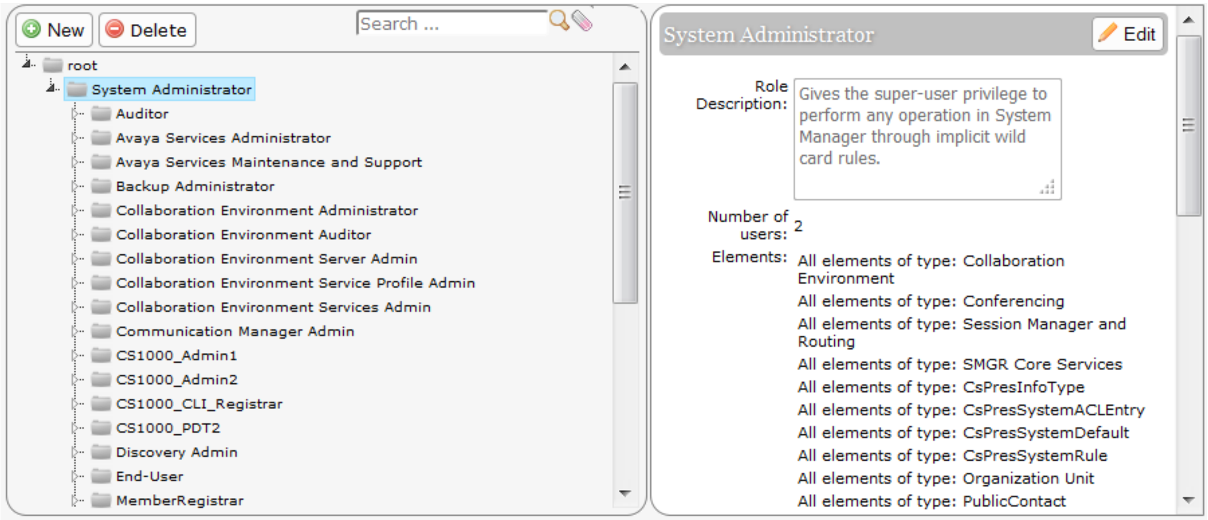
Roles field descriptions on page 155

Adding a custom role

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role, and perform one of the following:
   - Click **New**.
   - Right-click and select **New**.

   The role that you select becomes the parent of the role that you create. The permissions available to the new role are limited to the permissions of the parent role.


New
Delete
Search ...
root
System Administrator
Auditor
Avaya Services Administrator
Avaya Services Maintenance and Support
Backup Administrator
Collaboration Environment Administrator
Collaboration Environment Auditor
Collaboration Environment Server Admin
Collaboration Environment Service Profile Admin
Collaboration Environment Services Admin
Communication Manager Admin
CS1000_Admin1
CS1000_Admin2
CS1000_CLI_Registrar
CS1000_PDT2
Discovery Admin
End-User
MemberRegistrar
System Administrator
Edit

Role Description: Gives the super-user privilege to perform any operation in System Manager through implicit wild card rules.

Number of users: 2

Elements: All elements of type: Collaboration Environment
All elements of type: Conferencing
All elements of type: Session Manager and Routing
All elements of type: SMGR Core Services
All elements of type: CsPresInfoType
All elements of type: CsPresSystemACLEntry
All elements of type: CsPresSystemDefault
All elements of type: CsPresSystemRule
All elements of type: Organization Unit
All elements of type: PublicContact

   On the Add New Role page, the system displays the parent role in the **Parent Role Name** field.

4. Type the relevant information in **Role Name** and **Role Description** fields.
5. Click **Commit and Continue**.

   The system displays the Role Details page.

6. On the **Element/Service Permissions** tab, click **Add mapping** to define permissions for a role.

   You can also click **Copy All From** to copy all the permissions on all types of elements or services from an existing role. For instructions, see Copying permission mapping for a role.

7. Select a group from the **Group Name** field.

   Ensure that you create a group before you select the group. For instructions, see Creating groups. For instructions to assign resources to a group, see Assigning resources to a group.

8. **(Optional)** If you leave the **Group Name** field blank, in the **Element or Resource Type** field, click an element or **All**.
9. Click **Next**.

   The title of the Permission Mapping page displays the element type that you selected.
10. On the Permission Mapping page, change the permissions that are available for this role as appropriate.

    The system displays the permissions that are available for the parent of the role that you created. The system also displays unassigned permissions in a read-only format. Only an administrator can deny, change, or view the permissions for the role.
11. Click **Commit**.

    The system displays the Role Details page and the selected permissions.
12. Click **Commit**.

Related links

Copying permission mapping for a role on page 153
Creating groups on page 120
Assigning resources to a group on page 123
Add Mapping field descriptions on page 157
Add New Role field descriptions on page 156
Mapping permissions by using the template on page 152
Copying permission mapping for a role on page 153
Creating groups on page 120
Assigning resources to a group on page 123
Add Mapping field descriptions on page 157
Add New Role field descriptions on page 156
Mapping permissions by using the template on page 152

Adding a custom tenant administrator role

Procedure

1. On the System Manager web console, click **Services** > **Tenant Management** and perform the following:
   a. Create a tenant.
   b. Add the level 1 organization hierarchy or site to the tenant.
   c. **(Optional)** Add the level 2 and level 3 organization hierarchy to the tenant.

      For more information, see Creating a tenant.
2. On the System Manager web console, click **Users** > **Groups & Roles**.
3. In the left navigation pane, click **Roles**.

4. On the Roles page, select **System Administrator** and perform one of the following:
    - Click **New**.
    - Right-click and select **New**.
5. On the Add New Role page, enter the values in the **Role Name** and **Role Description** fields.
6. Click **Commit and Continue**.

    The system displays the Role Details page.
7. Click **Copy All From**.
8. In the **Copy from Role** field, click **Tenant Administrator Template**.
9. Click **Copy**.
10. On the Role Details page, click **Add Mapping**.
11. On the Select Element and/or Network Service to Map to Role page, perform the following:
    a. In **Element or Resource Type**, click **Organization Unit**.
    b. In **Element or Resource Instance**, click the name of the tenant that you created in Step 1, and click **Next**.
    c. Select **All** or **Create**, **Delete**, **Edit**, or **View** to set the appropriate permissions.
    d. Click **Commit**.
12. Perform Step 8 and Step 9 to provide appropriate permissions to the tenant for the following organization hierarchy:
    - Level 1 or the site
    - (Optional) Level 2 or the department
    - (Optional) Level 3 or the team

    In the **Element or Resource Instance** field, click site, department, or team as appropriate to which you want to set permissions. See Step 11b.
13. **(Optional)** On the Role Details page, click **Add Mapping**, and provide permission mapping.
14. Click **Commit** to confirm your settings.

Related links

Creating a tenant on page 1121
Creating a tenant on page 1121

Assigning permissions to access Solution Deployment Manager

About this task

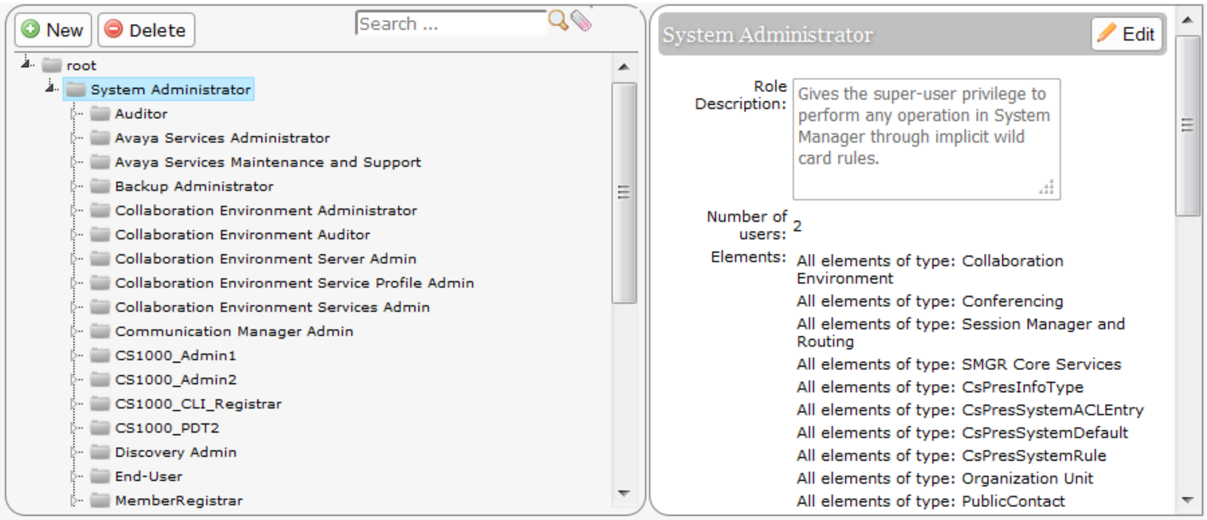
System Manager provides access permissions to Solution Deployment Manager through Role Based Access Control (RBAC) for elements, such as Communication Manager, Session Manager, Branch Session Manager, and IP Office. System Manager defines flexible access privileges for deployment, migration, upgrade, and update so that the users with administrator credentials can create their own roles.

With RBAC, System Manager supports access privileges at the element level and physical location level.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and perform one of the following steps:
   - Click **New**.
   - Right-click and select **New**.

   The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



- root
  - System Administrator
    - Auditor
    - Avaya Services Administrator
    - Avaya Services Maintenance and Support
    - Backup Administrator
    - Collaboration Environment Administrator
    - Collaboration Environment Auditor
    - Collaboration Environment Server Admin
    - Collaboration Environment Service Profile Admin
    - Collaboration Environment Services Admin
    - Communication Manager Admin
    - CS1000_Admin1
    - CS1000_Admin2
    - CS1000_CLI_Registrar
    - CS1000_PDT2
    - Discovery Admin
    - End-User
    - MemberRegistrar

System Administrator

Role Description: Gives the super-user privilege to perform any operation in System Manager through implicit wild card rules.

Number of users: 2

Elements: All elements of type: Collaboration Environment
All elements of type: Conferencing
All elements of type: Session Manager and Routing
All elements of type: SMGR Core Services
All elements of type: CsPresInfoType
All elements of type: CsPresSystemACLEntry
All elements of type: CsPresSystemDefault
All elements of type: CsPresSystemRule
All elements of type: Organization Unit
All elements of type: PublicContact

4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. In **Group Name**, select the group of templates to which you want to apply this permission.

   You can leave **Group Name** blank if you do not want to select a group.
7. Click **Next**.
8. In the left navigation pane, click **Manage Software** > **Communication Manager**.
9. Click **Next**.
10. In the **Element or Resource Type** field, select **Solution Deployment Manager**.
11. In Upgrade Management and VM Management, select appropriate permissions, and click **Commit**.
12. In the **Element or Resource Type** field, select **scheduleroperation**.

13. Click **Next**.
14. Select **all operations**, and click **Commit**.

    The user can now access the Solution Deployment Manager links.

    To assign IP Office upgrade permissions, select **IP Office** in **Element or Resource Type**, select **upgrade** on the Permission Mapping page. With this permission, the user can only upgrade IP Office devices. The **Communication Manager** link is unavailable to this user.

Mapping permissions by using the template

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. In the **Element/Service Permissions** tab, click **Add Mapping**.
5. In the **Element or Resource Type** field, select an element, for example, CS 1000.
6. Click **Next**.

   The system displays the permission mapping for the element that you selected.
7. Perform the following as appropriate to modify permissions:
   a. Select a different permission from the **Template for permission set** field.
   b. Select permissions.
   c. Clear permissions.
8. Click **Commit**.

Related links

Permission mapping field descriptions on page 159
Permission mapping field descriptions on page 159

Assigning users to a role

To assign a role to an end user, follow the instructions outlined in Assigning roles to a user. An end user is a user with no role or the End-User role.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.

4. On the Role Details page, click the Assigned Users tab.
5. Click **Select Users** to assign a role to users or edit a role.

   The system displays the Assigned Users page.

   > ✳ **Note:**
   >
   > The system does not display end users in the **Assigned Users** list. You can assign a role to an end user from **User Management** > **Manage Users**. For more information, see Assigning roles to a user.

6. Select users to whom you want to assign the role.
7. Click **Commit**.

   The system displays the permissions for the role on the Role Details page.

Related links

Assigning roles to a user on page 195
Assigned Users field descriptions on page 158
Assigning roles to a user on page 195
Assigned Users field descriptions on page 158

Unassigning users from role

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, click the Assigned Users tab.
5. Click **Selected Users**.
6. On the Assigned Users page, clear the check box of the user whom you want to unassign.
7. Click **Commit**.

Copying permission mapping for a role

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, click the **Element/Service Permissions** tab.

5. Click **Copy All From**.

   The system displays the Permission Mapping page.

6. In the **Copy From Role** field, select a role.

   The system displays all child roles of the parent of this role and all child roles of this role.

   Note:

   Using the **Copy From Role** option, you cannot copy permissions from the System Administrator role.

7. Click **Copy**.

   The system displays the Role Details page

8. Click **Commit**.

   The system displays the Roles page where you can view the details of the role.

Related links

Permission mapping field descriptions on page 158
Permission mapping field descriptions on page 158

Editing a custom role

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, edit the **Role Name** and **Description** fields.
5. Click **Commit and Continue**.
6. On the **Element/Service Permissions** tab, click **Add mapping** and change the permissions for a role as appropriate.

   For more information, see Mapping permissions using the template.

7. Click **Commit**.

Related links

Mapping permissions by using the template on page 152
Mapping permissions by using the template on page 152

Deleting custom roles

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select one or more roles that you must delete and perform one of the following:
    - Click **Delete**.
    - Right-click and select **Delete**.
4. On the Delete Roles page, click **Delete** to continue with the deletion.

    When you delete a role, the system deletes all child roles of the role.

    You cannot delete the implicit roles from the Roles page. However, the system deletes the implicit roles when the administrator deletes the tenant or site.

Roles field descriptions

The Roles page contains two panes. The left pane displays the tree structure of roles. The right pane displays the details of the role that you select on the left pane.

Field	Description
Role Description	A brief description of the role
No of users	The number of users associated with the role
Elements	The name of elements that are mapped to the role

Button	Description
New	Displays the Add New Role page where you can add a custom role.
Delete	Displays the Delete Roles page where you can confirm the deletion of the custom role.
Edit	Displays the Role Details page where you can change the custom role.

Icon	Description
🔍	Searches for the role based on the search text.
⌫	Clears the search text.

Add New Role field descriptions

Field	Description
Parent Role Name	The parent role that you selected on the Roles page to create the new role. **Parent Role Name** is a read-only field.
Role Name	The name of the custom role that you want to add. The name must be 1 to 256 characters long and can include characters: a-z, A-Z, 0-9, -, _, and space. You can add up to 1500 roles.
Role Description	A brief description of the role.

Button	Description
Commit and Continue	Saves the role name and description and takes you to the Roles Details page.
Cancel	Cancels the permission mapping and takes you back to the Roles page.

Related links

Copying permission mapping for a role on page 153
Creating groups on page 120
Assigning resources to a group on page 123
Copying permission mapping for a role on page 153
Creating groups on page 120
Assigning resources to a group on page 123

Role Details field descriptions

Field	Description
Parent Role Name	The parent role that you selected on the Roles page to create the new role. **Parent Role Name** is a read-only field.
Role Name	The name of the custom role that you want to add. The name must be 1 to 256 characters long and can include characters: a-z, A-Z, 0-9, -, _, and space.
Description	A brief description of the role that you add.

Button	Description
Commit	Saves the changes and returns to the Roles page.
Cancel	Discards the changes to the permission mapping and returns to the Roles page.
Add Mapping	Displays the permissions page where you can map permissions for the role.
Delete Mapping	Displays the Delete Mapping page where you can delete a permissions set.
Copy All From	Displays the Permission Mapping page where you can copy a permission set.

Add Mapping field descriptions

Field	Description
Group Name	The name of the group that you can select for the role. The options are: • When you select a group, the system disables the **Element or Resource Type** field. • When you do not select a group, the **Element or Resource Type** field is mandatory.
Element or Resource Type	The element types that are available. The system displays elements in **Element or Resource Instance** based on the element type that you select in this field.
Element or Resource Instance	The elements that are available or the resource instance. The field lists the available elements based on the element type that you selected in the **Element or Resource Type** field. When you select a group in **Group Name**, the system disables the **Element or Resource Type** field.

Button	Description
Next	Saves your changes in this page and takes you to the Permission Mapping page.
Cancel	Cancels your selection and takes you to the Roles Details page.

Related links

Copying permission mapping for a role on page 153

Creating groups on page 120
Assigning resources to a group on page 123
Copying permission mapping for a role on page 153
Creating groups on page 120
Assigning resources to a group on page 123

Assigned Users field descriptions

The system displays the Assigned Users page when you click **Select Users** on the **Assigned Users** tab of the Role Details page. You can select users to grant permissions that are associated with this role.

Field	Description
User Name	The name of the user that you assign to the role.
Full Name	The full name of the user that is assigned to the role.
Type	The type of user. The options are: • **local**: Indicates that users are stored in the directory server of System Manager. • **external**: Indicates that users are stored in the directory server of the customer.

Button	Description
Commit	Assigns the selected users to the role.
Cancel	Cancels the action and returns to the Role Details page.

Permission mapping field descriptions

The page displays the following fields when you click **Copy All From** on the Role Details page.

Field	Description
Copy from Role	The role from where you can copy all permission mappings for the element or service

Button	Description
Copy	Copies the permission mapping for your custom role.
Cancel	Cancels the copy action and returns to the Role Details page.

Permission mapping field descriptions

The page displays the following fields when you click **Add Mapping** on the Role Details page.

Field	Description
Template for permission set	The permission to which you want to map the role.
Select/Unselect All	A toggle button to select or clear the functions that users with a role can perform on the element.

Button	Description
Commit	Maps the permissions to the custom role.
Cancel	Cancels the permission mapping action and returns to the Role Details page.

Chapter 6: Granular role based access control

Granular RBAC

With Granular role based access control (RBAC), you can restrict access to resources such as Communication Manager servers, and objects of the resources such as endpoints and hunt groups.

When you create a role, you must select the resources for which a user should have access. You can assign permissions, or a combination of permissions to users. The permissions include adding, editing, deleting, or duplicating objects.

For certain objects, you can provide restricted access for a specific range to achieve range-level granularity of permissions. For example, for endpoints, you can provide access to a particular range of extensions.

Using Granular RBAC, you can define the range for the following Communication Manager objects:

Name	Supported range
Endpoint	Endpoint extension ranges
Agent	Agent extension ranges
Announcement	Announcement extension ranges
Audio Group	1–50
Best Service Routing	1–511
Holiday Table	1–999
Variables	From A-Z and AA-ZZ for all Communication Manager templates
Vector	1–8000
Vector Directory Number	Digits
Vector Routing Table	1–999
Service Hours Table	1–999
Coverage Answer Group	1–1500
Coverage Path	1–9999
Coverage Remote	1–10000
Coverage Time of Day	1–1000
Off PBX Endpoint Mapping	Off PBX Endpoint Mapping range

Table continues…

Name	Supported range
Group Page	1–999
Hunt Group	1–8000
Intercom Group	1–1024
Pickup Group	1–5000
Terminating Extension Group	1–32
Route Pattern	1–2000
Class of Restriction	0–995
Uniform Dial Plan	UDP range

- The roles and permissions also apply to the classic view apart from the Communication Manager objects mentioned.
- Granular RBAC is not applicable when you view the Communication Manager objects by clicking **Element Cut Through**. However, to access **Element Cut Through**, you must have the Element Cut Through permissions.
- When you assign a role to a user, the range permissions are considered along with the operation permissions.
- You must log off and log in for any permission you assign to take effect.

Implicit permissions required for Communication Manager objects

As a user, you require additional permissions to perform certain actions. The following table specifies the implicit permissions required for performing these actions:

Steps	Action	Implicit permissions that are required
	Duplicating an endpoint	Add endpoint permission
	Adding endpoints in bulk	Add endpoint permission
	Editing an endpoint extension	Edit endpoint permission
	Changing global parameters of endpoints	Edit endpoint permission
	Swapping endpoints	Edit endpoint permission
	Deleting endpoints in bulk	Delete endpoint permission
• Edit a user with the help of the Agent communication profile. • Import users in bulk	Changing an extension with an existing extension	Edit permission and delete permission

Table continues…

Steps	Action	Implicit permissions that are required
• Edit a user using the Agent communication profile. • Import users in bulk	Changing an extension with a new extension	Add permission and delete permission
• Edit a user using the Agent communication profile. • Import users in bulk	Changing other fields other than extension	Edit permissions
Check the port extension remove option, and assign an endpoint extension to an agent.	Deleting an endpoint	Delete agents and add agents permissions
	Editing agents in bulk	Edit agents permission
	Adding agents in bulk	Add agents permission
	Deleting agents in bulk	Delete agents permission
	Adding or editing a Communication Manager instance through inventory	One of the following permissions: • ALL • Audit • View Audit Report • Synchronization
	Using File Transfer Settings in Announcements	ALL in Announcements Edit permission Move permission
	Downloading backed up announcements Setting compact flash in announcements	ALL in Announcements
	Downloading audio groups	ALL in Audio Group
	Adding entries for AAR and ARS analysis	Add permission Edit permission
	Updating UDP entries	New permission Edit permission
	Manage UDP Group permission for a specific Communication Manager	Manage UDP Group permission in Communication Manager
	Adding, viewing, editing, and removing UDP Groups across Communication Managers	Add permission Edit permission View permission

Sample scenario for the range feature

When you assign a range for Hunt Group, and go to the **Hunt Group** > **New** page, the system prompts you to enter a qualifier. You can enter the hunt group number, or click **Next** to add the next available group.

- If you enter a group number that is not a part of the assigned range, the system displays an error message.
- If you enter a group number within the assigned range, the system displays the NCM screen, where you can complete the add operation.
- If you enter a group number that is already present, the system displays the *Identifier previously assigned* message.

Range in endpoints

You can assign range in endpoints and add permissions even for specific fields in endpoint. Specify a definite range, comma separated values, or a single value in the endpoints range field.

For example, type 5600:6000 to assign permissions for extensions 5000 to 6000 . Whenever you use **:** to specify the extension range, the starting and the ending extensions must have the same number of digits.

When you enter comma separated values like 1, 3, 7, 9, and 45, you assign the permissions only to these specified extensions.

Note:

Enter `*` in the **Range** field, to assign the permissions for the entire extension range.

- If you assign a specific endpoint range to a user, you can view, add, delete, edit and duplicate only those endpoints within the specified range.
- You can also assign a specific range to the **COR** and **Coverage Path** fields in endpoints.
- You can manage only those endpoint extensions within the specified range.
- For a user, you can assign only those extensions that you specify in the CM Endpoint Communication Profile. For example, if you assign the range 100:200 to user A, and user A adds an endpoint with extension 201, the system displays an error message and the endpoint add job fails.

Assigning range for endpoints

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. Click **Add..**.
4. Enter the name and the description for the role.
5. Click **Add Mapping**.
6. In **Group Name**, select the group of Communication Manager systems to which you want to apply this permission.

   You can leave **Group Name** blank if you do not want to select any group.
7. In **Element or Resource Type**, select **Communication Manager**.
8. In **Element or Resource Instance**, select the Communication Manager to which you want to apply this permission.

   When you select **Group Name**, this field appears disabled. By default, **Group Name** shows All.
9. Click **Next**.
10. On the Permission Mapping page, enter the range you want to specify in the **Extension Range** field.

    You can specify a definite range, enter comma separated values, or a single value in endpoints. For example, 5600:6000, 1, 3, 7, 9, and 45.
11. You can also assign operation permissions like **Bulk Add**, **Bulk Edit**, **Delete**, **Edit**, **List Usage**, **Swap**, **List Trace Station**.

    The user can perform only the actions that are assigned in the operation permissions.
12. Click **Commit**.

Assigning permissions in User Management

The range feature in endpoints and agents is also applicable in **User Management**. When you assign a range for endpoints and agents, as per the permissions that are defined, you can add, edit, delete, and duplicate only the extensions that are associated with the user. Range is validated when you assign an endpoint extension or an agent extension through the endpoint or agent editor.

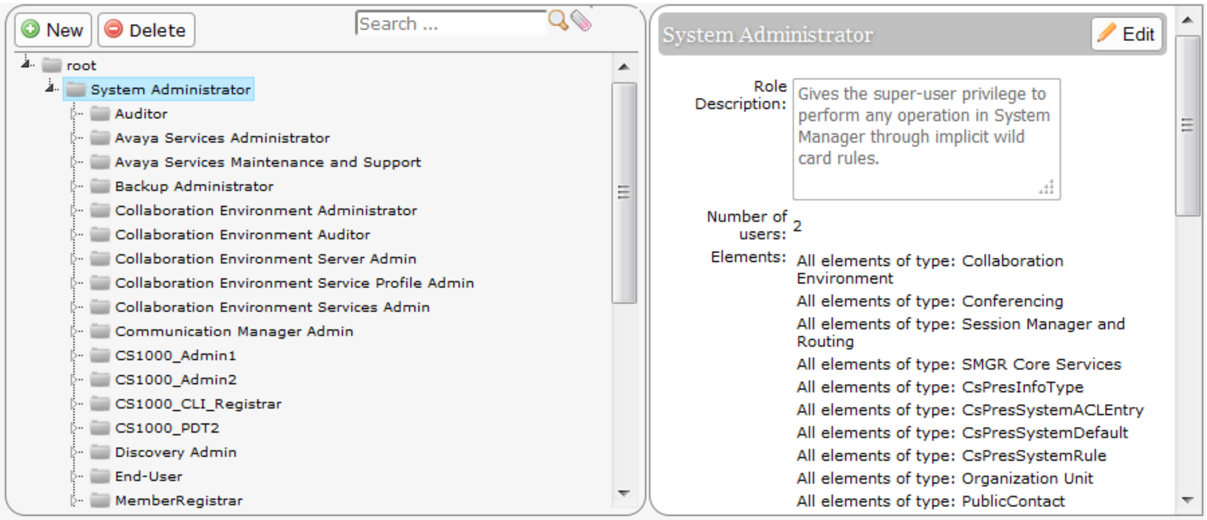
Assigning permissions through User Management

About this task

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and perform one of the following steps:
   - Click **New**
   - Right-click and select **New**.

   The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



root
- System Administrator
  - Auditor
  - Avaya Services Administrator
  - Avaya Services Maintenance and Support
  - Backup Administrator
  - Collaboration Environment Administrator
  - Collaboration Environment Auditor
  - Collaboration Environment Server Admin
  - Collaboration Environment Service Profile Admin
  - Collaboration Environment Services Admin
  - Communication Manager Admin
  - CS1000_Admin1
  - CS1000_Admin2
  - CS1000_CLI_Registrar
  - CS1000_PDT2
  - Discovery Admin
  - End-User
  - MemberRegistrar

System Administrator

Role Description: Gives the super-user privilege to perform any operation in System Manager through implicit wild card rules.

Number of users: 2

Elements: All elements of type: Collaboration Environment
All elements of type: Conferencing
All elements of type: Session Manager and Routing
All elements of type: SMGR Core Services
All elements of type: CsPresInfoType
All elements of type: CsPresSystemACLEntry
All elements of type: CsPresSystemDefault
All elements of type: CsPresSystemRule
All elements of type: Organization Unit
All elements of type: PublicContact

4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping**.
7. In **Group Name**, select the group of templates to which you want to apply this permission.

   You can leave **Group Name** blank if you do not want to select a group.
8. In the **Element or Resource Type** field, click **users**.
9. In the **Element or Resource Instance** field, click the Communication Manager devices to which you want to apply this permission.
10. Click **Next**.
11. On the Permission Mapping page, select the **Role Resource Type Action** and **Role Resource Type Attributes**.
12. Click **Commit**.

The system displays the Role Details page with the permission mapping you created.

13. Click **Add Mapping**.
14. To specify the operation resource type mapping, in the **Element or Resource Type** field, click **operation**.
15. Click **Next**.
16. On the Permission Mapping page, perform the following actions:
    a. Click **Others** > **RTS_Administration**.
    b. Click **Others** > **RTS_Administration/RTS_Edit_Operation**.
    c. Click **Users** > **Users/UserManagement**
17. Click **Commit**.

Field-level RBAC

System Manager supports field-level RBAC for Communication Manager objects. You can assign permissions for the following Communication Manager objects:

Communication Manager object	Field
Endpoints	• Name • Security Code • IP Softphone • IP Video Softphone • EC500 State • EC500 Button • Coverage Path 1 • Coverage Path 2 • Tenant Number • Extension Number • Type • Port • Name • Lock Messages • Hunt-to Station • BCC • TN

Table continues…

Communication Manager object	Field
	• Location • Loss Group • Speakerphone • Display Language • Survivable GK Node • Survivable COR • Survivable Trunk Dest • Message Lamp Ext • Mute Button Enabled • Media Complex Ext • Short/Prefixed Registration Allowed • LWC Reception • LWC Activation • LWC Log External Calls • CDR Privacy • Redirect Notification • Per Button Ring Control • Bridged Call Alerting • Active Station Ringing • H.320 Conversion • 4Service Link Mode • Multimedia Mode • MWI Served User Type • AUDIX Name • IP Hoteling • Auto Select Any Idle Appearance • Coverage Msg Retrieval • Auto Answer • Data Restriction • Idle Appearance Preference • Bridged Idle Line Preference • EMU Login Allowed

Table continues…

Communication Manager object	Field
	• Per Station CPN Send Calling No • Audile Message Waiting • Display Client Redirection • Select Last Used Appearance • Coverage After Forwarding • Multimedia Early Answer • Direct IP-IP Audio Connections • Always Use • IP Audio Hairpinning • Remote Softphone Emergency Calls • Emergency Location Ext • Conf/Trans on Primary Appearance • Bridged Appearance Origination Restriction • Call Appearance Display Format • IP Phone Group ID • Hot Line Destination – Abbreviated Dialing List Number • Hot Line Destination – Dial Code • Feature Button Assignments 1 - 3 • Button types displayed to the Administrator
Service Hours Table	• Description • Use time adjustments from location
Holiday Table	• Name
Hunt Group	• Group Name • Group Extension • Group Type • TN • COR • Security Code • ISDN/SIP Caller Display • ACD • Queue • Vector

Table continues…

Communication Manager object	Field
	• Coverage Path • Night Service Destination • NM Early Answer • Local Agent Preference • LWC Reception • Audix Name • Message Center • Ignore Call Forwarding • Re-hunt On No Answer (rings)
Announcements	• Annc Name • Annc Type • COR • TN • Queue • Rate • Protected • Group/Board

Note:

Field-level RBAC is applicable only for the Edit operation.

Field-level RBAC is not applicable when you add Communication Manager objects.

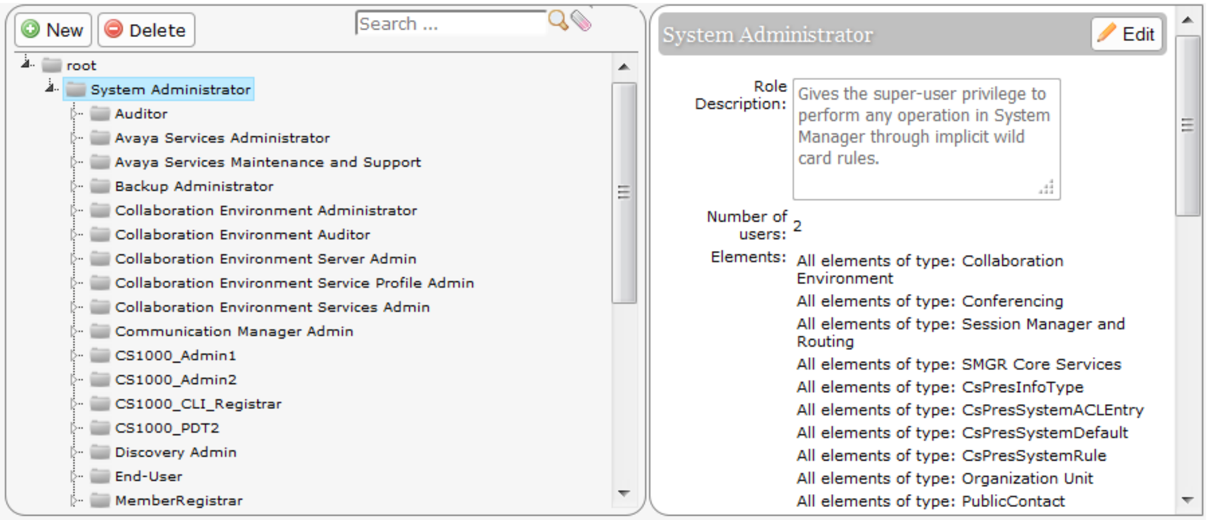
Assigning permissions for fields in endpoints

Field-level RBAC for Communication Manager objects is applicable only for the edit operation.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and perform one of the following steps:
    - Click **New**
    - Right-click and select **New**.

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



- root
  - System Administrator
    - Auditor
    - Avaya Services Administrator
    - Avaya Services Maintenance and Support
    - Backup Administrator
    - Collaboration Environment Administrator
    - Collaboration Environment Auditor
    - Collaboration Environment Server Admin
    - Collaboration Environment Service Profile Admin
    - Collaboration Environment Services Admin
    - Communication Manager Admin
    - CS1000_Admin1
    - CS1000_Admin2
    - CS1000_CLI_Registrar
    - CS1000_PDT2
    - Discovery Admin
    - End-User
    - MemberRegistrar

System Administrator

Role Description: Gives the super-user privilege to perform any operation in System Manager through implicit wild card rules.

Number of users: 2

Elements: All elements of type: Collaboration Environment
All elements of type: Conferencing
All elements of type: Session Manager and Routing
All elements of type: SMGR Core Services
All elements of type: CsPresInfoType
All elements of type: CsPresSystemACLEntry
All elements of type: CsPresSystemDefault
All elements of type: CsPresSystemRule
All elements of type: Organization Unit
All elements of type: PublicContact

4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping**.
7. In the **Element or Resource Type** field, click **Communication Manager**.
8. On the Permission Mapping page, in the **Endpoint Attributes Permission for Edit Operation**, and **Endpoint Buttons Permission for Edit Operation** sections, select the button and attributes that you want to assign to this role.
9. Click **Commit**.

   If you assign this role to a user, the user can edit only the fields that you have assigned in the Permission Mapping page.

Chapter 7: Managing users, public contacts, and shared addresses

Managing users

Users, public contacts, and shared addresses

Manage users

User Management is a shared service that users can gain access from the System Manager web console. User Management supports a logically centralized data store. Applications can gain access to this data store and get the user information that applications need. Administrators or end users do not need to enter user information for each application.

User Management provides administrators with mechanisms to:

- Administer all user attributes, contact information, group membership, user provisioning rule assignment, organization hierarchy assignment, and role assignment, also product-specific user data.
- For each product, extend the underlying user model for product-specific properties, attributes, and any relationship between the attributes.
- Manage specific aspects of user data such as changing a user name or address.

Using User Management, you can:

- Add user profiles.
- View, change, and delete existing user profiles.
- Assign or remove permissions, roles, groups, addresses, and contacts for users.
- Assign user provisioning rule and organization hierarchy.
- Add and change the communication profile of users.
- Change the identity and communication profile data of users in bulk.
- Bulk import users and their attributes, public contact, and shared addresses from an XML file.

  Bulk import users and their attributes from an Excel file.
- Bulk export users and their attributes to an XML and Excel file from the System Manager web console and command line interface.
- Search users.

User Management uses data synchronization to achieve a single-point user administration. User Management synchronizes the user data event that the system generates at the application level with the central user space and other connected applications. If an enterprise directory is connected, then User Management maintains synchronization at the enterprise level. User Management directly adjusts to the changes that occur in the enterprise directory, specifically additions, deletions, and modifications. For more information, see the Directory synchronization overview section.

Roles based access control (RBAC) applies to User Management so that the user role determines the access to user level tasks and access to administrative tasks. Users with login privileges must have permissions to add, change, and delete user accounts on the management console.

To perform the user provisioning by using User Management, map the user to the role with the following permissions:

Resource type	Permissions
All elements of type:elements	add, delete, edit, and view

To perform the user provisioning by using the user provisioning rule, map the user to the role with the following permissions:

Resource type	Permissions
All elements of type:elements	view

Manage public contacts

As an administrator, you can define public contacts of users in System Manager for an enterprise. You can share public contacts by all users in System Manager.

Manage shared address

All users in the enterprise can share the common addresses called shared address. As an administrator, you can create, change, and delete a shared address of users in the enterprise.

Access to administrative users

Starting from System Manager Release 6.3.8, when you create a role with access to **User Management**, you can restrict the access to the Administrative Users page.

The roles that are created earlier than Release 6.3.8 with permissions to access **User Management** can access the Administrative Users page by default. The roles continue to have permission after the upgrade to Release 6.3.8 or later. To restrict access to the Administrative Users page, clear the **Allow access to Administrative Users Web UI** check box on the Permission Mapping page.

To gain access to the Administrative Users page, log on to the System Manager web console and click the **Users** > **Administrators** link. The Administrative Users page displays the list of administrative users that are available in the system. By default, when you add user-related permissions to a role, the system selects the **Allow access to Administrative Users Web UI** permission.

End user self provisioning

Using the URL that administrator provides, end users can access the Self Provisioning web interface to change the communication profile password.

End users can start the self provisioning interface from any device that supports a web browser. For example, from a web browser on the computer, mobile phone, and notebook.

Related links

Enabling self provisioning on page 173

Changing the communication profile password from the self provisioning interface on page 173

Enabling self provisioning

About this task

Administrator must enable self provisioning on System Manager for the end user to change the communication profile password.

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Settings** > **SMGR**.
3. On the Edit Profile:SMGR page, set **Self Provisioning Status** to **true**.

   If you set the status to false, the system displays the message `The provisioning application is currently disabled. Please contact your system administrator.`

Related links

Changing the communication profile password from the self provisioning interface on page 173

Changing the communication profile password from the self provisioning interface

Before you begin

From **Services** > **Configurations** > **Settings** > **SMGR**, the administrator must set the **Self Provisioning Status** field to true.

If the option is set to false, the system displays the message `The provisioning application is currently disabled. Please contact your system administrator.`

About this task

Using this procedure, the end user can change the communication profile password from the Self Provisioning web interface.

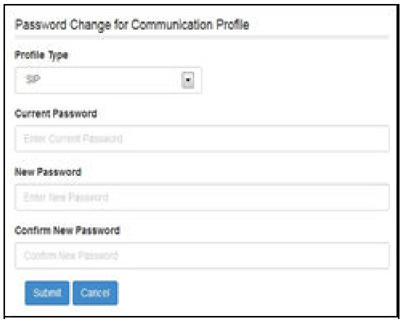
When the system is overloaded, the Self Provisioning web interface displays `The Provisioning Application has reached maximum supported load. Please try again after some time` message.

Procedure

1. To gain access to the Self Provisioning web interface, type `https://<IP address of System Manager>/selfprovisioning/`.
2. On the Login page, type the user ID and password and click **Login**.

   Note:

   - Use communication address as user name and communication profile password or SIP password as password.
   - For users with Communication Manager communication profile, use the Communication Manager extension and security password.
   - Do not leave the user name and password fields blank.
3. On the Password Change for Communication Profile page, in the **Profile Type** field, click SIP or H.323.

   Password Change for Communication Profile

   Profile Type: SIP

   Current Password

   New Password

   Confirm New Password

4. Type the current password and new password, and click **Submit**.

Related links

Enabling self provisioning on page 173

Viewing details of a user

Before you begin

You require appropriate permissions.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user.
4. To view details of the selected user account, click **View**.

Note:

You can only view details of one user account at a time.

Related links

User Profile View field descriptions on page 244

Creating a new user account

You can create new user account using this section or by providing the user provisioning rule.

Before you begin

- You require permission to add a new user account.
- The role must have the following permissions assigned:

  For resource type elements, all permissions in the **Role Resource Type Actions** section.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **New**.
4. On the New User Profile page, complete the following steps:
    a. **(Optional)** In the **Organization** section, select a tenant from the **Tenant** field.

       You must select a tenant only if the user must belong to a tenant.

    b. **(Optional)** In the **User Provisioning Rule** field, select a user provisioning rule.

       You can provide only one user provisioning rule.

       Note:

       When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

    c. Enter the required information in the remaining fields.
5. Perform one of the following:
    - To save the changes, click **Commit**.
    - To save the changes and stay on the same page, click **Commit & Continue**.

   Before you click **Commit**, ensure that all mandatory fields have valid information.

Important:

The Communication Manager systems that are undergoing synchronization or are busy, displays the following behavior:

- In Firefox, the system displays the status of the Communication Manager systems that are undergoing synchronization as disabled. The Communication Manager systems are available only after the synchronization is complete. To view the Communication Manager systems, you must start the new user operation again.
- In Internet Explorer, the system does not display the Communication Manager systems that are undergoing synchronization in the list. The Communication Manager systems are available only after the synchronization is complete. To view the Communication Manager systems, you must start the new user operation again.

Related links

Creating a new user profile using the user provisioning rule on page 176

New User Profile field descriptions on page 257

Creating a new user profile using the user provisioning rule

Before you begin

Ensure that the role has the following permissions:

For resource type elements, all permissions in the **Role Resource Type Actions** section.

About this task

When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **New**.
4. On the New User Profile page, complete the following fields:
   - **User Provisioning Rule**

     You can provide only one user provisioning rule.
   - **Last Name**
   - **First Name**
   - **Login Name**
5. Perform one of the following:
   - To save the changes, click **Commit**.

- To save the changes and stay on the same page for making further changes, click **Commit & Continue**.

Before you click **Commit**, ensure that all mandatory fields contain valid information.

The system creates the user with attributes that are defined in the user provisioning rule.

Related links

Creating a new user account on page 175
New User Profile field descriptions on page 257
Results of using the user provisioning rule on page 177

Results of using the user provisioning rule

You can expect the following results when you provision the user using the user provisioning rule.

Provisioning method	Scenario	Expected result
User management	Create user	
	The administrator selects the user provisioning rule without adding the communication profile data.	The system displays a warning message. The system applies the user provisioning rule and adds the communication profiles data based on the user provisioning rule.
	The administrator adds the communication profile data, and then selects the user provisioning rule.	The system displays a warning message. The system creates the communication profile based on the user provisioning rule and overwrites the communication profiles data with the data in the user provisioning rule.
	The administrator selects the user provisioning rule. The system populates the communication profile data for the user. The administrator changes the user provisioning rule to blank.	If the user provisioning rule is blank, the system removes all communication profiles that the system used from the user provisioning rule.
	Edit user	
	The communication profile data already exists for the user that was created using the user provisioning rule, and the administrator selects a different user provisioning rule.	The system displays an error message if a communication profile exists for the user and the same profile is present in the user provisioning rule that you select. If there are no conflicts in the communication profile, the system merges the communication profile with the existing communication profile and the new user provisioning rule that you select. For example, the user has the Session Manager communication profile that is

Table continues…

Provisioning method	Scenario	Expected result
		created using a user provisioning rule, and the administrator selects a different user provisioning rule that has the Communication Manager communication profile. The user now has the Communication Manager and Session Manager communication profiles.
	The communication profile data that is created without the user provisioning rule exists for the user. The administrator selects the user provisioning rule.	The system displays an error message if a communication profile exists for the user and the same profile is present in the user provisioning rule that you select. If there are no conflicts in the communication profile, the system merges the communication profile with the existing communication profile and the new user provisioning rule that you select. For example, the user has the Session Manager communication profile and the user provisioning rule that is created with Communication Manager communication profile. When the administrator uses the user provisioning rule, the user contains the Communication Manager and Session Manager communication profiles.
	The administrator sets the user provisioning rule to blank in the Edit User page.	The system disassociates the user provisioning rule with the user. The communication profiles created using the user provisioning rule remain unchanged.
Bulk import	Create user	
	The administrator creates the user using the bulk import feature from the XML or Excel file. The XML or Excel file contains the user provisioning rule without the communication profile data.	The system applies the user provisioning rule and populates the communication profiles provided in the user provisioning rule.
	The administrator creates the user using the bulk import feature from the XML or Excel file. The XML or Excel file contains the user provisioning rule with the communication profile data.	The communication profile data in the XML or Excel file takes precedence over the user provisioning rule. The system uses the user provisioning rule only for the communication profile that is not present in the XML or Excel file.
	Edit user	
	The communication profile data that is created using the user provisioning rule exists for the user.	The system disassociates the user provisioning rule with the user. The communication profiles in the Merge and

Table continues…

Provisioning method	Scenario	Expected result
	In bulk import, the user provisioning rule is not mentioned in the XML file.	Replace option with the Complete and Partial Import type remain unchanged.
	The communication profile data that is created without the user provisioning rule. The user provisioning rule is mentioned in the XML file.	The user import operation fails if any communication profile exists for the user and the same is present in the user provisioning rule provided in XML. If there are no conflicts in the communication profile, the system merges the communication profile with the existing communication profile and the new user provisioning rule that you provided in XML. For example, the user has the Session Manager communication profile that is created using a user provisioning rule, and the administrator selects a different user provisioning rule that has the Communication Manager communication profile. After import, the user contains the Communication Manager and Session Manager communication profiles.
	Note: You cannot select a different user provisioning rule for partial import. Use the complete XML import with Merge or Replace option to change the user provisioning rule.	
Directory synchronization	Create user	
	The user provisioning rule is configured in the LDAP mapping.	The system applies the user provisioning rule and populates the communication profiles provided in the user provisioning rule.
	Edit user	
	The communication profile that is created using the user provisioning rule exists for the user. The value of the user provisioning rule is changed in LDAP.	User synchronization fails if the communication profile exists for the user and the same profile is present in the new user provisioning rule that is configured in LDAP. If no conflicts in communication profile, then the system merges the communication profile with the existing communication profile and the new user provisioning rule that you select.
	The user provisioning rule is not associated with the existing user. The new user provisioning rule values are configured in LDAP for the user.	User synchronization fails if the communication profile exists for the user and the same profile is present in the new user provisioning rule that is configured in LDAP.

Table continues…

Provisioning method	Scenario	Expected result
		If no conflicts in communication profile, the system merges the communication profile with the existing communication profile and the new user provisioning rule that you select.
	The communication profile that is created using the user provisioning rule exists for the user, and the value of the user provisioning rule is set to blank in LDAP.	The system disassociates the user provisioning rule with the user. The communication profiles that are created using the user provisioning rule remain unchanged.

Modifying user accounts

Before you begin

- You require permissions to modify the user details. If you select a user that does not have the permission to modify the details, the system does not display the **Edit** button.
- The role must have the following permissions assigned:

  For resource type elements, all permissions in the **Role Resource Type Actions** section.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user.

   Note:

   At one time, you can edit only one user account.
4. To edit a user account, perform one of the following:
   - Click **Edit**.
   - Click **View** > **Edit**.
5. On the User Profile Edit page, perform the following:

   a. **(Optional)** In the **Organization** section, select a tenant from the **Tenant** field.

   You must select a tenant only if the user must belong to a tenant.

   b. **(Optional)** In the **User Provisioning Rule** field, select a user provisioning rule.

   You can provide only one user provisioning rule.

   Note:

   When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

   c. Enter the required information in the remaining fields.

For information, see User Profile Edit field descriptions.

- You cannot edit the tenant. If you select a different level 1 for the tenant from the organization hierarchy, the **Level 2** and **Level 3** fields become blank. You can select new values for level 2 and level 3. If you select a different level 2 for the tenant from the organization hierarchy, the **Level 3** field becomes blank. You can select a new value for level 3.
- If you must change the tenant, delete the user and associate the user with the tenant.
- System Manager does not automatically modify the user if the user provisioning rule changes.
- You can select a different user provisioning rule when you modify the user information.

✱ **Note:**

You can associate the user to an existing tenant.

6. Perform one of the following:
   - To save the changes, click **Commit**.
   - To save the changes and stay on the same page, click **Commit & Continue**.

Related links

User Profile Edit field descriptions on page 277
Results of using the user provisioning rule on page 177

Creating duplicate users

You can duplicate the user details to create a new user account by copying information from an existing user account. Using the Duplicate feature, you cannot copy the confidential information, such as addresses, private contacts and associated contacts in the contact list, password, and login name of the user.

Using the Duplicate feature, you can also copy the communication profiles like CM Endpoint and Session Manager. However, you cannot copy CS 1000 Endpoint Profile or CallPilot Messaging Profile communication. You must add the CS 1000 Endpoint Profile or CallPilot Messaging Profile communication profile after you create a duplicate user.

Before you begin

You require permission to copy the user details.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select the user account that you must duplicate.
4. Click **Duplicate**.

5. On the User Profile Duplicate page, enter the appropriate information.
6. Perform one of the following:
    - To save the changes, click **Commit**.
    - To save the changes and stay on the same page, click **Commit & Continue**.

Removing user accounts

About this task

When you remove a user, the system marks the user as deleted and saves the user in a list of deleted users. The system removes the roles associated with the user. However, the contacts, addresses, and communication profiles of the user still exist in the database. You can permanently remove the deleted users from the database.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select one or more users from the table, and click **Delete**.
4. On the User Delete Confirmation page, click **Delete**.

    ✱ **Note:**

    You cannot delete users:

    - With the login name *admin* from the User Management page.
    - Synchronized from LDAP.

Related links

Removing the deleted users from the database on page 182

Removing the deleted users from the database

Using this procedure, you can permanently delete a user from the database.

Before you begin

Permission to delete the selected user.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **More Actions** > **Show Deleted Users**.
4. On the Deleted Users page, select the users to delete, and click **Delete**.

5. On the User Delete Confirmation page, click **Delete**.

Related links

Removing user accounts on page 182

Editing users in bulk

About this task

On the System Manager web console, you can change the identity and communication profile data of users in bulk.

Note:

With **Bulk Edit Users**, you can select multiple users and create or update the communication profile data for the users. However, you cannot delete communication profiles.

While performing bulk edit operation, you do not validate the details of the users because bulk operation impacts all users.

You can schedule the bulk edit job to run at a later time.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. Select one or more users and click **More Actions** > **Bulk Edit Users**.
4. On the User Bulk Editor page, in the **Basic** and **Communication Profile** tabs, change the fields as appropriate.

   When you provide the communication profile password during the bulk edit of users, the system overwrites the existing communication profile password of the user.
5. Click **Run Now** or **Schedule**.
6. To view the status of the bulk edit job, click **More Actions** > **Status of Bulk Edit Users Jobs**.

   For more information, see Viewing bulk user edit jobs.

Related links

User Bulk Editor field descriptions on page 185

Viewing bulk user edit jobs

Before you begin

Create a bulk user edit job and run the job.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. Click **More Actions** > **Status of Bulk Edit Users Jobs**.
4. On the Schedule Bulk Edit of Users page, select a bulk edit job and click **View**.

   The system displays job details on the Bulk Edit Job Details page.
5. To view any latest changes in job details, click **Refresh**.

Deleting the bulk user edit job

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. Click **More Actions** > **Status of Bulk Edit Users Jobs**.
4. On the Schedule Bulk Edit of Users page, select one or more bulk edit jobs and click **Delete**.
5. On the Filter Profile Delete Confirmation page, click **Delete**.

   The system deletes the bulk edit job.

Create new profile option

During add and edit profile operations, based on the selection of the **Create New Profile if it doesn't exist for the user** check box and the availability of the communication profile, System Manager provides the following:

Create New Profile if it doesn't exist for the user check box	Communication profile	Add operation	Edit operation
Selected	Exists	You cannot update the existing communication profile.	The profile remains unchanged.
Selected	Does not exist	The system creates the communication profile.	The profile remains unchanged.
Not selected	Exists	The communication profile that is already created remains unchanged.	The system updates the communication profile based on the changes you make.

Table continues…

Create New Profile if it doesn't exist for the user check box	Communication profile	Add operation	Edit operation
Not selected	Does not exist	No change because you have not selected the check box.	No change. You cannot update a communication profile that does not exist.

User Provisioning Rules and User Bulk Editor

You can edit the users in bulk from one of the following:

- On the User Provisioning Rules page, from the **User Provisioning Rule** link. For more information, see User Provisioning Rule field descriptions on page 545.
- On the User Bulk Editor page, from the **User Management** > **Manage Users** > **More Actions** > **Bulk Edit Users** link. For more information, see User Bulk Editor field description on page 185.

User Bulk Editor field descriptions

Basic

Note:

On the Basic tab, when you provide the value in a field, the system applies the same value for all selected users.

Name	Description
SIP Domain	The name of the configured SIP domain name. If **SIP Domain** is nonblank, create an Avaya SIP communication address for the user. The system changes the SIP domain for all selected users with the value that you provide in this field.
Presence/IM Domain	The name of the configured Presence domain name. If **Presence/IM Domain** is nonblank, create an Avaya Presence/IM communication address for the user. The system changes the Presence/IM Domain domain for all selected users with the value that you provide in this field.

Table continues…

Name	Description
Prefix for Avaya E164 Handle	The digits that the system must prefix to the telephone number or Avaya E.164 handle. The default is plus (+).
Communication Profile Password	The communication profile password. To change the password, click **Edit**.
Language Preference	The preferred written or spoken language of the user. For example, English.
Time Zone	The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.
Allow H.323 and SIP Endpoint Dual Registration	

Communication Profile: Session Manager Profile

✱ **Note:**

The system displays the following fields only if a communication profile of the user exists for the product.

Name	Description
Create New Profile if it doesn't exist for the user	An option to create the profile for the user if a profile does not already exist. The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data. For more information, see Create new profile option on page 184.

Name	Description
Primary Session Manager	The instance that you want to use as the home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura® network. You must select the primary Session Manager server.
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. A selection is optional.

Table continues…

Name	Description
Survivability Server	For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile when the local connectivity to Session Manager instances in Avaya is lost. If you select a Branch Session Manager , and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional. **Note:** If a termination or origination application sequence contains a Communication Manager application, the Communication Manager instance associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.
Block New Registration When Maximum Registrations Active	If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint. **Note:** **Block New Registration When Maximum Registrations Active** is available only when you select the **Create New Profile if it doesn't exist for the user** check box while creating the user profile.
Origination Application Sequence	The application sequence that the system will invoke when routing the calls from this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application,

Table continues…

Name	Description
	Communication Manager must be the same in both the sequences.
Termination Application Sequence	The application sequence that will be invoked when the system routes the calls to this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Home Location	The home location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any of the location. You must specify a value.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.

Communication Profile tab: Engagement Development Platform Profile

Name	Description
Create New Profile if it doesn't exist for the user	An option to create the profile for the user if a profile does not already exist. The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data. For more information, see Create new profile option on page 184.

Name	Description
Service Profile	The profile that you assign to the user. The user can gain access to the service contained in the profile.

Communication Profile: CM Endpoint Profile

Name	Description
Create New Profile if it doesn't exist for the user	An option to create the profile for the user if a profile does not already exist.

Name	Description
	The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data. For more information, see Create new profile option on page 184.

By default, the system displays only **Profile Type**, **Template**, **Security Code**, and **Preferred Handle** fields. The system displays the remaining fields only when you select the **Create New Profile if it doesn't exist for the user** check box while creating the communication profile.

Field	Description
Use Next Available Extension	Select the check box to instruct the system to create a new extension for the user. ✱ **Note:** For LDAP synchronization, the value in the **Use Phone Number last ..... digits for Extension** field takes priority.
Template	The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add. You must select the template.
Security Code	The security code for authorized access to the endpoint.
Preferred Handle	Avaya SIP or Avaya E.164 handle that is administered for the user. The field is optional. By default, the field is blank.
Password	The password to gain access to the endpoint. The system displays the field if you select Agent in the **Profile Type** field.
Allow H.323 and SIP Endpoint Dual Registration	The option to register both an H.323 endpoint and a SIP endpoint together at the same time to the same extension.

Communication Profile: CS 1000 Endpoint Profile

The communication profile is available only for creating a user profile.

Name	Description
Create New Profile if it doesn't exist for the user	An option to create the profile for the user if a profile does not already exist. The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data.

Name	Description
	For more information, see Create new profile option on page 184.

Name	Description
System	The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.
Target	The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template.
Template	The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template.
Include in Corporate Directory	The option to add this profile to the CS 1000 Corporate Directory feature.
Delete Endpoint on Unassign of Endpoint from User	An option to specify whether to delete the endpoint from the CS 1000 system when you unassign the endpoint from the user.

Communication Profile: Messaging Profile

Name	Description
Create New Profile if it doesn't exist for the user	An option to create the profile for the user if a profile does not already exist. The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data. For more information, see Create new profile option on page 184.

By default, the system displays only **Template** and **Password** fields. The system displays the remaining fields only when you select the **Create New Profile if it doesn't exist for the user** check box while creating the communication profile.

Name	Description
System	The messaging system on which you add the subscriber. You must select the system.
Mailbox Number	The mailbox number of the subscriber. The options are: • Use CM Extension: Use this option only if the Communication Manager profile and Session Manager profile are specified.

Table continues…

Name	Description
	• Use Next Available Subscriber: Use this option if the system must use the next mailbox number to associate with this profile.
Template	The system-defined or user-defined template that you associate with the subscriber.
Password	The password for logging in to the mailbox. You must provide the password.
Delete Subscriber on Unassign of Subscriber from User or on Delete User	The option to specify whether 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.

Communication Profile: CallPilot Messaging Profile

The communication profile is available only for creating a user profile.

Name	Description
Create New Profile if it doesn't exist for the user	An option to create the profile for the user if a profile does not already exist. The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data. For more information, see Create new profile option on page 184.

Field	Description
System	The CallPilot system of the messaging profile. The selection is mandatory required.
Target	The field that maps to the CallPilot **Location** field. CallPilot Manager provides the **Target** field. You must select the target.
Template	The mailbox template that you use. Select a template from the drop down list. The element manager maintains all the mailbox templates. You must select the template.

Communication Profile tab: Presence Profile

Name	Description
Create New Profile if it doesn't exist for the user	An option to create the profile for the user if a profile does not already exist. The system displays the check box only when you select the communication profile. If the

Name	Description
	communication profile already exists, the system does not make any changes to the profile data. For more information, see Create new profile option on page 184.

Name	Description
System	The Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile: • Aggregate presence • Archive instant messages if the Instant Messages option is enabled
SIP Entity	The option to route the SIP-based messages through the Presence Services This system selects the SIP entity only if you select a Presence Services instance in the **System** field. **SIP Entity** is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.
IM Gateway	The IP address of the IM gateway.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with the AES Collector. The options are: • **System Default** • **Off** • **On** The default is **System Default**. You can change the default value. You do not require to configure AES Collector in the Presence Services server.

Communication Profile: IP Office Profile

Name	Description
Create New Profile if it doesn't exist for the user	An option to create the profile for the user if a profile does not already exist. The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data. For more information, see Create new profile option on page 184.

By default, the system displays only **Extension**, **Template**, and **Set Type** fields. The system displays the remaining fields only when you select the **Create New Profile if it doesn't exist for the user** check box for creating the communication profile.

Field	Description
System	The list of IP Office device names from which you can select the IP Office device that you associate with the user. You must select the template.
Extension	The extension of the endpoint to which you associate the profile. The options are: • Use CM Extension: Use this option only if Communication Manager profile is specified. • Use Next Available Extension: Use this option if the system must use the next extension to associate with this profile.
Template	A list of user templates from which you can select a template to set the user configurations.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the system automatically populates the set type value.

Communication Profile: Conferencing Profile

The communication profile is available only for creating a user profile.

Name	Description
Create New Profile if it doesn't exist for the user	An option to create the profile for the user if a profile does not already exist. The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data. For more information, see Create new profile option on page 184.

Name	Description
Template	The template that you use to set the user configurations.
Location	The location that Conferencing uses when the IP address of the calling phone does not match the IP address pattern of any location. The field is used to support the mobility of the user.
Select Auto-generated Code Length	The number of digits in the security code that the system generates.

Table continues…

Name	Description
Auto Generate Participant and Moderator Security Codes	The option to instruct the system to generate the security codes for the participant and moderator.

Button	Description
Run Now	Runs the bulk user edit job immediately.
Schedule	Schedules the bulk user edit job.
Cancel	Cancels the edit operation and returns to the User Management page.

Related links

Create new profile option on page 184

Filtering users

About this task

You can apply filter to the following user information:

- Last Name
- First Name
- Display Name
- Login Name
- SIP Handle

You can apply one or more filters to view users that match the filter criteria.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **Filter: Enable**.

   The system displays the **Filter: Enable** button at the upper-right corner of the table that displays users.
4. Enter the information for one or more of the following filter criteria:
   - To filter users by the last name, in the **Last Name** column, enter the last name of the user.
   - To filter users by the first name, in the **First Name** column, enter the name of the user.

     To filter names that begin with a specific letter, enter the letter in the field. You can enter a string of letters to filter the names that begin with the string.
   - To filter users by the login name, in the **Login Name** column, enter the login name.

     To filter the login names that begin with a specific letter, enter the letter in the field. You can enter a string of letters to filter login names that begin with the string.

- To filter users by the SIP handle, in the **SIP Handle** column, enter the SIP handle of the user.

5. **(Optional)** To hide the column filters, click **Disable**.

   This action does not clear any filter criteria that you had set.
6. Click **Apply**.

   The table displays the users that match the filter criteria.
7. To clear the filter criteria, click **Clear**.

Searching for users

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **Advanced Search** at the upper-right corner of the page.
4. In the Criteria section, do the following:
   a. In the first field, select the search criterion.
   b. In the second field, select the operator.
   c. In the third field, enter the search value.
5. To add another search criterion, click plus (**+**) and repeat Step 4a through Step 4c.

   To delete a search criterion, you must click minus (-). The system displays **-** when more than one search criterion is available.
6. Click **Search**.

   The **Users** table lists the users that match the search criteria.

Assigning roles to a user

To provide access to resources, you must assign roles to users. Use this procedure to assign an admin role to an end user. You can assign up to 20 roles per user.

You can also assign roles to users by using the Roles page, on the System Manager web console.

During the tenant administration, the **Membership** tab is unavailable for the tenant administrator.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.

3. On the User Management page, perform one of the following:
   - To assign roles while setting up a new user account, click **New**.
   - To assign roles to an existing user, select the user and click **Edit** or **View** > **Edit**.
4. On the User Profile Edit or New User Profile page, click the Membership tab.
5. Click **Assign Roles**.
6. In the Assign Roles section, select the roles.
7. To assign the roles to the selected user, click **Select**.
8. On the User Profile Edit or New User Profile page, click **Commit**.

   Note:

   - For a new user, if you assign a role other than the End-User role, the system prompts for the password.
   - For an existing user, the system resets the password to match the login name of the user when you:
     - Change the login name.
     - Assign a role other than End-User role and you do not provide a new password.

     When the user logs in, the system prompts the user to change the password on the next login.

Assigning roles to multiple users

To provide access to resources, you must assign roles to the user accounts. Use this procedure to assign admin role to an end user.

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**.

During the tenant administration, the **Membership** tab is unavailable for the tenant administrator.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select the users and click **More Actions** > **Assign Roles**.
4. On the Assign Roles page, select the roles from the **Available Roles** section.
5. Click **Commit** to assign the roles to the selected users.

Removing roles from a user

Before you begin

You must have permissions to remove the roles for the user.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
    - To remove a role in the edit mode, select a user and click **Edit**.
    - To remove a role in the view mode, select a user and click **View** > **Edit** on the View User Profile page.
4. On the User Profile Edit page, click the **Membership** tab.
5. Select the roles you want to remove and click **UnAssign Roles**.

    You can also assign roles to users using the Roles functionality in System Manager. To access Roles, on the System Manager console, click **Groups & Roles** > **Roles**
6. Click **Commit** to save the changes.

    Note:

    You can also assign roles to users using the Roles functionality in System Manager. To access Roles, on the System Manager console, click **Groups & Roles** > **Roles**.
7. Perform one of the following:
    - To save the changes, click **Commit**.
    - To save the changes and stay on the same page, click **Commit & Continue**.

Assigning groups to a user

You can also assign groups to users using the groups functionality in System Manager. To gain access to **Groups**, on System Manager web console, click **Groups & Roles** > **Groups**.

During the tenant administration, the **Membership** tab is unavailable for the tenant administrator.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
    - To assign groups while setting up a new user account, click **New**.

- To assign groups to an existing user, select the user and click **Edit** or **View** > **Edit**.

4. On the User Profile Edit page or the New User Profile page, click the **Membership** tab.
5. In the Group Membership section, click **Add To Group**.
6. On the Assign Groups page, select the groups from the **Available Groups** section.
7. Click **Select** to assign the groups to the user.
8. Perform one of the following:
    - To save the changes, click **Commit**.
    - To save the changes and stay on the same page, click **Commit & Continue**.

Assigning groups to multiple users

You can also assign groups to users using the groups functionality in System Manager. To access **Groups**, on System Manager web console, click **Groups & Roles** > **Groups**.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select the users and click **More Actions** > **Add To Group**.
4. On the Assign Groups page, select the groups from the **Available Groups** section.
5. Click **Commit** to assign groups to the selected users.

Removing a user from groups

You can also assign groups to users using the groups functionality in System Manager. To access **Groups**, on System Manager web console, click **Groups & Roles** > **Groups**.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
    - To remove a group in the edit mode, select the user and click **Edit**.
    - To remove a group in the view mode, select the user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Membership** tab.
5. In the Group Membership section, select the groups from which you want to remove the user and click **Remove From Group**.
6. Click **Commit** to save the changes.

Viewing the deleted users

When you remove a user from the User Management page using the **Delete** option, the system removes the user temporarily and stores the user in the **Deleted Users** table. To view the temporarily deleted users, use the **Show Deleted Users** option.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **More Actions** > **Show Deleted Users**.

   On the Deleted Users page, the system displays the temporarily deleted users in the Deleted Users table.

Restoring a deleted user

You can use this functionality to restore a user that you deleted using the **Delete** option on the User Management page.

Before you begin

You require permission to restore the selected user that is already deleted.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **More Actions** > **Show Deleted Users**.
4. On the Deleted Users page, select the user you want to restore, and click **Restore**.
5. On the User Restore Confirmation page, click **Restore**.
6. Click **Commit**.

   Note:

   For a restored user, if you assign a role other than End-User, the system prompts for a password.

Assigning users to roles

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.

3. From the list of roles, click the name of the role.
4. On the **Assigned Users** tab, click **Select Users**.

   The system displays the list of users.
5. Select the users and click **Commit**.

Unassigning users from role

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, click the Assigned Users tab.
5. Click **Selected Users**.
6. On the Assigned Users page, clear the check box of the user whom you want to unassign.
7. Click **Commit**.

Managing addresses

Adding an address of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To add an address while setting up a new user account, click **New** > **Identity** > **Address** > **New**.
   - To add a new address for an existing user, select the user and click **Edit** > **Identity** > **Address** > **New**.
   - To add a new address for an existing user, select the user and click **View** > **Edit** > **Identity** > **Address** > **New**.
4. On the Add Address page, enter the address details.

   You can select from the list of shared address.
5. Click **Add** to add the address.
6. Perform one of the following:
   - To save the changes, click **Commit**.

- To save the changes and stay on the same page, click **Commit & Continue**.

Related links

Add Address field descriptions on page 202

Modifying an address

About this task

You can use this functionality to modify the address of a user.

Note:

You cannot modify a shared address using this feature.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
    - Select a user, and click **Edit** > **Identity** > **Address**.
    - Select a user, and click **View** > **Edit** > **Identity** > **Address**.
4. In the **Address** area, select the mailing address you want to modify and click **Edit**.

    You cannot modify a shared address using this feature.
5. On the Edit Address page, modify the information.
6. Click **Add**.
7. Click **Commit**.

Deleting an address

About this task

You can use this functionality to delete a private mailing address from the database.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. 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 an address, then navigate to **Identity** > **Address**.
    - On the User Management page, select a user and click **Edit** > **Identity** > **Address**.
    - On the User Management page, select a user and click **View** > **Edit** > **Identity** > **Address**.
4. Select the address you want to delete and click **Delete**.

If the address you require to delete is a shared address, the system removes the address from the address list of user, but not from the database

5. Perform one of the following:
    - To save the changes, click **Commit**.
    - To save the changes and stay on the same page, click **Commit & Continue**.

Assigning a shared address to the user

About this task

You can use the functionality to choose a shared address for a user from common addresses. You can assign and unassign a shared address.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following:
    - To assign shared addresses to a new user while creating the user, click **New**.
    - To assign shared addresses to an existing user, select the user, and click **Edit** or **View** > **Edit**.
4. On the New User Profile page or the User Profile Edit page, click **Identity** > **Address** > **Choose Shared Address**.
5. On the Choose Address page, select one or more shared addresses.

    For a new user, enter valid information in all mandatory fields on all tabs of the New User Profile page before you click **Commit**. If you enter invalid information, the system displays an error message.
6. Click **Select**.
7. Perform one of the following:
    - To save the changes, click **Commit**.
    - To save the changes and stay on the same page for making further modifications, click **Commit & Continue**.

Related links

Choose Address field descriptions on page 204

Add Address field descriptions

Name	Description
Address Name	The unique label that identifies the mailing address.

Table continues…

Name	Description
Address Type	The mailing address type such as home or office address.
Building	The name of the building.
Room	The number or name of the room.
Street	The name of the street.
City	The name of the city or town.
State or Province	The full name of the province.
Postal Code	The postal code or zip code used by postal services to route mail to a destination. For the United States, specify the Zip code.
Country	The name of the country.

Phone Details section

Name	Description
Business Phone	The business phone number of the user.
Other Business Phone	The secondary or alternate business phone number if applicable.
Home Phone	The residential phone number of the user.
Other Home Phone	The secondary or alternate residential phone number if applicable.
Mobile Phone	The mobile number of the user.
Other Mobile Phone	The secondary or alternate mobile number of the user if applicable.
Fax	The telephone number for direct reception of faxes.
Pager	The number used to make calls to the pager of the user.
Other Pager	The secondary or alternate number used to make calls to the pager of the user.

Button	Description
Add	Adds the mailing address of the user.
Cancel	Cancels the add address operation.

Related links

Modifying a shared address on page 533

Adding a shared address on page 532

Choose Address field descriptions

Name	Description
Name	The unique label that identifies the address.
Address Type	The mailing address type such as home or office address.
Street	The name of the street.
City	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. In the United States, this is Zip code.
Province	The full name of the province.
Country	The name of the country.

Button	Description
Select	Adds the selected mailing address as the shared contact for the user account.
Cancel	Cancels the choose address operation.

Managing communication profiles

Communication profiles

You can provide communication profiles to associate elements with users. Communication profiles supports communication interactions established through Avaya Communication Services. Communication profiles can be CM Endpoint, Messaging, Session Manager, CS 1000, CallPilot Messaging, IP Office, Presence, Engagement Development Platform, or Conferencing profile.

You can provide communication profiles in User Management through Communication Profile Extension Pack (EP). You can use a communication profile to represent a subscription of the user to a communication subsystem and the specific configuration needs for the user. A communication subsystem is a service or infrastructure that manages the establishment and controls or routes the communication interactions.

System Manager supports a maximum of five communication profile sets for a user. You can add a maximum of three CM Endpoint profiles and one Messaging profile per user, and remaining two communication profile sets can contain other profiles.

Adding a communication profile for the user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.

3. On the User Management page, perform one of the following steps:
    - To create a new user account, click **New**.
    - To add a communication profile to an existing user, select the user and click **Edit**.
4. On the New User Profile or the User Profile Edit page, click the **Communication Profile** tab.
5. In the communication profile section, click **New**.
6. In the **Name** field, enter the name of the new communication profile.
7. To mark the profile as default, select the **Default** check box.
8. Click **Done**.
9. Click **Commit**.

Related links

New User Profile field descriptions on page 257

Deleting the communication profile of a user

About this task

You cannot delete default communication profiles.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
    - Select a user and click **Edit**.
    - Select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **Communication Profile** section, click a profile.
6. Click **Delete**.
7. Click **Commit**.

Result

When you delete a communication profile, System Manager deletes all the communication addresses associated with the communication profile.

Creating a new communication address for a communication profile

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.

3. On the User Management page, perform one of the following steps:
   - To create a new user account, click **New**.
   - To add a communication profile address to an existing user, select the user and click **Edit**.
4. On the New User Profile or the User Profile Edit page, click the **Communication Profile** tab.
5. In the Communication Profile section, click a communication profile.
6. In the Communication Address section, click **New**.
7. In the **Type** field, enter a communication protocol.
8. In the **Fully Qualified Address** field, enter a contact address in the format supported by the value that you selected in the **Type** field. A contact address can be an e-mail ID, instant messenger ID, or the SIP address of a SIP-enabled device.
9. Enter the domain name from the field next to **Fully Qualified Address** field.
10. Click **Add**.
11. Click **Commit**.

Related links

User Profile Edit field descriptions on page 277
New User Profile field descriptions on page 257

Modifying the communication address

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - Select a user and click **Edit**.
   - Select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **Communication Profile** section, select a profile.
6. In the **Communication Address** section, select a communication address.
7. Click **Edit**.
8. Modify the information in the respective fields.
9. Click **Add**.
10. Click **Commit**.

Related links

User Profile Edit field descriptions on page 277
New User Profile field descriptions on page 257

Deleting a communication address from a communication profile

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following:
   - Select a user and click **Edit**.
   - Select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Communication Profile section, click a communication profile.
6. In the Communication Address section, select a communication address from the table.
7. Click **Delete**.
8. Click **Commit**.

Related links

User Profile Edit field descriptions on page 277
New User Profile field descriptions on page 257

Session Manager communication profile administration

In the Session Manager Communication Profile section, you can associate 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 is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura® network.

All communication addresses of type SIP for the communication profile are associated with the Avaya Aura® network. If you select a secondary Session Manager instance, Session Manager provides continued service to SIP devices associated with this communication profile when the primary Session Manager is unavailable.

You can configure the system to invoke application sequences when routing calls from (origination application sequence) or to (termination application sequence) the currently displayed user.

You can specify a conference factory set for users for improved voice, video and text conferencing.

For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile that is used when local connectivity to Session Manager instances in the Aura core is lost. If you select a Branch Session Manager, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues locally to the Communication Manager remote survivable server resident with the Branch Session Manager.

When this user calls numbers that are not associated with an administered user, the system applies dial-plan rules to complete the call based on this home location if the IP address of the SIP device used to make the call is unassigned to a location.

Related links

Multi Device Access on page 208

New User Profile field descriptions on page 257

Multi Device Access

With the Multi Device Access feature, a SIP user can register multiple SIP endpoints with the same extension. You can specify the maximum number of SIP endpoints that can simultaneously register and receive calls in the **Max. Simultaneous Devices** field of the Session Manager communication profile section on the User Profile page. The default is 1. For more information, see *Avaya Aura® Multi Device Access White Paper* on the Avaya Support site at http://support.avaya.com/.

If the number of registration requests exceed the administered limit, and if the **Block New Registration When Maximum Registrations Active** field is:

- Cleared, the system accepts the new registration and unregisters the endpoint with the oldest registration. If the endpoint with the oldest registration is active on a call, the system waits for the call to complete before unregistering.
- Selected, the system denies any new registrations and sends the 403 Forbidden response with an appropriate warning header to the registering device.

The system routes incoming INVITE requests or call attempts to all the registered devices for a given user simultaneously. When the caller answers the call, the system cancels the INVITE request to the other devices.

The system routes an incoming CANCEL request to all the registered devices if the caller hangs up before the call is answered.

Presence communication profile administration

You can configure attributes for the Presence communication profile when you create a user or edit the existing user. You can also configure the Presence-related attributes by using the user provisioning rule.

In System Manager, you must configure the Avaya Aura® users and assign typically some or all of the following attributes:

- Avaya E.164 communication address
- Avaya SIP communication address
- CM Endpoint profile
- Session Manager profile

You can configure the attributes from **User Management** > **Manage Users**.

You can create Presence profiles only for the default communication profile.

Note:

To create the Presence communication profile, you must select **Avaya Presence/IM** and provide the communication address.

CM Endpoint profile administration

CM Endpoint and Messaging profiles of a user

With User Profile Management, you can create the following types of communication profiles for a user:

- CM Endpoint Profile, to create an association between an endpoint and a user
- Messaging Profile, to create an association between a subscriber mailbox and a user

You can add, view, modify, and delete endpoint and messaging profiles. You can go to Endpoint or Subscriber Management pages to modify any of the endpoint or subscriber fields that are not available through User Profile Management.

Login name of endpoint 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, CM Endpoint and Messaging. This user name appears in the User column in the Endpoint List or Subscriber List.

For endpoints, the **Localized Display Name** and **Endpoint Display Name** fields in the Identity section of the User Profile Management user profile map to the **Name** and **Localized Display Name** fields of CM Endpoint. 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 User Profile Management 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 User Profile Management 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 CM Endpoint and Messaging profiles

You can create one default or primary Communication Profile for a user. To this default profile, you can add one CM Endpoint and one Messaging profile. In addition, you can add two more CM Endpoint profiles. You can add a maximum of three CM Endpoint profiles and one Messaging profile per user.

Adding a CM Endpoint profile for a user

Before you begin

Add Communication Manager by using Manage Elements or Discovery from **Inventory**.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - If you are creating a CM Endpoint profile for a new user profile, click **New**.
   - If you are creating a CM Endpoint profile for an existing user, select the user and click **Edit**.
4. Click the **Communication Profile** tab.

5. In the CM Endpoint Profile section, select the check box next to the **CM Endpoint Profile** label.
6. In the CM Endpoint Profile section, enter the relevant information.

   Note:

   To delete the endpoint from the communication management device after removing the association between the endpoint and the user, select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box.
7. Perform one of the following:
   - To save the changes, click **Commit**.
   - To save the changes and stay on the same page, click **Commit & Continue**.

   From User Management, you can create or add endpoints. After you select the Communication Manager in which you want to add an endpoint, the system allows you to complete the fields for creating a new endpoint.

   The **Preferred Handle** field specifies numeric only handles, SIP or non SIP, that are administered for a user. If the SIP entity is of Communication Manager type, Session Manager uses the **Preferred Handle** field in the CM Endpoint profile. By default, for a SIP station, Communication Manager uses the extension number as the phone number entry on an OPS station-mapping table. If your enterprise dial plan has SIP handles that are different from the Communication Manager extension, then use the **Preferred Handle** field to change the phone number entry on the OPS station-mapping table on the Communication Manager.

   To modify the phone number entry, the Communication Address in System Manager should have a SIP handle. In the CM Endpoint Communication Profile, set the **Preferred Handle** field to the SIP handle format. After you click **Commit**, System Manager sets the **Phone Number** field in the OPS station-mapping table on Communication Manager to the SIP handle format. If you do not need this feature then set the **Preferred Handle** value to **None**.

Related links

New User Profile field descriptions on page 257

Viewing a station profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.
4. Click the **Communication Profile** tab.

Modifying a CM Endpoint profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.

3. On the User Management page, select a user and perform one of the following steps:
    - Click **Edit**.
    - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the CM Endpoint Profile section, modify the relevant information in the fields.
6. To save the changes to the database, click **Commit**.

    To cancel the action and return to the previous page, click **Cancel**.

Related links

New User Profile field descriptions on page 257

Using the automatically generated call routes for SIP routing

About this task

Based on the primary or secondary Session Manager that you have specified in the **Session Manager Communication Profile**, the system automatically determines a route pattern.

Before you begin

In the Communication Manager instance that you have associated with System Manager, make sure that:

1. On the Route Pattern page, you have specified the primary Session Manager.
2. You have selected an SIP endpoint.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. Click **Communication Profile**.
4. In **Session Manager Profile** > **SIP Registration** > **Primary Session Manager**, click a primary session manager.

    Note:

    You must add a primary Session Manager.

    For more information, see *Administering Avaya Aura® Communication Manager*.
5. In **CM Endpoint Profile**, do the following:
    a. In the **Set Type** field, enter the details of an SIP set type.
    b. Select the **Calculate Route Pattern** check box.

Result

For the user that you specified and for the Session Manager that you set as a primary Session Manager, the system automatically generates route patterns.

Removing association between an CM Endpoint and a user

Before you begin

Ensure that you have not selected the **Delete Endpoint on Unassign of Endpoint from User or Delete User** check box while associating a station with a user.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
    - Click **Edit**.
    - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **CM Endpoint Profile** section, clear the check box next to the **CM Endpoint Profile** label.
6. Click **Commit**.

Result

The system removes the association between the endpoint and the user. The endpoint is still provisioned on the communication management device.

Deleting a CM Endpoint profile of a user

Before you begin

Select the **Delete Endpoint on Unassign of Endpoint from User or Delete User** check box while associating a endpoint to a user.

About this task

The delete functionality removes the association between the endpoint and the user, and deletes the endpoint from the communication management device.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
    - Click **Edit**.
    - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **CM Endpoint Profile** section, clear the check box next to the **CM Endpoint Profile** label.
6. Click **Commit**.

Note:

You can delete only those endpoints that are associated with a user through User Management. You can delete nonuser associated endpoints through Endpoint management.

Related links

New User Profile field descriptions on page 257

Messaging profile administration

Adding a messaging profile for a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. 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**.
4. Click the **Communication Profile** tab.
5. In the Messaging Profile section, select the check box next to the **Messaging Profile** label.
6. In the Messaging Profile section, complete the relevant fields.

   Note:

   To delete the subscriber mailbox from the communication management device after removing the association between the subscriber and the user, select the **Delete Messaging on Unassign of Subscriber from User or Delete User** check box.
7. Click **Commit** or **Commit & Continue** to add the messaging profile, or click **Cancel** to return to return to the previous page.

   The field names that are marked with an asterisk (*) are mandatory fields. You must enter valid information in these fields to create the CM Endpoint profile.

   Note:

   You must add the messaging devices through Runtime Topology System (RTS) before you add a messaging profile for a user. After you create the user-subscriber association, the user name appears in the **User** column in the subscriber list.

Related links

New User Profile field descriptions on page 257

Modifying a messaging profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.

2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
    - Click **Edit**.
    - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Messaging Profile section, modify the relevant information in the fields.
6. Perform one of the following:
    - To save the changes to the database, click **Commit**.
    - To save the changes to the database and remain on the same page, click **Commit & Continue**.
    - To cancel the action and return to the previous page, click **Cancel**.

Related links

New User Profile field descriptions on page 257

Viewing a messaging profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.
4. Click the **Communication Profile** tab.

Result

The Messaging Profile section displays the messaging profile information of the user.

Related links

New User Profile field descriptions on page 257

Removing association between a subscriber mailbox and a user

Before you begin

The **Delete Subscriber on Unassign of Subscriber from User or Delete User** check box is clear while associating a mailbox with a user.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
    - Click **Edit**.
    - Click **View** > **Edit**.

4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Messaging Profile tab, clear the check box next to the **Messaging Profile** label.
6. Click **Commit**.

Result

The system removes the association between the subscriber mailbox and the user. The subscriber mailbox is still provisioned on the communication management device.

Deleting a subscriber mailbox

Before you begin

You have selected the **Delete Subscriber on Unassign of Subscriber from User or on Delete User** check box while associating a subscriber mailbox to a user.

About this task

This functionality deletes the subscriber mailbox from the messaging device after removing the association between the subscriber mailbox and the user.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Messaging Profile section, clear the check box next to the **Messaging Profile** label.
6. Click **Commit**.

   Note:

   You can delete only those subscribers that are associated with a user through User Management. You can delete non-user associated subscriber mailboxes only through Subscriber Management.

CS 1000 and CallPilot profile administration

CS 1000 and CallPilot profile administration

With User Management, you can create the following types of communication profiles for a user:

- CS 1000 Endpoint Profile. To create an association between an endpoint and a user.
- CallPilot Messaging Profile. To create an association between a subscriber mailbox and a user.

Note:

You cannot assign the mailbox number in the CallPilot communication profile by using the user provisioning rule. You must add the mailbox number for the CallPilot communication profile.

To modify an endpoint or subscriber field that is not available through User Management, navigate to the Endpoint or Subscriber Management pages and modify the information. For information, see Redirecting the CS 1000 or CallPilot user to Element Manager.

Related links

Redirecting the CS 1000 or CallPilot user to Element Manager on page 216

Redirecting the CS 1000 or CallPilot user to Element Manager

Before you begin

A user must exist with at least one communication profile. To create a user, navigate to **User Management** > **New**.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. Select **CS 1000 Endpoint Profile** or **CallPilot Messaging Profile** that you must update and click **Update**.

   The system opens the user profile in the element manager that you select.

   Note:

   The system discards all unsaved changes that you make to the current user including the changes to communication profiles.
6. Enter the relevant information and click **Save**.

   The system displays the User Management page.

Adding a CallPilot profile for a user

Before you begin

A user must exist. To create a user, navigate to **User Management** > **New**.

About this task

For a communication profile, you can provide a maximum of one CallPilot mailbox. To add additional mailboxes for a user, you must add another communication profile.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a profile for a new user, click **New**.
   - To create a profile for an existing user, select the user and click **Edit**.
4. On the New User Profile page, click the **Communication Profile** tab.
5. In the CallPilot Messaging Profile section, select the check box and complete the following fields:
   - In the **System** field, select a CallPilot system. The system displays a list of systems that are registered with the element registry.
   - In the **Target** field, select the location of CallPilot, if provisioned.
   - In the **Template** field, select a template that CallPilot Element Manager provisions.
   - In the **Mailbox Number** field, enter a mailbox number for CallPilot.

   Note:

   You must enter the mailbox number even if the value is same as Primary DN.
6. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Adding a CS 1000 profile for a user

Before you begin

A user must exist. To create a new user, navigate to **User Management** > **New**.

About this task

For a communication profile, you can provide a maximum of one CS 1000 phone. To add additional phones for a user, you must add another communication profile.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a profile for a new user profile, click **New**.
   - To create a profile for an existing user, select the user and click **Edit**.

4. On the New User Profile page, click the **Communication Profile** tab.
5. In the **CS1000 Endpoint Profile** section, select the check box and complete the following fields:
    a. In the **System** field, select a CS 1000 system.

       The system displays a list of systems that are registered with the element registry.

    b. Perform one of the following:
        - Click **Add new** and complete the following fields:
            a. In the **Target** field, select a CS 1000 customer number.
            b. In the **Template** field, select a template that CS 1000 Element Manager provides.
            c. In the **Primary DN** field, enter a preferred primary DN.

               Note:

               If you do not provide a primary DN, CS 1000 Element Manager automatically assigns a primary DN.

            d. In the **Terminal Number** field, enter a preferred TN.
        - Click **Link existing**, and in the **Existing TN** field, enter the terminal number from the list of existing numbers.

    c. Clear the **Include in Corporate Directory** check box to exclude the profile in the CS 1000 corporate directory.
    d. **(Optional)** Select **Delete Endpoint on Unassign of Endpoint from User** if you must delete the endpoint from CS 1000 when you remove the association between the endpoint and the user.
6. Perform one of the following:
    - To save the changes to the database, click **Commit**.
    - To save the changes to the database and remain on the same page, click **Commit & Continue**.
    - To cancel the action and return to the previous page, click **Cancel**.

Modifying a CS 1000 or CallPilot user profile

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
    - Click **Edit**.
    - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.

5. In the CS 1000 Endpoint Profile or CallPilot Messaging Profile section, enter the relevant information in the fields.
6. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Changing passwords of CS 1000 Presence users

Procedure

1. To log on to the System Manager personal agent console, enter `http://<SMGR server-name>/pa`.
2. Click **Change Password**.
3. Enter the old and new passwords, and then click **Save**.

   Presence Services recognizes the password change.

   Note:

   The system needs a synchronized password that is the same password as the password that Presence Services uses to update CS 1000.

IP Office profile administration

Adding an IP Office endpoint profile on a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a profile for a new user, click **New**.
   - To create a profile for an existing user, select the user and click **Edit**.
4. On the New User Profile page, click the **Communication Profile** tab.
5. Select the **IP Office Endpoint Profile** check box.
6. Complete the **IP Office Endpoint Profile** section.
7. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Note:

To assign an extension to the user, perform one of the following actions:

- Assign an available extension to the user, select the **Use Existing Extension** check box, and select an unassigned extension from the drop-down box.
- Or assign an available module-port to the user from the **Module-Port** drop-down box, and type the new extension. The module-port combination is valid only when you associate a digital or an analog extension type to the user.

To assign an extension to a user with other set types, perform one of the following actions:

- Type an appropriate extension.
- Select the **Use Existing Extension** check box to choose an existing extension.
- Select an unassigned extension from the drop-down field.

Related links

New User Profile field descriptions on page 257

Viewing an IP Office endpoint profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select the user whose profile you want to view.
4. Click **View**.
5. Click the **Communication Profile** tab.

   Click the **IP Office Endpoint** section to view the IP Office endpoint profile of the user you selected.

Related links

New User Profile field descriptions on page 257

Modifying an IP Office endpoint profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select the user whose profile you want to edit.
4. Click **Edit**.
5. Select the **Communication Profile** tab.
6. Edit the required fields in the **IP Office Endpoint Profile** section.

7. Perform one of the following:
    - To save the changes to the database, click **Commit**.
    - To save the changes to the database and remain on the same page, click **Commit & Continue**.
    - To cancel the action and return to the previous page, click **Cancel**.

    Note:

    To assign an extension to the user, perform one of the following actions:

    - Assign an available extension to the user, select the **Use Existing Extension** check box, and select an unassigned extension from the drop-down box.
    - Or assign an available module-port to the user from the **Module-Port** drop-down box, and type the new extension. The module-port combination is valid only when you associate a digital or an analog extension type to the user.

    To assign an extension to a user with other set types, perform one of the following actions:

    - Type an appropriate extension.
    - Select the **Use Existing Extension** check box to choose an existing extension.
    - Select an unassigned extension from the drop-down field.

Related links

New User Profile field descriptions on page 257

Removing the association between an IP Office endpoint profile and a user

About this task

You must add, edit, or delete the end point profile for a user with an IP Office Endpoint profile only when IP Office is active and connected to System Manager.

Note:

Do not perform the add, edit, or delete operations when IP Office is temporarily unreachable. However, in situations when IP Office is unused or corrupted, you must set the force_delete_user property to true in the `IPOffice.properties` file by using putty to delete IP Office Endpoint Profile from System Manager users.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user, and perform one of the following:
    - Click **Edit**.
    - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.

5. Clear the **IP Office Endpoint Profile** check box.
6. Click **Commit**.

Related links

Removing the association between an IP Office endpoint profile and a user from properties file on page 222

Removing the association between an IP Office endpoint profile and a user from properties file

About this task

Perform the procedure to remove between an IP Office endpoint profile and a user only when IP Office is unused or corrupted.

Procedure

1. Using putty navigate to the `/opt/Avaya/ABG/6.3.8/tools` folder.
2. Open the `IPOffice.properties` file and set the force_delete_user property to true.

   By default, the force_delete_user property is set to false to make sure that the user data on IP Office and System Manager are in synchronization.
3. Save the properties file.
4. To restart the JBoss service, at the prompt, type `service jboss restart`.

   Wait until the JBoss service starts.
5. On System Manager web console, click **Users** > **User Management** and delete the IP Office Endpoint Profile of the user that exist on the abandoned or corrupted IP Office.
6. Set the force_delete_user property to false and restart the JBoss service.

Related links

Removing the association between an IP Office endpoint profile and a user on page 221

Managing default contact list of the user

Adding a contact in the Default Contact list

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following:
   - To add a contact for a new user, click **New**.
   - To add a contact for an existing user, select a user and click **Edit**.
4. Click the **Contacts** tab.

5. In the **Default Contact List** section, enter a brief description of the contact list in the **Description** field.
6. In the **Associated Contacts** section, click **Add**.
7. On the Attach Contacts page, select one or more contacts and click **Select**.

   Note:

   In the Multi Tenancy environment, when the tenant administrator of a tenant creates or updates the user, the administrator can attach only the following contacts:

   - Private contacts of the user
   - Public contacts
   - Users who belong to that tenant

   The system displays the new contacts in the table in the **Associated Contacts** section.

Related links

Attach Contacts field descriptions on page 224

Modifying membership details of a contact in a contact list

About this task

Use this feature to set the speed dial and presence buddy information for the contacts in the Default Contact list.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the **Associated Contacts** section, select a contact and click **Edit**.
6. On the Edit Contact List Member page, in the **Contact Membership Details** section, change the required information in the fields.

   You can only change the information in the fields displayed in the **Contact Membership Details** section.
7. Click **Add**.
8. Click **Commit** to save the changes.

Related links

Edit Contact List Member field descriptions on page 226

Viewing membership details of a contact in the contact list

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.
4. On the User Profile View page, click the **Contacts** tab.
5. In the Associated Contacts section, click the last name link under the **Last Name** column.

Result

The View Contact List Member page displays the details of the selected contact.

Related links

View Contact List Member field descriptions on page 227

Deleting contacts from the default contact list

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. Select one or more contacts from the Associated Contacts section and click **Remove**.

Attach Contacts field descriptions

In the Multi Tenancy environment, when the tenant administrator of a tenant creates or updates the user, the administrator can attach only the following contacts:

- Private contacts of the user
- Public contacts
- Users who belong to that tenant

Field	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Scope	The categorization of the contact based on whether the contact is a user, public, or private contact.
Display/Login Name	The unique login name or display name of the contact.

Table continues…

Field	Description
Contact Address	The address of a private or public contact. No contact address is associated with a contact type user.
User Handles	The communication handles associated with the user. These handles are defined in the communication profile of a user.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays fields under selected columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.
Advanced Search	Displays fields that you can use to specify the search criteria to search for contacts.

Button	Description
Select	Adds the selected contact in the list of associated contacts.
Cancel	Cancels your selection and takes you to the Contacts tab.

The page displays the following fields when you click **Advanced Search** at the upper-right corner of the contact table.

Field	Description
Search On	The search options that must base on the **Contact** or **User**.
Criteria	The search criteria for searching the contacts. Displays the following three fields: • Field 1 - The list of criteria that you can use to search the contacts. You can search based on the first name, last name, or the address/handle of the contact. • Field 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. • Field 3 - The value for the search criterion.

Button	Description
+	Adds one more search criteria section.

Table continues…

Button	Description
-	Clears the last search criteria. This button is applicable only if there is more than one search criteria.

Edit Contact List Member field descriptions

Contact Membership Details

Field	Description
Label	The text description for classifying this contact.
Alternative Label	The text description for classifying this contact. The field is similar to **Label**, and is used to store label in an alternate language.
Description	The brief description about the contact.
Presence Buddy	An option to indicate whether to allow monitoring of the presence information of the contact.
Speed Dial	An option to indicate whether to allow speed dial for the contact.
Address/Handle	The fully qualified URI for interacting with the contact. This field is available only if you select the **Speed Dial** check box.
Speed Dial Entry	The reduced number that represents the speed dial number. This field is available only if you select the **Speed Dial** check box.

Contact Details

Field	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Middle Name	The middle name of the contact.
Description	The brief description about the contact.
Company	The name of the company to which the contact belongs.
Localized Display Name	The localized display name of a user. The name is usually the localized full name.
Endpoint Display Name	The endpoint display name of the contact.
Language Preference	The list of languages from which you set a language as the preferred language for the contact.
Update Time	The time when the contact information was last updated.
Source	The source of provisioning the contact.

Postal Address

Field	Description
Name	The name of the contact.
Address Type	The type of mailing address such as, home or office address.
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	The postal code of the locality of the city or town.
Province	The full name of the province of the contact.
Country	The name of the country of the contact.

Contact Address

Field	Description
Address	The address that you can use to communicate with the contact. The address can be a phone number, email address, or IM of the contact.
Type	The type of communication medium for interacting with the user.
Category	The categorization of the address based on the location.
Label	The description for classifying this contact.
Alternative Label	The description for classifying this contact. The field is similar to **Label**, and is used to store label in an alternate language.

Button	Description
Add	Saves the modified information in the database.

View Contact List Member field descriptions

Contact Membership Details

Name	Description
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. The **Alternative Label** field is similar to **Label**, but you use the field to store label in an alternate language.
Description	Displays a brief description about the contact.

Table continues…

Name	Description
Presence Buddy	Provides the option to indicate whether to allow monitoring of the presence information of the contact.
Speed Dial	Provides the option to indicate whether to allow speed dial for the contact.
Address/Handle	Displays a fully qualified URI for interacting with the contact. This field is available only if you select the **Speed Dial** check box.
Speed Dial Entry	Displays the reduced number that represents the speed dial number. This field is available only if you select the **Speed Dial** check box.

Contact Details

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Middle Name	Displays the middle name of the contact.
Description	Displays a brief description about the contact.
Company	Displays the name of contact's company
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Displays the endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.
Update Time	Displays the time when the contact information was last updated.
Source	Displays the source of provisioning the contact.

Postal Address

Name	Description
Name	Displays the name of the contact.
Address Type	Displays the mailing address type such as, home or office address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the postal code of the locality of the city or town.
Province	Displays the full name of the contact's province.
Country	Displays the name of the contact's country.

Contact Address

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, email address, or IM of the contact.
Type	Displays the type of communication medium for interacting with the user.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This field is similar to **Label**, but it is used to store label in an alternate language.

Managing private contacts of a user

Adding a private contact to a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To add a private contact while setting up a new user, click **New**.
   - To add a private contact to an existing user, select the user and click **Edit**.
4. Click the **Contacts** tab.
5. In the Private Contacts section, click **New**.
6. On the New Private Contact page, enter the last name, first name, middle name, description, company name, localized display name, endpoint display name, and language preference in the Contact Details section.

   Enter a valid information in the fields.
7. 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.
8. In the Contact Address section, click **New** to choose a contact address for the contact.
9. Click **Add** to add the private contact.
10. Perform one of the following:
    - To save the changes, click **Commit**.

- To save the changes and stay on the same page, click **Commit & Continue**.

Related links

New Private Contact field descriptions on page 235

Modifying details of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the **Private Contacts** area, select a contact.
6. Click **Edit**.
7. On the Edit Private Contact page, modify the information of the contact.
8. Click **Add** to save the modified information.

Related links

Edit Private Contact field descriptions on page 236

Viewing details of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.
4. On the User Profile View page, click the **Contacts** tab.
5. Click **Private Contacts**.
6. In the Private Contacts section, click the link displayed in the **Last Name** column for a contact.

   The View Private Contact page displays the details of the contact whose last name you have clicked.

Related links

View Private Contact field descriptions on page 238

Deleting private contacts of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.

4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select one or more contacts from the table displaying private contacts.
6. Click **Delete**.
7. On the **Contact Delete Confirmation** page, click **Delete**.

   The system displays the User Profile Edit page.
8. Perform one of the following:
   - To save the changes, click **Commit**.
   - To save the changes and stay on the same page, click **Commit & Continue**.

Adding a postal address of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - If you are adding a postal address of a private contact to a new user, click **New**.
   - If you are adding a postal address of a private contact to an existing user, select a user and click **Edit**.
4. Click the **Contacts** tab.
5. In the **Private Contacts** area, perform one of the following:
   - If you are adding a postal address for a new private contact, click **New**.
   - If you are adding a postal address for an existing private contact, select a private contact and click **Edit**.
6. On the New Private Contact or Edit Private Contact page, click **New** in the Postal Address section.
7. On the Add Address page, enter the required information in the respective fields.

   Enter valid information in these fields.
8. Click **Add** to create a new postal address for the private contact.

Related links

Add Address field descriptions on page 202

Modifying postal address of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.

3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select a contact and click **Edit**.
6. On the Edit Private Contact page, select an address from the **Postal Address** area.
7. Click **Edit**.
8. On the Edit Address page, modify the information in the respective fields.

   Enter valid information in the fields.
9. Click **Add**.
10. Perform one of the following:
    - To save the changes, click **Commit**.
    - To save the changes and stay on the same page, click **Commit & Continue**.

Related links

Edit Address field descriptions on page 240

Deleting postal addresses of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select a contact and click **Edit**.
6. On the Edit Private Contact page, select one or more addresses from the **Postal Address** area.
7. Click **Delete**.
8. Click **Add**.

Choosing a shared address for a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To choose a shared address for a private contact while creating a new user, click **New**.
   - To choose a shared address for a private contact of an existing user, select the user and click **Edit**.
4. Click the **Contacts** tab.

5. In the Private Contacts section, perform one of the following actions:
    - To add a new contact and add an address to the contact, click **New**.
    - To add an address to an existing contact, select the contact and click **Edit**.
6. On the New Private Contact or the Edit Private Contact page, click **Choose Shared Address** in the **Postal Address** area.
7. On the Choose Address page, select one or more shared addresses.
8. Click **Select**.
9. Click **Add** to add the selected addresses to the private contact.
10. Perform one of the following:
    - To save the changes, click **Commit**.
    - To save the changes and stay on the same page, click **Commit & Continue**.

Related links

Choose Address field descriptions on page 204

Adding a contact address for a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
    - To add a contact address of a private contact while creating a new user, click **New**.
    - To add a contact address of a private contact for an existing user, select the user and click **Edit**.
4. Click the **Contacts** tab.
5. In the Private Contacts section, perform one of the following steps:
    - To add a contact address for a new private contact, click **New**.
    - To add a contact address for an existing private contact, select the private contact from the list and click **Edit**.
6. On the New Private Contact or the Edit Private Contact page, click **New** in the **Contact Address** area.
7. On the Add Address page, enter the appropriate information in the respective fields.

    Enter a valid information in these fields.
8. Click **Add**.
9. Perform one of the following:
    - To save the changes, click **Commit**.

- To save the changes and stay on the same page, click **Commit & Continue**.

Related links

Add Address field descriptions on page 239

Modifying a contact address of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select a contact and click **Edit**.
6. On the Edit Private Contact page, select a contact address from the **Contact Address** area.
7. Click **Edit**.
8. On the Edit Address page, modify the information in the respective fields.

   Enter valid information in these fields.
9. Click **Add** to save the modified address.
10. On the Edit Private Contact page, click **Add**.

    The system displays the User Profile Edit page.
11. Perform one of the following:
    - To save the changes, click **Commit**.
    - To save the changes and stay on the same page, click **Commit & Continue**.

Related links

Edit Address field descriptions on page 240

Deleting contact addresses of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contact section, select a contact and click **Edit**.
6. On the Edit Private Contact page, select one or more addresses from the Contact Address section.
7. Click **Delete**.

8. Click **Commit**.

New Private Contact field descriptions

Contact Details

Name	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Middle Name	The middle name of the contact.
Description	A brief description about the contact.
Company	The name of contact's company.
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	The endpoint display name of the contact.
Language Preference	The list of languages from which you set one language as the preferred language for the contact.

Postal Address

Name	Description
Address Name	The unique label that identifies the address.
Address Type	The mailing address type such as, home or office address.
Building	The name of the building.
Room	The name or number of the room.
Street	The name of the street.
City	The name of the city or town of the contact.
State or Province	The full name of the state or province where the contact's office or home is located.
Postal Code	The postal code of the of the city or town where the contact's office or home is located.
Country	The name of the country where the contact's office or home is located.

Button	Description
Edit	Displays the **Edit Address** page where you can modify an existing postal address of the private contact.
New	Displays the **Add Address** page where you can add a new postal address of the private contact.
Delete	Deletes the selected postal address.

Table continues…

Button	Description
Choose Shared Address	Displays the **Choose Address** page where you can choose addresses of the private contact.

Contact Address

Name	Description
Address	The address that you can use to communicate with the contact. This can be a phone number, email address, or IM of the contact.
Type	The type of communication medium for interacting with the user.
Category	The 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 field is similar to **Label**, but it is used to store label in an alternate language.

Button	Description
Edit	Displays the **Edit Address** page. Use this page to edit a contact address of the private contact.
New	Displays the **Add Address** page. Use this page to add a contact address of the private contact.
Delete	Deletes the selected contact address.

Button	Description
Add	Creates a new contact. **Note:** Enter valid information in the mandatory fields to successfully create a new contact.

Edit Private Contact field descriptions

Contact Details

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Middle Name	Displays the middle name of the contact.
Description	Displays a brief description about the contact.
Company	Displays the name of contact's company

Table continues…

Name	Description
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Displays the endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.
Update Time	Displays the time when the contact information was last updated.
Source	Displays the source of provisioning the contact.

Postal Address

Name	Description
Name	Displays the unique label that identifies the address.
Address Type	Displays the mailing address type such as, home or office address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the postal code of the of the city or town where the contact's office or home is located.
Province	Displays the full name of the province where the contact's office or home is located.
Country	Displays the name of the country where the contact's office or home is located.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to modify an existing postal address of the private contact.
New	Opens the **Add Address** page. Use this page to add new postal address of the private contact.
Delete	Deletes the selected contact address.
Choose Shared Address	Opens the **Choose Address** page. Use this page to choose addresses of the private contact.

Contact Address

Name	Description
Address	Displays the 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	Displays the type of communication medium for interacting with the user.

Table continues…

Name	Description
Category	Displays the categorization of the address based on the location.
Label	Displays the text description for classifying this contact.
Alternative Label	Displays the text description for classifying this contact. This is similar to **Label**, but it is used to store label in an alternate language.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to edit a contact address of the private contact.
New	Opens the **Add Address** page. Use this page to add a contact address of the private contact.
Delete	Deletes the selected private contacts.

Button	Description
Add	Saves the modified information to the database.

View Private Contact field descriptions

Contact Details

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Middle Name	Displays the middle name of the contact.
Description	Displays a brief description about the contact.
Company	Displays the name of contact's company
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.
Endpoint Display Name	Displays the endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.
Update Time	Displays the time when the contact information was last updated.
Source	Displays the source of provisioning the contact.

Postal Address

Name	Description
Name	Displays the unique label that identifies the address.

Table continues…

Name	Description
Address Type	Displays the mailing address type such as, home or office address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the postal code of the of the city or town where the contact's office or home is located.
Province	Displays the full name of the contact's province.
Country	Displays the name of the contact's country.

Contact Address

Name	Description
Address	Displays the 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	Displays the type of communication medium used to interact with the user.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays 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
Done	Takes you to the previous page.

Add Address field descriptions

Use this page to add communication address of the contact.

Name	Description
Address	Displays the 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 select in the **Type** field.
Type	Displays the type of address. The types of addresses are: • **Phone**: This address type supports phone numbers.

Table continues…

Name	Description
	- **SIP**: This address type supports SIP-based communication. - **MSRTC**: This address type supports communication with a Microsoft RTC server. - **IBM Sametime**: This address type supports communication with IBM Sametime. Specify the address in the DN=IBMHandle format. - **XMPP**: This address type supports xmpp-based communication. - **SMTP**: This address type supports communication with the SMTP server.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays 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
Add	Adds the contact address of the public contact to the database.

Related links

Adding a contact address of a public contact on page 523

Edit Address field descriptions

Use this page to edit the details of a contact's communication address.

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, email address, SIP, or IM of the contact. The format of the address must conform to the type of address that you select in the **Type** field.
Type	Displays the type of address. The types of addresses are: - **Phone**: This address type supports phone numbers. - **SIP**: This address type supports SIP-based communication.

Table continues…

Name	Description
	• **MSRTC**: This address type supports communication with a Microsoft RTC server. • **IBM Sametime**: This address type supports communication with IBM Sametime. Specify the address in the DN=IBMHandle format. • **XMPP**: This address type supports xmpp-based communication. • **SMTP**: This address type supports communication with the SMTP server.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays 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
Add	Saves the modified information to the database.

Related links

Modifying the details of a public contact on page 523

User Management field descriptions

Tenant organization

The page displays the tenant organization that the administrator configured on the **Services** > **Tenant Management** page.

Note:

The system displays the tenant-related section only when the Multi Tenancy feature is enabled on this system.

Icon	Description
🔍	Searches for users on the basis of first name, last name, login name, surname, handles, first name (Latin translation) and last name (Latin translation). You can view, edit, or delete a user that is displayed in the list.

Field	Description
Select check box	Select the check box for the tenant from the list of tenants to view the organization hierarchy. You must select the check box at each level to view the hierarchy.
Enable auto refresh	Updates the information in the **Users** section automatically based on the selection in the tenant organization hierarchy when you select the check box.
Refresh Users	Updates the tenant organization hierarchy. Use the button to view the changes that the administrator makes from **Services** > **Tenant Management**.
Search	Searches and displays the tenant organization.
Clear	Clears the search criteria.

Users

Field	Description
Last Name	The last name of the user.
First Name	The first name of the user.
Display Name	The unique name of the user displayed by the system.
Login Name	The unique name that gives access to the system.
SIP Handle	The unique communication address of the user.
Organization Hierarchy	The hierarchy of the tenant organization in the format Tenant/Site/Department/Team. For example, Citi/Pune/HomeLoans/LoanSupport **Note:** The system displays the field only when the administrator enables the Multi Tenancy feature.
Last Login	The date and time when the user successfully logged into the system.

Button	Description
View	Displays the User Profile View page where you can view the details of the selected user.
Edit	Displays the User Profile Edit page where you can modify the details of the selected user.
New	Displays the New User Profile page where you can create a new user.

Table continues…

Button	Description
Duplicate	Displays the User Profile Duplicate page where you can create a duplicate user.
Delete	Displays the User Delete Confirmation page where you can temporarily delete the selected users.
More Actions > **Assign Roles**	Displays the Assign Roles page where you can assign roles to selected users.
More Actions > **Add To Group**	Displays the Assign Groups page where you can assign groups to selected users.
More Actions > **Show Deleted User**	Displays the Deleted Users page where you can view, permanently delete, or restore the deleted users.
More Actions > **Bulk Edit Users**	Displays the User Bulk Editor page where you can change the user data.
More Actions > **Status of Bulk Edit Users Jobs**	Displays the Schedule Bulk Edit of Users page where you can view or delete the bulk edit job.
More Actions > **Import Users**	Displays the Import users page where you can import the user-related data in bulk.
More Actions > **Export All Users**	Displays the Export users page where you can export the user-related data in bulk of all users.
More Actions > **Export Selected Users**	Displays the Export users page where you can export the user-related data in bulk of the users that you selected.
More Actions > **Import Global Settings**	Displays the Import global settings page where you can import shared addresses, public contacts, and presence access control list (ACLs) in bulk.
More Actions > **Download Excel Template**	Navigates to the location from where you can download the Excel template that System Manager supports.
Advanced Search	Displays fields where you can specify the search criteria for searching a user.
Filter: Enable	Displays fields under columns where you can set the filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters users based on the filter criteria.
Select: All	Selects all users in the table.
Select: None	Clears the check box selections.
🔄	Refreshes the user information in the table.

Criteria

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the upper-right corner of the page.

Field	Description
Criteria	The criteria to search. The following fields are available: • Field 1 – Lists the criteria that you can use to search users. • Field 2 – Lists the operators for evaluating the expression. The operators displayed depends on the criterion that you selected in **Field 1** field. • Field 3 – Lists the value for the search criterion. The User Management service retrieves and displays users that match this value.

User Profile View field descriptions

Organization

Name	Description
Tenant	The name of the tenant that you must select.
Level 1	The name of the level 1 hierarchy of the tenant organization. For example, Site. The tenant administrator provides the hierarchy on the Tenant Management page.
Level 2	The name of the level 2 hierarchy of the tenant organization. For example, Department.
Level 3	The name of the level 3 hierarchy of the tenant organization. For example, Team.

User Provisioning Rule

Name	Description
User Provisioning Rule	The name of the user provisioning rule. You can provide only one user provisioning rule.

Note:

When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

Identity tab — Identity section

Name	Description
Last Name	The last name of the user. For example, Miller.

Table continues…

Name	Description
Last Name (Latin Translation)	The user-preferred last name that the system must display on the end points. For example, Miller. Typically, the name is the written or spoken language of the user. **Note:** When you create a user, if the **Last Name (Latin Translation)** and **First Name (Latin Translation)** fields are: • Blank, the system displays the last name and first name in the fields. The values change when the last name and first names change. • Filled, the values remain even after you change the values in the **Last Name** and **First Name** fields.
First Name	The first name of the user. For example, John.
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Status	The login status of the user.
Update Time	The time when the user details were last modified.
Login Name	The unique system login name given to the user. The login name takes the form of username@domain. You use the login name to create the user's primary handle. The login name is not case-sensitive. For example, if you enter JMILLER@AVAYA.COM, the system converts the login name to lowercase, that is, jmiller@avaya.com. However, on the login page, you can enter JMILLER@AVAYA.COM or jmiller@avaya.com. The login name can be in uppercase or lowercase. You cannot edit the **Login Name** field for users with the login name admin.
Authentication Type	Authentication type defines how the system performs user authentication. The options are: • **Enterprise**: The enterprise authenticates the user login.

Table continues…

Name	Description
	• **Basic**: Avaya Authentication Service authenticates the user login.
Source	The entity that created this user record. The options are IP Address/Port, or a name representing an enterprise LDAP, or Avaya.
Localized Display Name	The localized display name of a user. Usually, the name is the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. The field supports display names that cannot handle localized text, for example, some endpoints.
Title	The personal title for address a user. Usually, the title is a social title and not the work title.
Language Preference	The preferred written or spoken language of the user.
Time Zone	The preferred time zone of the user.
Employee ID	The employee number for the user.
Department	The department to which the user belongs.
Company	The organization where the user works.

Identity tab — Address section

Name	Description
Name	The unique label that identifies the address.
Address Type	The type of the address. Types of addresses are: • Office • Home
Street	The name of the street.
City	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. In United States, this is Zip code.
Province	The full name of the province.
Country	The name of the country.

Identity tab — Localized Names section

Name	Description
Language	The localized languages for displaying the user name.
Display Name	The user name in the localized language you choose.

Button	Description
New	Allows you to add a new localized name for the user.
Edit	Allows you to edit the localized name for the user.
Delete	Deletes the localized names you select for the user.
Add	Adds or edits the localized name for the user.
Cancel	Cancels your add or edit of the localized name.

Communication Profile tab — Communication Profile

Use this section to create, modify, and delete a communication profile of the user. Each communication profile can contain one or more communication addresses for a user.

Name	Description
Communication Profile Password	The communication profile password. The field is available only if you enable the communication profile. The password policy is configured from **Users** > **User Management** > **Communication Profile Password Policy**.
Option button	The option to view the details of the selected communication profile.
Name	The name of the communication profile. You must select the name.

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Done	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding of a communication profile.

The system enables the following fields when you click **New** in the Communication Profile section.

Communication Profile tab — Communication Address section

Name	Description
Type	The type of the handle.
Handle	The unique communication address for the user.
Domain	The name of the domain with which the handle is registered.

Communication Profile tab — Session Manager section

Note:

The system displays the following fields only if a communication profile of the user exists for the product.

Name	Description
Primary Session Manager	The Session Manager instance that you use as home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point to connect devices that are associated with the communication profile to the Avaya network. A selection is required.
Secondary Session Manager	If you select a secondary Session Manager instance, this Session Manager provides continued service to SIP devices associated with this Communication Profile when the primary Session Manager becomes unavailable. A selection is optional.
Survivability Server	For local survivability, a survivability server that you can specify to provide survivability communication services for devices associated with a communication profile if local connectivity to Session Manager instances in Avaya Aura® is lost. If Branch Session Manager is selected, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to the Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional. **Note:** If a termination or origination application sequence contains a Communication Manager application, the Communication Manager associated with the application must be the main Communication Manager for the Communication Manager survivable remote server that is resident with Branch Session Manager.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.
Block New Registration When Maximum Registrations Active	If you select the check box and an endpoint attempts to register using this communication profile after the

Table continues…

Name	Description
	registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint.
Origination Application Sequence	An application sequence that will be invoked when the system routes the calls from this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Termination Application Sequence	An application sequence that will be invoked when calls are routed to this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.
Home Location	The location that Session Manager uses when the IP address of the calling phone does not match any IP address pattern of any location. This field is specified to support mobility of the user.

Communication Profile tab: Engagement Development Platform Profile

Name	Description
Service Profile	The profile that you assign to the user. The user can gain access to the service contained in the profile.

Communication Profile tab — CM Endpoint Profile

Note:

The system displays these fields only if a CM Endpoint profile exists for the user.

Name/Button	Description
System	Communication Manager on which you add the endpoint. The Communication Manager system on which you add the endpoint. You must select the system.
Profile Type	The type of the profile for the user.
Extension	The extension of the endpoint that you associate this profile with. You must select the extension.
View Endpoint	The list of existing or available endpoints based on the selection of the **Use Existing Endpoints** check box.
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. You must select the port.
Voice Mail Number	The voice mail number of the endpoint you associate with.
Preferred Handle	Numeric only handles, SIP handles, or nonSIP handles, that are administered for a user. The **Preferred Handle** field is optional. By default, the field is blank. If SIP entity is of the Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
Enhanced Callr-Info display for 1–line phones	The option to activate the enhanced Callr-info operation on the phone. The **Enhanced Callr-Info display for 1-line phones** field on the station form is valid for the following set types: • 1603, 1608, 1616, 1408, 1416 • 2402, 2410, 2420 • 4606, 4612, 4612CL, 4624, 4602, 4602+, 4630, 4610, 4622, 4620, 4621, 4625, • 6402D, 6408D, 6408D+, 6416D+, 6424D+, 607A1 • 7506D, 7507D • 8405D+, 8410D, 8405D, 8411D

Table continues…

Name/Button	Description
	• 9404, 9408, 9601, 9601+, 9610, 9620, 9621, 9608, 9611, 9630, 9640, 9641, 9650 The valid options are: • **No**: Does not change the callr-info interactions with the connected phone. The default setting. • **Yes**: Activates the enhanced Callr-info operation including the application of the existing feature related system parameters. Clear Callr-Info option settings of leave-ACW, next-call and on-call-release. If the **callr-info** button is not assigned to the phone on the station form, **Enhanced Callr-Info display for 1-line phones** does not apply.
Delete Endpoint on Unassign of Endpoint from User or Delete User	The option to specify whether 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.
Override Endpoint Name	The option to override the following: • The endpoint name on Communication Manager with the value you configured on the Manage users page during synchronization. If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization. • The localized display name on the Manage Users page in the **Localized Display Name** field of Communication Manager. If you clear the check box, the system does not override the localized display name in the **Localized Display Name** field.

Communication Profile tab - CS1000 Endpoint Profile

Name	Description
System	The CS 1000 system of the endpoint.
Target	The system customer number for the Communication Server.
Template	The phone or endpoint template that you can choose for the user. The element manager maintains all templates.
Update	The option to update the endpoint profile information for the user. When you click **Update**, the system takes displays the element manager cut through for the updates.

Table continues…

Name	Description
Service Details	The service details, such as set type of endpoints that the system displays after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values.
Include in Corporate Directory	The option to add this profile to the CS 1000 corporate directory.

Communication Profile tab — Messaging Profile

Note:

The system displays the following fields only if you can configure a messaging profile for the user.

Name	Description
System	The messaging system on which you add the subscriber.
Template	The template, system-defined or user-defined, that you associate with the subscriber.
Mailbox Number	The mailbox number of the subscriber.
Password	The password for logging on to the mailbox.
Delete Subscriber on Unassign of Subscriber from User	Provides the option to specify whether 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.

Communication Profile tab - CallPilot Messaging Profile

Field	Description
System	The CallPilot system of the mailbox that you can view.
Location	The location that is mapped to the **CallPilot Location** field. CallPilot Manager provides the **Location** field.
Template	The mailbox template that you apply. The element manager maintains all mailbox templates.
Update	An option to update the mailbox information for the user. The system cuts through to the element manager for the updates.
Service Details	The mailbox service details from endpoint after you create the mailbox.
Mailbox Number	The mailbox number or the extension DN of the user.

Communication Profile tab — IP Office Endpoint Profile

Use this profile to assign a new or an existing user to a System Manager device in User Management.

While adding a user, if you choose to assign a CM endpoint profile and an IP Office endpoint profile to the user, then the system uses the IP Office endpoint profile as the survivability option for the CM endpoint profile. That is, the endpoint extension used in the CM endpoint profile is also used for creating an IP Office endpoint profile so that when Communication Manager is unavailable, the IP Office device can serve the extension.

Note:

If a Communication Manager endpoint profile is present while adding or editing a user, the user administration functions in the centralized mode. If a Communication Manager endpoint profile is present, the user administration functions in the distributed mode.

Commit the Communication Manager endpoint profile and the Session Manager endpoint profile before you add an IP Office endpoint profile for a centralized user.

Name/Button	Description
System	The list of IP Office device names from which you can select the IP Office device you associate with the user.
Template	The list of user templates from which you can select your preferred template to set the user configurations.
Use Existing Extension	Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint you associate. The field lists the endpoints, existing or available, based on option you selected in the **Use Existing Endpoints** check box.
Endpoint Editor button	Starts the IP Office application, where you can edit or view the details of the IP Office endpoint. After you save the changes in IP Office manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Module-Port	The module port combination list for IP Office analog extensions. You must select **Module-Port** for centralized users with Set Type as **Analog**.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the set type is auto populated.

Table continues…

Name/Button	Description
Delete Extension On User Delete check box	Provides the option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with **Analog** and **Digital** set types.

Communication Profile tab — Presence Profile

Name	Description
System	The Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile: • Aggregate presence • Archive instant messages if the Instant Messages option is enabled
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with the AES Collector. The options are: • **System Default** • **Off** • **On** The default is **System Default**. You can change the default value. You do not require to configure AES Collector in the Presence Services server.

Communication Profile tab: Conferencing Profile

Name	Description
Select Auto-generated Code Length	The number of characters in PIN. The default is 6. The system displays this field if you select the **Auto Generate Participant and Moderator Security Code** check box.
Auto Generate Participant and Moderator Security Code	Select the check box if the system must generate the participant security code and moderator security code for this user. Clear the check box to assign a specific participant security code or moderator security code for this user.
Participant Security Code	The participant security code that you assign for this user.

Table continues…

Name	Description
	The system displays this field only when the **Auto Generate Participant and Moderator Security Code** check box is clear.
Moderator Security Code	The moderator security code that you assign for this user. The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Location	The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users. For SIP users, the system uses the location value from the **Home Location** field in the Session Manager profile.
Template	The Conferencing template that you assign to this user.

Button	Description
Get Templates	Displays the list of Conferencing templates that you can assign to this user.

Communication Profile tab: Work Assignment Profile

Name	Description
Account	The account name.
Account Address	The account address.
Source	The source name.
Source Address	The source address.

When you click **Resource Details**, **Account Details**, or **Source Details**, the system displays the Assignment Management page in Work Assignment.

Button	Description
Resource Details	Displays the Assignment Management page where you can configure assignment targets for the user. You can assign resource details to an agent only when the user has the Work Assignment profile assigned to the user.
Account Details	Displays the text box where you can add or modify the account name and account address. You can add attributes to the account only when the account is added to the agent.

Table continues…

Button	Description
Source Details	Displays the text box where you can add or modify the source name and source address. You can add properties and attributes to the source only when the source already exists.

Membership tab — Roles section

Name	Description
Name	The name of the role.
Description	A brief description about the role.

Membership tab — Group Membership section

Name	Description
Name	The name of the group.
Type	The group type based on the resources.
Hierarchy	The position of the group in the hierarchy.
Description	A brief description about the group.

Contacts tab — Default Contact List section

Name	Description
Description	A brief description of the contact list.

Contacts tab — Associated Contacts section

Name	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Scope	The categorization of the contact based on whether the contact is a public or private contact.
Speed Dial	The value that specifies whether the speed dial is set for the contact.
Speed Dial Entry	The reduced number that represents the speed dial number.
Presence Buddy	The value that specifies whether you can monitor the presence information of the contact or not. **False** indicates that you cannot track the presence of the contact.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.

Table continues…

Button	Description
Filter: Enable	Text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab — Private Contacts section

Use this section to add new private contacts, modify and deletes existing contacts.

Name	Description
Last Name	The last name of the private contact.
First Name	The first name of the private contact.
Display Name	Display name of the private contact.
Contact Address	The address of the private contact.
Description	A brief description about the contact.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Edit	Opens the User Profile Edit page. Use the User Profile Edit page to modify the details of the user account.
Done	Closes the User Profile View page and returns to the User Management page.

New User Profile field descriptions

Use the New User Profile page to create a new user. This page has four tabs:

- **Identity**
- **Communication Profile**
- **Membership**
- **Contacts**

Note:

Fields marked with an asterisk are mandatory and you must enter appropriate information in these fields.

Organization

Name	Description
Tenant	The name of the tenant that you must select.
Level 1	The name of the level 1 hierarchy of the tenant organization. For example, Site. The tenant administrator provides the hierarchy on the Tenant Management page.
Level 2	The name of the level 2 hierarchy of the tenant organization. For example, Department.
Level 3	The name of the level 3 hierarchy of the tenant organization. For example, Team.

User Provisioning Rule

Name	Description
User Provisioning Rule	The name of the user provisioning rule. You can provide only one user provisioning rule.

Note:

When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

Identity tab: Identity

Name	Description
Last Name	The last name of the user. For example, Miller.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the end points. For example, Miller. Typically, the name is the written or spoken language of the user. **Note:** When you create a user, if the **Last Name (Latin Translation)** and **First Name (Latin Translation)** fields are: • Blank, the system displays the last name and first name in the fields. The values change when the last name and first names change.

Table continues…

Name	Description
	- Filled, the values remain even after you change the values in the **Last Name** and **First Name** fields.
First Name	The first name of the user. For example, John.
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Login Name	The login name of the user. The login name is not case-sensitive. For example, if you enter JMILLER@AVAYA.COM, the system converts the login name to lowercase, that is, jmiller@avaya.com. However, on the login page, you can enter JMILLER@AVAYA.COM or jmiller@avaya.com. The login name can be in uppercase or lowercase. If you log in to the system as admin, you cannot edit the login name. **Note:** To create the user data by using a blank excel template, append the login name with #ProfileSetName in all worksheets except Basic and Profile Set. The system associates the user records with the communication profile that you have provided. For example, jmiller@avaya.com#ProfileSetName.
Authentication Type	The type of authentication that defines how the system performs the authentication of the user. The options are: • **Enterprise**: Directory servers that are external to System Manager authenticate the user login. • **Basic**: Avaya authentication service authenticates the user login. For bulk import of users by using Excel, **Authentication Type** is always Basic. Therefore, the **Authentication Type** field remains invisible in the Excel file.
Password	The password to log in to the System Manager web console.

Table continues…

Name	Description
Confirm Password	The password that you reenter for confirmation.
Localized Display Name	The localized display name of a user. The name is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. The display name supports displays that cannot handle localized text, for example, some endpoints.
Title	The personal title that is set to address a user. The title is typically a social title and not the work title. For example, Mr.
Language Preference	The preferred written or spoken language of the user. For example, English.
Time Zone	The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.
Employee ID	The employee number for the user. For example, 20081234.
Department	The department to which the user belongs. For example, Human Resources.
Company	The organization where the user works. For example, Avaya Inc.

Identity tab: Address

Name	Description
Select check box	The option to select an address in the table.
Name	The name of the addressee. For example, Avaya.
Address Type	The type of address. The values are: • **Office** • **Home**
Street	The name of the street. For example, Magarpatta.
City	The name of the city or town. For example, Pune.
Postal Code	The postal code used by postal services to route mail to a destination. For example, 411028. For United States, the postal code is the Zip code.
Province	The full name of the province. For example, Maharashtra.
Country	The name of the country. For example, India.

Button	Description
New	Displays the Add Address page. Use the page to add the address details.

Table continues…

Button	Description
Edit	Displays the Edit Address page. Use the page to modify the address.
Delete	Deletes the selected address.
Choose Shared Address	Displays the Choose Address where you choose a shared or common address.

Identity tab: Localized Names

Note:

Use the **Localized Names** section only for the CS 1000 system. The section does not apply for Session Manager and Communication Manager.

Name	Description
Language	The localized languages for displaying the user name. For example, English. You must select the language.
Display Name	The user name in the localized language you choose. For example, John Miller.

Button	Description
New	Displays fields that you can use to create a new localized name for the user.
Edit	Displays fields that you can use to modify the localized name for the user.
Delete	Deletes the localized names that you select for the user.
Add	Adds or edits the localized name for the user.
Cancel	Cancels the addition or edits of the localized name.

Communication Profile tab: Communication Profile

Use this section to create, modify, and delete a communication profile of the user. Each communication profile can contain one or more communication addresses for a user.

Name	Description
Communication Profile Password	The communication profile password. The field is available only if you enable the communication profile. The password policy is configured from **Users** > **User Management** > **Communication Profile Password Policy**.
Confirm Password	The communication profile password that you reenter for confirmation.

Table continues…

Name	Description
Option button	The option to view the details of the selected communication profile.
Name	The name of the communication profile. You must select the name.

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Done	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding of a communication profile.

The system enables the following fields when you click **New** in the **Communication Profile** section.

Name	Description
Name	The name of the communication profile for the user.
Default	The option to select a profile as default or the active profile. At a time, only one active profile can exist.

Communication Profile tab: Communication Address

Use this section to create, modify, and delete the communication address of a user. Each communication profile can contain one or more communication addresses for a user.

Name	Description
Type	The type of the handle.
Handle	A unique communication address of the user.
Domain	The name of the domain with which the handle is registered.

Button	Description
New	The fields for adding a new communication address.
Edit	The 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. The following fields define the communication address for the user.

Name	Description
Type	The type of the handle. The different types of handles are: • **Avaya SIP**: Indicates that the handle supports Avaya SIP-based communication. • **Avaya E.164**: Indicates 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. • **Microsoft SIP**: Indicates that the handle supports SIP-based communication. • **Microsoft Exchange**: Indicates that the handle is an email address and supports communication with Microsoft SMTP server. • **Lotus Notes**: Indicates that the handle is for Lotus Notes and domino calender. • **IBM Sametime**: Indicates that the handle is for IBM Sametime. The address must be in the DN=IBMHandle format. • **Avaya Presence/IM**: Indicates that the handle is an address that is used for Extensible Messaging and Presence Protocol (XMPP)-based Internet Messaging (IM) services, and XMPP or Session Initiation Protocol-based (SIP) Presence services. **Note:** To create the Presence communication profile, you must select **Avaya Presence/IM** and provide the communication address. • **GoogleTalk**: Indicates that the handle supports XMPP-based communication with the Google Talk service. • **Other Email**: Indicates that the handle is an email address other than MS Exchange email addresses. • **Other SIP**: Indicates that the handle supports SIP-based communication other than the listed ones. • **Other XMPP**: Indicates that the handle supports XMPP-based communication other than the listed ones. • **Work Assignment**: Indicates that the handle supports accounts which can be assigned to an agent for Work Assignment.

Table continues…

Name	Description
Fully Qualified Address	The fully qualified domain name or uniform resource identifier. The address can be an email address, IM user, or an address of a communication device by using which the user can send or receive messages. You must provide the fully qualified address.

Button	Description
Add	Saves the new communication address or modified communication address information in the database.
Cancel	Cancels the addition of communication address.

Communication Profile tab: Session Manager

✱ **Note:**

The system displays the following fields only if a communication profile of the user exists for the product.

Name	Description
Primary Session Manager	The instance that you want to use as the home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura® network. You must select the primary Session Manager server.
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. A selection is optional.
Survivability Server	For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile when the local connectivity to Session Manager instances in Avaya is lost. If you select a Branch Session Manager , and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional.

Table continues…

Name	Description
	Note: If a termination or origination application sequence contains a Communication Manager application, the Communication Manager instance associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.
Block New Registration When Maximum Registrations Active	If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint. If you clear the check box, the system accepts the new registration and unregisters the endpoint with the oldest registration. However, if the endpoint with the oldest registration is active on a call then the system does not unregister the endpoint until the call completes.
Origination Application Sequence	The application sequence that the system will invoke when routing the calls from this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Termination Application Sequence	The application sequence that will be invoked when the system routes the calls to this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.

Table continues…

Name	Description
Home Location	The home location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any of the location. You must specify a value.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.
Enable Centralized Call History	The option to enable the call history feature for SIP users. By default, the system disables the call history feature. The maximum number of call logs per communication profile is 100.

Communication Profile tab: Engagement Development Platform Profile

Name	Description
Service Profile	The profile that you assign to the user. The user can gain access to the service contained in the profile.

Communication Profile tab: CM Endpoint Profile

Note:

The system displays these fields only if a CM Endpoint profile exists for the user.

Field/Button	Description
System	The Communication Manager system on which you add the endpoint. You must select the system.
Profile Type	The type of the Communication Manager Endpoint profile that you create. You must select the profile type.
Use Existing Endpoints	Select the check box to use the existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint that you associate this profile with. You must select the extension. The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.

Table continues…

Field/Button	Description
Endpoint Editor button	Click to start the Communication Manager application where you can edit or view details of the endpoint. After you save the changes in Communication Manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Template	The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add. You must select the template.
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. You must select the port. The field lists the possible ports based on the selected set type.
Voice Mail Number	The voice mail number of the endpoint you associate with.
Preferred Handle	Numeric only handles, SIP handles, or nonSIP handles, that are administered for a user. The **Preferred Handle** field is optional. By default, the field is blank. If the type of the SIP entity is Communication Manager, Session Manager uses preferred handle in CM Endpoint profile.
Calculate Route Pattern	The option to automatically select the route pattern based on the primary or secondary Session Manager configured in **Session Manager Communication Profile**.
Sip Trunk	The system makes this field available only for the SIP set type. If you select **Calculate Route Pattern** check box, the system: • Populates the **Sip Trunk** field • Makes the **Sip Trunk** field read-only.
Enhanced Callr-Info display for 1–line phones	The option to activate the enhanced Callr-info operation on the phone.

Table continues…

Field/Button	Description
	The **Enhanced Callr-Info display for 1-line phones** field on the station form is valid for the following set types: • 1603, 1608, 1616, 1408, 1416 • 2402, 2410, 2420 • 4606, 4612, 4612CL, 4624, 4602, 4602+, 4630, 4610, 4622, 4620, 4621, 4625, • 6402D, 6408D, 6408D+, 6416D+, 6424D+, 607A1 • 7506D, 7507D • 8405D+, 8410D, 8405D, 8411D • 9404, 9408, 9601, 9601+, 9610, 9620, 9621, 9608, 9611, 9630, 9640, 9641, 9650 The valid options are: • **No**: Does not change the callr-info interactions with the connected phone. The default setting. • **Yes**: Activates the enhanced Callr-info operation including the application of the existing feature related system parameters. Clear Callr-Info option settings of leave-ACW, next-call and on-call-release. If the **callr-info** button is not assigned to the phone on the station form, **Enhanced Callr-Info display for 1-line phones** does not apply.
Delete Endpoint on Unassign of Endpoint from User or on Delete User	The option to specify whether 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.
Override Endpoint Name and Localised Name	The option to override the following endpoint names: • The endpoint name on Communication Manager with the value you configured on the Manage users page during synchronization. If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization. • The localized display name on the Manage Users page in the **Localized Display Name** field of Communication Manager. If you clear the check box, the system does not override the localized display name in the **Localized Display Name** field.

Table continues…

Field/Button	Description
Allow H.323 and SIP Endpoint Dual Registration	The option to register both an H.323 endpoint and a SIP endpoint together at the same time to the same extension.

Communication Profile tab: CS 1000 Endpoint Profile

Name	Description
System	The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.
Add new	The option to create a new phone.
Target	The system customer number for the CS 1000 system. You must select the target. The system displays the field only when you select **Add new**.
Template	The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template. The system displays the field only when you select **Add new**.
Update	Updates the station profile information for the user. When you click **Update**, the system takes you to the element manager cut-through for the updates.
Service Details	The service details of endpoints, such as set type, after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values for this field. The system displays the field only when you select **Add new**.
Terminal Number	The terminal number of the phone. The system displays the field only when you select **Add new**.
Link existing	The option to associate with the existing phone.
Existing TN	The terminal number from the list of existing numbers. The system displays the field only when you select **Link existing**.
Include in Corporate Directory	The option to add this profile to the CS 1000 Corporate Directory feature.

Communication Profile tab: Messaging Profile

Note:

The system displays the following fields only if you can configure a messaging profile for the user.

Name	Description
System	The messaging system on which you add the subscriber. You must select the system.
Use Existing Subscriber on System	The option to specify whether to use an existing subscriber mailbox number to associate with this profile.
Mailbox Number	The mailbox number of the subscriber. You must select the mailbox number. The field takes the existing mailbox number that you associate with this profile. This value in the field is valid only if you select the **Use Existing Subscriber on System** check box.
Messaging Editor	Click to start the Messaging application where you can edit or view details of the profile of the messaging endpoint. After you save the changes in the Messaging system, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Template	The system-defined or user-defined template that you associate with the subscriber.
Password	The password for logging in to the mailbox. You must provide the password.
Delete Subscriber on Unassign of Subscriber from User or on Delete User	The option to specify whether 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.

Communication Profile tab: CallPilot Messaging Profile

Name	Description
System	The CallPilot system to which you add a mailbox. You must select the system.
Target	The field that maps to the CallPilot **Location** field. CallPilot Manager provides the **Target** field. You must select the target.
Template	The mailbox template that you use. Select a template from the drop down list. The element

Table continues…

Name	Description
	manager maintains all the mailbox templates. You must select the template.
Update	Updates the mailbox information for the user. If you click the **Update** button, the system cuts through to the element manager for the updates.
Service Details	Displays mailbox service details from the endpoint after you create the mailbox.
Mailbox Number	The mailbox number or the extension DN of the user. You must select the mailbox number.

Communication Profile tab: IP Office Endpoint Profile

Use this profile to assign a new or an existing user to a System Manager device in User Management.

While adding a user, if you choose to assign a CM endpoint profile and an IP Office endpoint profile to the user, then the system uses the IP Office endpoint profile as the survivability option for the CM endpoint profile. That is, the endpoint extension used in the CM endpoint profile is also used for creating an IP Office endpoint profile so that when Communication Manager is unavailable, the IP Office device can serve the extension.

Note:

If a Communication Manager endpoint profile is present while adding or editing a user, the user administration functions in the centralized mode. If a Communication Manager endpoint profile is present, the user administration functions in the distributed mode.

Before you add an IP Office endpoint profile for a centralized user, commit the changes to the Communication Manager endpoint profile and the Session Manager endpoint profile.

Field/Button	Description
System	The list of IP Office device names from which you can select the IP Office device that you associate with the user. You must select the template.
Template	The list of user templates from which you can select your preferred template to set the user configurations. You must select the template.
Use Existing Extension	Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint you associate with. You must select the extension. The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.

Table continues…

Field/Button	Description
Endpoint Editor	Starts the IP Office application where you can edit or view the details of the IP Office endpoint. After you save the changes in the IP Office manager, the system updates the modified data on the device or database only when you commit the changes on the User Profile Edit page.
Module-Port	The module port combination list for IP Office analog extensions. You must select **Module-Port** for centralized users with Set Type as **Analog**.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the system populates the set type.
Delete Extension On User Delete	The option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with **Analog** and **Digital** set types.

Communication Profile tab: Presence Profile

You can create Presence profiles only for the default communication profile.

Name	Description
System	The Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile: • Aggregate presence • Archive instant messages if the Instant Messages option is enabled
SIP Entity	The option to route the SIP-based messages through the Presence Services This system selects the SIP entity only if you select a Presence Services instance in the **System** field. **SIP Entity** is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.
IM Gateway	The IP address of the IM gateway.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with the AES Collector. The options are: • **System Default**

Table continues…

Name	Description
	- **Off** - **On** The default is **System Default**. You can change the default value. You do not require to configure AES Collector in the Presence Services server.

Communication Profile tab: Conferencing Profile

Name	Description
Select Auto-generated Code Length	The number of characters in PIN. The default is 6. The system displays this field if you select the **Auto Generate Participant and Moderator Security Code** check box.
Auto Generate Participant and Moderator Security Code	Select the check box if the system must generate the participant security code and moderator security code for this user. Clear the check box to assign a specific participant security code or moderator security code for this user.
Participant Security Code	The participant security code that you assign for this user. The system displays this field only when the **Auto Generate Participant and Moderator Security Code** check box is clear.
Moderator Security Code	The moderator security code that you assign for this user. The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Location	The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users. For SIP users, the system uses the location value from the **Home Location** field in the Session Manager profile.
Template	The Conferencing template that you assign to this user.

Button	Description
Get Templates	Displays the list of Conferencing templates that you can assign to this user.

Communication Profile tab: Work Assignment Profile

Name	Description
Account	The account name.
Account Address	The account address.
Source	The source name.
Source Address	The source address.

When you click **Resource Details**, **Account Details**, or **Source Details**, the system displays the Assignment Management page in Work Assignment.

Button	Description
Resource Details	Displays the Assignment Management page where you can configure assignment targets for the user. You can assign resource details to an agent only when the user has the Work Assignment profile assigned to the user.
Account Details	Displays the text box where you can add or modify the account name and account address. You can add attributes to the account only when the account is added to the agent.
Source Details	Displays the text box where you can add or modify the source name and source address. You can add properties and attributes to the source only when the source already exists.

Membership tab: Roles

Name	Description
Select check box	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.
Name	The name of the role.
Description	A brief description about the role.

Button	Description
Assign Roles	Displays the Assign Role page that you can use to assign the roles to the user account.
Unassign Roles	Removes the selected role from the list of roles associated with the user account.

Membership tab: Group Membership

Name	Description
Select check box	Use this check box to select a group.
Name	The name of the group.
Type	The group type based on the resources.
Hierarchy	The position of the group in the hierarchy.
Description	A brief description about the group.

Button	Description
Add To group	Displays the Assign Groups page that you can use to add the user to a group.
Remove From Group	Removes the user from the selected group.

Contacts tab: Default Contact List

Name	Description
Description	A brief description of the contact list.

Contacts tab: Associated Contacts

Name	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Scope	The 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 cannot track the presence of the contact.

Button	Description
Edit	Displays the Edit Contact List Member page. Use this page to modify the information of the selected contact.
Add	Displays the Attach Contacts page. Use this page to select one or more contacts from the list of contacts. In the Multi Tenancy environment, when the tenant administrator of a tenant creates or updates the user,

Table continues…

Button	Description
	the administrator can attach only the following contacts: • Private contacts of the user • Public contacts • Users who belong to that tenant
Remove	Removes one or more selected contacts from the list of the associated contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Displays the text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab: Private Contacts

Use this section to add new private contacts, and edit and delete the existing contacts.

Name	Description
Last Name	The last name of the private contact.
First Name	The first name of the private contact.
Display Name	The display name of the private contact.
Contact Address	The address of the private contact.
Description	A brief description about the contact.

Button	Description
Edit	Displays the Edit Private Contact page. Use this page to edit the information of the contact you selected.
New	Displays the **New Private Contact** page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Commit & Continue	Creates the user account in the database and retains you on the same page for further modifications.
Commit	Creates the user account and takes you to the User Management page.
Cancel	Cancels the user creation operation.

User Profile Edit field descriptions

Organization

Name	Description
Tenant	The name of the tenant that you must select.
Level 1	The name of the level 1 hierarchy of the tenant organization. For example, Site. The tenant administrator provides the hierarchy on the Tenant Management page.
Level 2	The name of the level 2 hierarchy of the tenant organization. For example, Department.
Level 3	The name of the level 3 hierarchy of the tenant organization. For example, Team.

Note:

You cannot edit the tenant. If you select a different level 1 for the tenant from the organization hierarchy, the **Level 2** and **Level 3** fields become blank. You can select new values for level 2 and level 3. If you select a different level 2 for the tenant from the organization hierarchy, the **Level 3** field becomes blank. You can select a new value for level 3.

User Provisioning Rule

Name	Description
User Provisioning Rule	The user provisioning rule that you must edit.

Identity tab — Identity section

Name	Description
Last Name	The last name of the user. For example, Miller.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the end points. For example, Miller. Typically, the name is the written or spoken language of the user.

Table continues…

Name	Description
	Note: When you create a user, if the **Last Name (Latin Translation)** and **First Name (Latin Translation)** fields are: • Blank, the system displays the last name and first name in the fields. The values change when the last name and first names change. • Filled, the values remain even after you change the values in the **Last Name** and **First Name** fields.
First Name	The first name of the user. For example, John.
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Status	The login status of the user
Update Time	The time when the user details were last modified.
Login Name	The login name of the user. The login name is not case-sensitive. For example, if you enter JMILLER@AVAYA.COM, the system converts the login name to lowercase, that is, jmiller@avaya.com. However, on the login page, you can enter JMILLER@AVAYA.COM or jmiller@avaya.com. The login name can be in uppercase or lowercase. If you log in to the system as admin, you cannot edit the login name. **Note:** To create the user data by using a blank excel template, append the login name with #ProfileSetName in all worksheets except Basic and Profile Set. The system associates the user records with the communication profile that you have provided. For example, jmiller@avaya.com#ProfileSetName.

Table continues…

Name	Description
Authentication Type	The type of authentication that defines how the system performs the authentication of the user. The options are: • **Enterprise**: Directory servers that are external to System Manager authenticate the user login. • **Basic**: Avaya authentication service authenticates the user login. For bulk import of users by using Excel, **Authentication Type** is always Basic. Therefore, the **Authentication Type** field remains invisible in the Excel file.
Change Password	The new password. The selection is required.
Source	The entity that created this user record. The possible values for this field is either an IP Address/Port, or a name representing an enterprise LDAP, or Avaya.
Localized Display Name	The localized display name of a user. The name is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. The display name supports displays that cannot handle localized text, for example, some endpoints.
Title	The personal title that is set to address a user. The title is typically a social title and not the work title. For example, Mr.
Language Preference	The preferred written or spoken language of the user. For example, English.
Time Zone	The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.
Employee ID	The employee number for the user. For example, 20081234.
Department	The department to which the user belongs. For example, Human Resources.
Company	The organization where the user works. For example, Avaya Inc.

Identity tab — Address section

Name	Description
Time Zone	The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.
Department	The department to which the user belongs. For example, Human Resources.

Table continues…

Name	Description
Address Type	The type of address. The values are: • **Office** • **Home**
Street	The name of the street. For example, Magarpatta.
City	The name of the city or town. For example, Pune.
Postal Code	The postal code used by postal services to route mail to a destination. For example, 411028. For United States, the postal code is the Zip code.
Province	The full name of the province. For example, Maharashtra.
Country	The name of the country. For example, India.

Button	Description
New	Displays the Add Address page. Use the page to add the address details.
Edit	Displays the Edit Address page. Use the page to modify the address.
Delete	Deletes the selected address.
Choose Shared Address	Displays the Choose Address where you choose a shared or common address.

Identity tab — Localized Names section

Name	Description
Language	The localized languages for displaying the user name. For example, English. You must select the language.
Display Name	The user name in the localized language you choose. For example, John Miller.

Button	Description
New	Displays fields that you can use to create a new localized name for the user.
Edit	Displays fields that you can use to modify the localized name for the user.
Delete	Deletes the localized names that you select for the user.
Add	Adds or edits the localized name for the user.
Cancel	Cancels the addition or edits of the localized name.

Communication Profile tab — Communication Profile

Use this section to create, modify, and delete a communication profile of the user. Each communication profile can contain one or more communication addresses for a user.

Name	Description
Calculate Route Pattern	The option to automatically select the route pattern based on the primary or secondary Session Managerconfigured in the **Session Manager Communication Profile**.
Sip Trunk	The system makes this field available only for the SIP set type. If you select **Calculate Route Pattern** check box, the system: • Populates the **Sip Trunk** field • Makes **Sip Trunk** field read-only.
Allow H.323 and SIP Endpoint Dual Registration	The option to register both an H.323 endpoint and a SIP endpoint together at the same time to the same extension.

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Done	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding of a communication profile.

The system enables the following fields when you click **New** in the Communication Profile section.

Name	Description
Name	The name of the communication profile for the user.
Default	The profile that is made default as the active profile. There can be only one active profile at a time.

Communication Profile tab — Communication Address

Use this section to create, modify, and delete the communication address of a user. Each communication profile can contain one or more communication addresses for a user.

Name	Description
Type	The type of the handle.
Handle	A unique communication address of the user.
Domain	The name of the domain with which the handle is registered.

Button	Description
New	The fields for adding a new communication address.
Edit	The 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** or **Edit** in the Communication Address section.

Name	Description
Type	The type of the handle. The different types of handles are: • **Avaya SIP**: Indicates that the handle supports Avaya SIP-based communication. • **Avaya E.164**: Indicates 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. • **Microsoft SIP**: Indicates that the handle supports SIP-based communication. • **Microsoft Exchange**: Indicates that the handle is an email address and supports communication with Microsoft SMTP server. • **Lotus Notes**: Indicates that the handle is for Lotus Notes and domino calender. • **IBM Sametime**: Indicates that the handle is for IBM Sametime. The address must be in the DN=IBMHandle format. • **Avaya Presence/IM**: Indicates that the handle is an address that is used for Extensible Messaging and Presence Protocol (XMPP)-based Internet Messaging (IM) services, and XMPP or Session Initiation Protocol-based (SIP) Presence services. **Note:** To create the Presence communication profile, you must select **Avaya Presence/IM** and provide the communication address. • **GoogleTalk**: Indicates that the handle supports XMPP-based communication with the Google Talk service. • **Other Email**: Indicates that the handle is an email address other than MS Exchange email addresses.

Table continues…

Name	Description
	- **Other SIP**: Indicates that the handle supports SIP-based communication other than the listed ones. - **Other XMPP**: Indicates that the handle supports XMPP-based communication other than the listed ones. - **Work Assignment**: Indicates that the handle supports accounts which can be assigned to an agent for Work Assignment.
Fully Qualified Address	The fully qualified domain name or uniform resource identifier. The address can be an email address, IM user, or an address of a communication device by using which the user can send or receive messages. You must provide the fully qualified address.

Button	Description
Add	Saves the new communication address or modified communication address information in the database.
Cancel	Cancels the addition of communication address.

Communication Profile tab:— Session Manager

Note:

The system displays the following fields only if a communication profile of the user exists for the product.

Name	Description
Primary Session Manager	The instance that you want to use as the home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura® network. You must select the primary Session Manager server.
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. A selection is optional.
Survivability Server	For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile when the local connectivity to Session Manager instances in Avaya is lost. If you

Table continues…

Name	Description
	select a Branch Session Manager , and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional. **Note:** If a termination or origination application sequence contains a Communication Manager application, the Communication Manager instance associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.
Block New Registration When Maximum Registrations Active	If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint.
Origination Application Sequence	The application sequence that the system will invoke when routing the calls from this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Termination Application Sequence	The application sequence that will be invoked when the system routes the calls to this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.

Table continues…

Name	Description
Home Location	The home location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any of the location. You must specify a value.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.

Communication Profile tab: Engagement Development Platform Profile

Name	Description
Service Profile	The profile that you assign to the user. The user can gain access to the service contained in the profile.

Communication Profile tab — CM Endpoint Profile

Note:

The system displays these fields only if a CM Endpoint profile exists for the user.

Name/Button	Description
System	The Communication Manager system on which you add the endpoint. You must select the system.
Profile Type	The type of the Communication Manager Endpoint profile that you create. You must select the profile type.
Use Existing Endpoints	Select the check box to use the existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint that you associate this profile with. You must select the extension. The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.
Template	The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add. You must select the template.

Table continues…

Name/Button	Description
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. You must select the port. The field lists the possible ports based on the selected set type.
Voice Mail Number	The voice mail number of the endpoint you associate with.
Preferred Handle	Numeric only handles, SIP handles, or nonSIP handles, that are administered for a user. The **Preferred Handle** field is optional. By default, the field is blank. If the type of the SIP entity is Communication Manager, Session Manager uses preferred handle in CM Endpoint profile.
Enhanced Callr-Info display for 1–line phones	The option to activate the enhanced Callr-info operation on the phone. The **Enhanced Callr-Info display for 1-line phones** field on the station form is valid for the following set types: • 1603, 1608, 1616, 1408, 1416 • 2402, 2410, 2420 • 4606, 4612, 4612CL, 4624, 4602, 4602+, 4630, 4610, 4622, 4620, 4621, 4625, • 6402D, 6408D, 6408D+, 6416D+, 6424D+, 607A1 • 7506D, 7507D • 8405D+, 8410D, 8405D, 8411D • 9404, 9408, 9601, 9601+, 9610, 9620, 9621, 9608, 9611, 9630, 9640, 9641, 9650 The valid options are: • **No**: Does not change the callr-info interactions with the connected phone. The default setting. • **Yes**: Activates the enhanced Callr-info operation including the application of the existing feature related system parameters. Clear Callr-Info option settings of leave-ACW, next-call and on-call-release. If the **callr-info** button is not assigned to

Table continues…

Name/Button	Description
	the phone on the station form, **Enhanced CallrInfo display for 1-line phones** does not apply.
Delete Endpoint on Unassign of Endpoint from User or on Delete User	The option to specify whether 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.
Override Endpoint Name and Localised Name	The option to override the following endpoint names: • The endpoint name on Communication Manager with the value you configured on the Manage users page during synchronization. If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization. • The localized display name on the Manage Users page in the **Localized Display Name** field of Communication Manager. If you clear the check box, the system does not override the localized display name in the **Localized Display Name** field.

Communication Profile tab - CS1000 Endpoint Profile

Field	Description
System	The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.
Target	The system customer number for the CS 1000 system. You must select the target. The system displays the field only when you select **Add new**.
Template	The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template. The system displays the field only when you select **Add new**.
Update	Updates the station profile information for the user. When you click **Update**, the system takes you to the element manager cut-through for the updates.
Service Details	The service details of endpoints, such as set type, after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values for this field.

Table continues…

Field	Description
	The system displays the field only when you select **Add new**.
Include in Corporate Directory	The option to add this profile to the CS 1000 Corporate Directory feature.

Communication Profile tab — Messaging Profile

Note:

The system displays the following fields only if you can configure a messaging profile for the user.

Name	Description
System	The messaging system on which you add the subscriber. You must select the system.
Use Existing Subscriber on System	The option to specify whether to use an existing subscriber mailbox number to associate with this profile.
Mailbox Number	The mailbox number of the subscriber. You must select the mailbox number. The field takes the existing mailbox number that you associate with this profile. This value in the field is valid only if you select the **Use Existing Subscriber on System** check box.
Messaging Editor	Click to start the Messaging application where you can edit or view details of the profile of the messaging endpoint. After you save the changes in the Messaging system, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Template	The system-defined or user-defined template that you associate with the subscriber.
Password	The password for logging in to the mailbox. You must provide the password.
Delete Subscriber on Unassign of Subscriber from User or on Delete User	The option to specify whether 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.

Communication Profile tab - CallPilot Messaging Profile

Field	Description
System	The CallPilot system of the messaging profile you edit. The selection is required.
Target	The field that maps to the CallPilot **Location** field. CallPilot Manager provides the **Target** field. You must select the target.
Template	The mailbox template that you use. Select a template from the drop down list. The element manager maintains all the mailbox templates. You must select the template.
Update	Updates the mailbox information for the user. If you click the **Update** button, the system cuts through to the element manager for the updates.
Service Details	Displays mailbox service details from the endpoint after you create the mailbox.
Mailbox Number	The mailbox number or the extension DN of the user. You must select the mailbox number.

Communication Profile tab — IP Office Endpoint Profile

Use this profile to assign a new or an existing user to a System Manager device in User Management.

While adding a user, if you choose to assign a CM endpoint profile and an IP Office endpoint profile to the user, then the system uses the IP Office endpoint profile as the survivability option for the CM endpoint profile. That is, the endpoint extension used in the CM endpoint profile is also used for creating an IP Office endpoint profile so that when Communication Manager is unavailable, the IP Office device can serve the extension.

Note:

If a Communication Manager endpoint profile is present while adding or editing a user, the user administration functions in the centralized mode. If a Communication Manager endpoint profile is present, the user administration functions in the distributed mode.

Commit the Communication Manager endpoint profile and the Session Manager endpoint profile before you add an IP Office endpoint profile for a centralized user.

Name/Button	Description
System	The list of IP Office device names from which you can select the IP Office device that you associate with the user. You must select the template.
Template	The list of user templates from which you can select your preferred template to set the user configurations.

Table continues…

Name/Button	Description
Use Existing Extension	Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Endpoint Editor button	The option to start the IP Office application, where you can edit or view the details of the IP Office endpoint. After you save the changes in IP Office manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Extension	The extension of the endpoint you associate with. You must select the extension. The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.
Module-Port	The module port combination list for IP Office analog extensions. You must select **Module-Port** for centralized users with Set Type as **Analog**.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the system populates the set type.
Delete Extension On User Delete	The option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with **Analog** and **Digital** set types.

Communication Profile tab — Presence Profile

Note:

Name	Description
System	The Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile: • Aggregate presence • Archive instant messages if the Instant Messages option is enabled

Communication Profile tab: Conferencing Profile

Name	Description
Select Auto-generated Code Length	The number of characters in PIN. The default is 6. The system displays this field if you select the **Auto Generate Participant and Moderator Security Code** check box.
Auto Generate Participant and Moderator Security Code	Select the check box if the system must generate the participant security code and moderator security code for this user. Clear the check box to assign a specific participant security code or moderator security code for this user.
Participant Security Code	The participant security code that you assign for this user. The system displays this field only when the **Auto Generate Participant and Moderator Security Code** check box is clear.
Moderator Security Code	The moderator security code that you assign for this user. The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Location	The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users. For SIP users, the system uses the location value from the **Home Location** field in the Session Manager profile.
Template	The Conferencing template that you assign to this user.

Button	Description
Get Templates	Displays the list of Conferencing templates that you can assign to this user.

Communication Profile tab: Work Assignment Profile

Name	Description
Account	The account name.
Account Address	The account address.
Source	The source name.
Source Address	The source address.

When you click **Resource Details**, **Account Details**, or **Source Details**, the system displays the Assignment Management page in Work Assignment.

Button	Description
Resource Details	Displays the Assignment Management page where you can configure assignment targets for the user. You can assign resource details to an agent only when the user has the Work Assignment profile assigned to the user.
Account Details	Displays the text box where you can add or modify the account name and account address. You can add attributes to the account only when the account is added to the agent.
Source Details	Displays the text box where you can add or modify the source name and source address. You can add properties and attributes to the source only when the source already exists.

Membership tab — Roles

Name	Description
Select check box	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.
Name	The name of the role.
Description	A brief description about the role.

Button	Description
Assign Roles	Displays the Assign Role page that you can use to assign the roles to the user account.
Unassign Roles	Removes the selected role from the list of roles associated with the user account.

Membership tab — Group Membership

Name	Description
Select check box	Use this check box to select a group.
Name	The name of the group.
Type	The group type based on the resources.
Hierarchy	The position of the group in the hierarchy.
Description	A brief description about the group.

Button	Description
Add To group	Displays the Assign Groups page that you can use to add the user to a group.
Remove From Group	Removes the user from the selected group.

Contacts tab — Default Contact List

Name	Description
Description	A brief description of the contact list.

Contacts tab — Associated Contacts

Name	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Scope	The 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 cannot track the presence of the contact.

Button	Description
Edit	Displays the Edit Contact List Member page. Use this page to modify the information of the selected contact.
Add	Displays the Attach Contacts page. Use this page to select one or more contacts from the list of contacts. In the Multi Tenancy environment, when the tenant administrator of a tenant creates or updates the user, the administrator can attach only the following contacts: • Private contacts of the user • Public contacts • Users who belong to that tenant
Remove	Removes one or more selected contacts from the list of the associated contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.

Table continues…

Button	Description
Filter: Enable	Displays the text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab — Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

Name	Description
Last Name	The last name of the private contact.
First Name	The first name of the contact.
Display Name	The display name of the private contact.
Contact Address	The address of the private contact.
Description	A brief description about the contact.

Button	Description
Edit	Displays the Edit Private Contact page. Use this page to edit the information of the contact you selected.
New	Displays the **New Private Contact** page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Commit & Continue	Saves your changes and retains you on the same page for further modifications.
Commit	Modifies the user account and takes you back to the User Management or User Profile View page. **Note:** While restoring a deleted user, use the **Commit** button to restore a deleted user.
Cancel	Cancels the operation of modifying the user information and takes you back to the User Management or User Profile View page.

User Profile Duplicate field descriptions

Organization

Name	Description
Tenant	The name of the tenant that you must select.
Level 1	The name of the level 1 hierarchy of the tenant organization. For example, Site. The tenant administrator provides the hierarchy on the Tenant Management page.
Level 2	The name of the level 2 hierarchy of the tenant organization. For example, Department.
Level 3	The name of the level 3 hierarchy of the tenant organization. For example, Team.

User Provisioning Rule

Name	Description
User Provisioning Rule	The name of the user provisioning rule. You can provide only one user provisioning rule.

Note:

When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

Note:

You cannot edit the tenant. If you select a different level 1 for the tenant from the organization hierarchy, the **Level 2** and **Level 3** fields become blank. You can select new values for level 2 and level 3. If you select a different level 2 for the tenant from the organization hierarchy, the **Level 3** field becomes blank. You can select a new value for level 3.

Identity tab — Identity section

Name	Description
Last Name	The last name of the user. For example, Miller.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the end points. For example, Miller. Typically, the name is the written or spoken language of the user.

Table continues…

Name	Description
	Note: When you create a user, if the **Last Name (Latin Translation)** and **First Name (Latin Translation)** fields are: • Blank, the system displays the last name and first name in the fields. The values change when the last name and first names change. • Filled, the values remain even after you change the values in the **Last Name** and **First Name** fields.
First Name	The first name of the user. For example, John.
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Login Name	The unique system login name given to the user. The login name takes the form of username@domain. You use the login name to create the primary handle of the user. The login name is not case-sensitive. For example, if you enter JMILLER@AVAYA.COM, the system converts the login name to lowercase, that is, jmiller@avaya.com. However, on the login page, you can enter JMILLER@AVAYA.COM or jmiller@avaya.com. The login name can be in uppercase or lowercase. You cannot edit the **Login Name** field for users with the login name admin.
Authentication Type	Authentication type defines how the system performs user's authentication. The options are: • **Enterprise**: User's login is authenticated by the enterprise. • **Basic**: User's login is authenticated by an Avaya Authentication Service.
Password	Type your password for the duplicate profile.
Confirm Password	Retype your password for confirmation.
Localized Display Name	The localized display name of a user. It is typically the localized full name.

Table continues…

Name	Description
Endpoint Display Name	The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.
Title	The personal title for address a user. This is typically a social title and not the work title.
Language Preference	The user's preferred written or spoken language.
Time Zone	The preferred time zone of the user.
Employee ID	The employee number for the user.
Department	The department which the user belongs to.
Company	The organization where the user works.

Identity tab — Address section

Name	Description
check box	Use this check box to select the address.
Name	The unique label that identifies the address.
Address Type	The type of address. The values are: • Office • Home
Street	The name of the street.
City	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. In United States this is Zip code.
Province	The full name of the province.
Country	The name of the country.

Button	Description
New	Displays the Add Address page that you can use to add the address details.
Edit	Displays the Edit Address page that you can use to modify the address details.
Delete	Deletes the selected address.
Choose Shared Address	Displays the Choose Address page that you can use to choose a common address.

Identity tab — Localized Names section

Name	Description
Language	The the localized languages for displaying the user name.
Display Name	The user name in the localized language you choose.

Button	Description
New	Allows you to add a new localized name for the user.
Edit	Allows you to edit the localized name for the user.
Delete	Deletes the localized names you select for the user.
Add	Adds or edits the localized name for the user.
Cancel	Cancels your add or edit of the localized name.

Button	Description
Commit	Creates the duplicate user.
Cancel	Cancels the duplicate user creation and returns to the User Management page.

Communication Profile tab — Communication Profile section

Name	Description
Option button	Use this button to view the details of the selected communication profile.
Name	The name of the communication profile.

Button	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 **New** button in the Communication Profile section.

Name	Description
Name	The name of the communication profile of the user.
Default	The profile that is made default is the active profile. There can be only one active profile at a time.

Communication Profile tab — Communication Address section

Name	Description
Type	The communication protocol to be used for the user.
Handle	A unique communication address for the user.
Domain	The domain name with which the handle is registered.

Button	Description
New	Displays the fields for adding a new communication address.
Edit	Saves the changes that you made to the 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
Type	The type of the handle. The different types of handles are: • **Avaya SIP**: Indicates that the handle supports Avaya SIP-based communication. • **Avaya E.164**: Indicates 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. • **Microsoft SIP**: Indicates that the handle supports SIP-based communication. • **Microsoft Exchange**: Indicates that the handle is an email address and supports communication with Microsoft SMTP server. • **Lotus Notes**: Indicates that the handle is for Lotus Notes and domino calender. • **IBM Sametime**: Indicates that the handle is for IBM Sametime. The address must be in the DN=IBMHandle format. • **Avaya Presence/IM**: Indicates that the handle is an address that is used for Extensible Messaging and Presence Protocol (XMPP)-based Internet Messaging (IM) services, and XMPP or Session Initiation Protocol-based (SIP) Presence services.

Table continues…

Name	Description
	Note: To create the Presence communication profile, you must select **Avaya Presence/IM** and provide the communication address. • **GoogleTalk**: Indicates that the handle supports XMPP-based communication with the Google Talk service. • **Other Email**: Indicates that the handle is an email address other than MS Exchange email addresses. • **Other SIP**: Indicates that the handle supports SIP-based communication other than the listed ones. • **Other XMPP**: Indicates that the handle supports XMPP-based communication other than the listed ones. • **Work Assignment**: Indicates that the handle supports accounts which can be assigned to an agent for Work Assignment.
Fully Qualified Address	The fully qualified domain name or uniform resource identifier. The address can be an email address, IM user, or an address of a communication device by using which the user can send or receive messages. You must provide the fully qualified address.

Button	Description
Add	Saves the new communication address or modified communication address information in the database.
Cancel	Cancels the addition of communication address.

Communication Profile tab — Session Manager

Note:

The system displays the following fields only if a communication profile of the user exists for the product.

Name	Description
Primary Session Manager	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.

Table continues…

Name	Description
Secondary Session Manager	The secondary Session Manager instance that provides continued service to SIP devices associated with this Communication Profile when the primary Session Manager is unavailable. A selection is optional.
Origination Application Sequence	An Application Sequence that will be invoked when calls are routed from this user. A selection is optional. ✱ **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Termination Application Sequence	An Application Sequence that will be invoked when calls are routed to this user. A selection is optional. ✱ **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.
Survivability Server	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 is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to the Communication Manager survivable remote server resident with the Branch Session Manager. A selection is optional.

Table continues…

Name	Description
	✱ **Note:** If a termination or origination application sequence contains a Communication Manager application, Communication Manager associated with the application must be the main Communication Manager server for the Communication Manager survivable remote server that is resident with the Branch Session Manager.
Home Location	A Home Location to support mobility for the currently displayed user. Session Manager uses the home location when the IP address of the calling phone does not match any IP Address Pattern of any of the location.

Communication Profile tab: Engagement Development Platform Profile

Name	Description
Service Profile	The profile that you assign to the user. The user can gain access to the service contained in the profile.

Communication Profile tab — CM Endpoint Profile

✱ **Note:**

The system displays these fields only if a CM Endpoint profile exists for the user.

Name/Button	Description
System	The Communication Manager system on which you add the endpoint. You must select the system.
Use Existing Endpoints	Select the check box to use the existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint that you associate this profile with. You must select the extension. The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.
Template	The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add. You must select the template.

Table continues…

Name/Button	Description
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. You must select the port. The field lists the possible ports based on the selected set type.
Voice Mail Number	The voice mail number of the endpoint you associate with.
Preferred Handle	Numeric only handles, SIP handles, or nonSIP handles, that are administered for a user. The **Preferred Handle** field is optional. By default, the field is blank. If SIP entity is of Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
Calculate Route Pattern	The option to automatically select the route pattern based on the primary or secondary Session Managerconfigured in the **Session Manager Communication Profile**.
Sip Trunk	The system makes this field available only for the SIP set type. If you select **Calculate Route Pattern** check box, the system: • Populates the **Sip Trunk** field • Makes **Sip Trunk** field read-only.
Delete Endpoint on Unassign of Endpoint from User	The option to specify whether 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.
Override Endpoint Name	Use this check box for the following two purposes: • To override the endpoint name on Communication Manager with the value you configured on the Manage Users page during synchronization. If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization.

Table continues…

Name/Button	Description
	• To override the Localized Display Name on the Manager Users page on the **Localized Display Name** field of Communication Manager. If you clear the check box, the system does not override the Localized display name in the **Localized Display Name** field.
Allow H.323 and SIP Endpoint Dual Registration	The option to register both an H.323 endpoint and a SIP endpoint together at the same time to the same extension.

Communication Profile tab - CS1000 Endpoint Profile

Field	Description
System	The CS1000 system to which you want to add a phone.
Target	The system customer number for the Communication Server.
Template	The phone or endpoint template that you can choose for the user. Select a template from the drop down list. The element manager maintains all the templates.
Update	Updates the station profile information for the user. When you click this button, the system takes you to the element manager cut through for the updates.
Service Details	Displays service details of endpoints, such as set type, after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values for this field.
Include in Corporate Directory	Use to add this profile to the CS1K Corporate Directory feature.

Communication Profile tab — Messaging Profile

Note:

You may see these fields only if a messaging profile can be configured for the user.

Name	Description
System	The Messaging System on which you need to add the subscriber.
Template	The template (system defined and user defined) you want to associate with the subscriber.

Table continues…

Name	Description
Use Existing Subscriber on System	Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.
Mailbox Number	The mailbox number of the subscriber. The field lists the existing subscriber if you select the **Use Existing Subscriber on System** check box.
Password	The password for logging into the mailbox.
Delete Subscriber on Unassign of Subscriber from User	Use 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.

Communication Profile tab - CallPilot Messaging Profile

Field	Description
System	The CallPilot system to which you want to add a mailbox.
Location	This field maps to the CallPilot Location field. This field is provided by the CallPilot Manager.
Template	The mailbox template you want to apply. Select a template from the drop down list. The element manager maintains all the mailbox templates.
Update	Updates the mailbox information for the user. If you click this button, the system cuts through to the element manager for the updates.
Service Details	Displays mailbox service details from endpoint after you create the mailbox.
Mailbox Number	Mailbox number or the extension DN of the user.

Communication Profile tab — IP Office Endpoint Profile

Use this profile to assign a new or an existing user to a System Manager device in User Management.

While adding a user, if you choose to assign a CM endpoint profile and an IP Office endpoint profile to the user, then the system uses the IP Office endpoint profile as the survivability option for the CM endpoint profile. That is, the endpoint extension used in the CM endpoint profile is also used for creating an IP Office endpoint profile so that when Communication Manager is unavailable, the IP Office device can serve the extension.

Note:

If a Communication Manager endpoint profile is present while adding or editing a user, the user administration functions in the centralized mode. If a Communication Manager endpoint profile is present, the user administration functions in the distributed mode.

Commit the Communication Manager endpoint profile and the Session Manager endpoint profile before you add an IP Office endpoint profile for a centralized user.

Name/Button	Description
System	Displays a list of IP Office device names from which you can select the IP Office device you want to associate with the user.
Template	Displays a list of user templates from which you can select your preferred template to set the user configurations.
Use Existing Extension	Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint you want to associate. The field lists the endpoints, existing or available, based on option you selected in the **Use Existing Endpoints** check box.
Endpoint Editor button	Launches the IP Office application, where you can edit or view details of the IP Office endpoint. After you save the changes in IP Office, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Module-Port	The module port combination list for IP Office analog extensions. You must select **Module-Port** for centralized users with Set Type as **Analog**.
Set Type	Displays the set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the set type is auto populated.
Delete Extension On User Delete check box	Provides the option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with **Analog** and **Digital** set types.

Communication Profile tab — Presence Profile

Name	Description
System	The Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile: • Aggregate presence

Table continues…

Name	Description
	• Archive instant messages if the Instant Messages option is enabled
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with the AES Collector. The options are: • **System Default** • **Off** • **On** The default is **System Default**. You can change the default value. You do not require to configure AES Collector in the Presence Services server.

Communication Profile tab: Conferencing Profile

Name	Description
Select Auto-generated Code Length	The number of characters in PIN. The default is 6. The system displays this field if you select the **Auto Generate Participant and Moderator Security Code** check box.
Auto Generate Participant and Moderator Security Code	Select the check box if the system must generate the participant security code and moderator security code for this user. Clear the check box to assign a specific participant security code or moderator security code for this user.
Participant Security Code	The participant security code that you assign for this user. The system displays this field only when the **Auto Generate Participant and Moderator Security Code** check box is clear.
Moderator Security Code	The moderator security code that you assign for this user. The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Location	The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users. For SIP users, the system uses the location value from the **Home Location** field in the Session Manager profile.

Table continues…

Name	Description
Template	The Conferencing template that you assign to this user.

Button	Description
Get Templates	Displays the list of Conferencing templates that you can assign to this user.

Communication Profile tab: Work Assignment Profile

Name	Description
Account	The account name.
Account Address	The account address.
Source	The source name.
Source Address	The source address.

When you click **Resource Details**, **Account Details**, or **Source Details**, the system displays the Assignment Management page in Work Assignment.

Button	Description
Resource Details	Displays the Assignment Management page where you can configure assignment targets for the user. You can assign resource details to an agent only when the user has the Work Assignment profile assigned to the user.
Account Details	Displays the text box where you can add or modify the account name and account address. You can add attributes to the account only when the account is added to the agent.
Source Details	Displays the text box where you can add or modify the source name and source address. You can add properties and attributes to the source only when the source already exists.

Membership tab — Roles section

Name	Description
check box	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.
Name	The name of the role.
Description	A brief description about the role.

Button	Description
Assign Roles	Opens the Assign Role page that you can use to assign roles to the user account.
UnAssign Roles	Removes the selected role from the list of roles associated with the user account.

Membership tab — Group Membership section

Name	Description
check box	Use this check box to 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.

Button	Description
Add To group	Opens the Assign Groups page that you can use to add the user to a group.
Remove From Group	Removes the user from the selected group.

Contacts tab — Default Contact List

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.

Contacts tab — Associated Contacts

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
Edit	Opens the Edit Contact List Member page. Use this page to modify the information of the selected contact.
Add	Opens the Attach Contacts page. Use this page to select one or more contacts from the list of contacts.
Remove	Removes one or more contacts from the list of the associated contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab — Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

Name	Description
Last Name	Last name of the private contact.
First Name	First name of the private contact.
Display Name	Display name of the private contact.
Contact Address	Address of the private contact.
Description	A brief description about the contact.

Button	Description
Edit	Opens the Edit Private Contact page. Use this page to modify the information of the selected contact.
New	Opens the New Private Contact page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Commit & Continue	Duplicates the user account and retains you on the same page for further modifications.

Table continues…

Button	Description
Commit	Duplicates the user account and takes you to the User Management page.
Cancel	Cancels the operation of modifying the user information and takes you back to the User Management page.

User Delete Confirmation field descriptions

Name	Description
Last Name	The last name of the user.
First Name	The first name of the user.
Display Name	The localized display name of a user. It is typically the localized full name.
Login Name	The login name of the you want to delete.
Last login	The date and time of last successful login on to System Manager.

Button	Description
Delete	Deletes the user.
Cancel	Closes the User Delete Confirmation page and returns to the User Management page.

Assign Roles to Multiple Users field descriptions

Selected Users

Name	Description
Last Name	The last name of the user.
First Name	The first name of the user.
Display Name	The localized display name of the user.
User Name	The unique name that gives access to the system .
Last login	The time and date when the user has logged in to the system.

Select Roles

Name	Description
Select Check box	The option to select a role.

Table continues…

Name	Description
Name	The name of the role.
Description	A brief description about the role.

Button	Description
Commit	Assigns roles to the selected users.
Cancel	Cancels the role assignment operation and returns to the User Management page.

Assign Roles field descriptions

Selected Roles

The 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	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	The option to select all the roles in the table.
Name	The roles that you can assign to the user account.
Description	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

Selected Groups

The section displays groups that are assigned to the user.

Name	Description
Name	The name of the group.

Table continues…

Name	Description
Type	The group type based on the resources.
Hierarchy	The position of the group in the hierarchy.
Description	A brief description of the group.

Available Groups

The table in this section displays groups that you can assign to the user account.

Name	Description
Select check box	The option to select a group.
Name	The name of the group.
Type	The group type based on the resources.
Hierarchy	The position of the group in the hierarchy.
Description	A brief description of the group.

Button	Description
Select	Assigns the selected groups to the user.
Cancel	Cancels the group assignment operation.
Select: ALL	Selects all groups in the table.
Select: None	Clears the selection.

Assign Groups to Multiple Users field descriptions

Use this page to add users to a group.

Selected Users

Name	Description
Last Name	The last name of the user.
First Name	The first name of the user.
Display Name	The localized display name of the user.
User Name	The unique name that gives access to the system.
Last login	The time and date when the user last logged on to the system.

Select Groups

Name	Description
Select check box	The option to select a group.
Name	The name of the group.

Table continues…

Name	Description
Type	The group type based on the resources.
Hierarchy	The position of the group within the groups.
Description	A brief description of the group.

Button	Description
Select: All	Selects all groups displayed in the table.
Select: None	Clears the selected check boxes.
Commit	Assigns groups to the selected users.
Cancel	Cancels the group assignment operation and returns 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
Select check box	The option to select a group.
Last Name	The last name of the deleted user.
First Name	The first name of the deleted user.
Display Name	The localized display name of the deleted user.
Login Name	The unique name that identifies the user in the system.
Organization Hierarchy	The hierarchy of the tenant organization in the format Tenant/Site/Department/Team. For example, Citi/Pune/HomeLoans/LoanSupport. **Note:** The system displays the field only when the administrator enables the Multi Tenancy feature.
Last login	The time and date when the user last logged on to the system.

Button	Description
Delete	Deletes the user permanently from the database.
Restore	Restores the deleted user.
Show Regular users	Returns to the User page and displays the active users.

User Restore Confirmation field descriptions

Use this page to restore a deleted user.

Name	Description
Last Name	The last name of the user.
First Name	The first name of the user.
Display Name	The localized display name of the user.
Login Name	The unique name of the user account.
Organization Hierarchy	The hierarchy of the tenant organization in the format Tenant/Site/Department/Team. For example, Citi/Pune/HomeLoans/LoanSupport. **Note:** The system displays the field only when the administrator enables the Multi Tenancy feature.
Last login	The date and time when the user last logged on to the system.

Button	Description
Restore	Removes the user from the list of deleted users and restores the user as an active user.
Cancel	Closes the User Restore Confirmation page and returns you back to the Deleted Users page.

Assign Users To Roles field descriptions

Use this page to assign one or more users to the selected roles. This page has the following two sections:

- Selected Roles
- Select Users

Selected Roles section

The roles to which you can assign users.

Name	Description
Name	Displays the name of the role.
Resource Type	Displays the resource type that the corresponding role is assigned.
Description	Displays a brief description about role.

Select Users section

The table displays the users to which you can assign the roles.

Name	Description
Select check box	Provides the option to select the user.
Last Name	Displays the last name of the user.
First Name	Displays the first name of the user.
Display Name	The display name of the user.
User Name	Displays the unique name that identifies the user.
Last Login	Displays the time and date when the user last logged on to the system.

Button	Description
Commit	Assigns user to the role.
Cancel	Cancels the assign users operation and returns to the Manage Roles page.

UnAssign Roles field descriptions

Selected Roles

The role from which users are unassigned.

Name	Description
Name	The name of the role.
Resource Type	The resource type that the role is assigned.
Description	A brief description of the role.

Select Users

The table displays the users for which you can remove the roles.

Name	Description
Select check box	The option to select the user.
Last Name	The last name of the user.
First Name	The first name of the user.
Display Name	The display name of the user.
User Name	The unique name that identifies the user.
Last Login	The time and date when the user last logged on to the system.

Button	Description
Commit	Unassigns the role from the users.
Cancel	Cancels the assign users operation and returns to the Manage Roles page.

Managing bulk import and export

Bulk import and export

In System Manager, you can bulk import and export user profiles and global settings. To import data in bulk, you must provide an XML file or an Excel file as input file. The system exports the data to an XML file and an Excel file. The System Manager database stores the imported user profiles and global settings data.

You can import and export the following user attributes in bulk:

- Identity data
- Communication profile set
- Handles
- Communication profiles

  The supported communication profiles are CM Endpoint, CM Agent, Messaging, Session Manager, CS 1000 Endpoint, CallPilot Messaging, Conferencing, IP Office, Presence, Engagement Development Platform, and Work Assignment.

You can import and export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- Default access control list (ACLs)

! **Important:**

System Manager does not support import and export of roles in bulk.

Bulk import and export using the Excel file

In System Manager, you can import and export user profiles in bulk by using an Excel file and an XML file. To import data in bulk, provide an XML file or an Excel file as input that System Manager supports. When you export the data from the System Manager web console, the system exports the data to an XML file and an Excel file that System Manager supports.

Microsoft Office Excel 2007 and later support bulk import and export in the `.xlsx` format. You can download the Excel file from the User Management page.

Import and export in bulk by using the Excel template provides the following features:

- Supports the following types of user information:
  - Basic. The identity attributes of the user that include user provisioning rule name for the user, the tenant, and organization hierarchy details

- - Profile Set. Entries for all communication profile sets for all users

    The Profile Set sheet contains an entry for each communication profile set for a user. The user must set only one communication profile set as true for a user in the **Is Default** column. The value true indicates that the communication profile set of the user is default
  - Handle. The communication address of the user
  - Session Manager profile
  - Engagement Development Platform profile
  - CM Endpoint profile with all attributes of the station communication profile
  - CM Agent profile with all attributes.
  - Messaging profile
  - CallPilot profile
  - IP Office Endpoint profile
  - CS 1000 Endpoint profile
  - Presence profile
  - Conferencing profile
  - Work Assignment profile
- Supports more than one communication profile set.
- Supports the creation, updation, and deletion of the user using the same Excel file. However, you can perform one operation at a time.
- For updation, supports only the partial merge operation.

  Bulk import and export by using Excel does not support complete or partial replace of the user for imports in bulk.

Bulk import and export by using Excel supports a subset of user attributes that XML supports. For example, Excel does not support user contacts, address, and roles.

The Excel file

The sample Excel file contains the sample data of some key attributes of the user. The Excel file provides a description of header fields. When you download the Excel template from the User Management page, the values remain blank. To use the Excel file, export some users for reference in an Excel file.

The login name in the **Basic** worksheet is the key attribute that you use to link the user records in other worksheets.

The login name of the user and the profile set name in the **Profile Set** worksheet are used as key to link to the user records in other worksheets for that user profile.

- Although you can edit the header fields in the Excel template, do not change any details of any headers in the worksheets. The import or export might fail if you change the details of the header.
- Do not change the column position in the Excel file or change the structure of the Excel template.

- Do not sort the data in worksheets.

CM Endpoint communication profile

The Excel file contains all attributes for the CM station endpoint profile that are spread in different worksheets. The parent sheet provides a link to the same user profile record in the child worksheet. The link points to the first record in the child sheet if the user profile contains multiple records in the child worksheet.

Related links

Downloading the Excel template file on page 326
Microsoft Excel data link error on page 322
Examples of bulk import and export of user by using the Excel file on page 319
Hierarchy in communication profile worksheets on page 321

Examples of bulk import and export of user by using the Excel file

The following are the credentials of John Miller, a user with two communication profile sets:

- Login name: johnmiller@avaya.com
- Name of the default communication profile set: Primary
- Name of the nondefault communication profile set: secondaryProfile

Example of navigation across Excel worksheets

In the exported file, you can use the hyperlink to navigate across worksheets to access various records for a profile data of a user.

In the **CM Endpoint Profile** worksheet, the **Station Site Data** and **Buttons** columns contain hyperlinks to navigate to the respective worksheets. If the child worksheet, for example, **Buttons** contains only one record in the worksheet for that user profile, the link points to the corresponding record of the user profile. If the child worksheet contains multiple records for that user profile, the link points to the first record in the list.

Login Name*	....	Station Site Data	Abbr List	Buttons
johnmiller@avaya.com#Primary	....	Go to Station Site Data worksheet		Go to Buttons worksheet

In the following **Station Site Data** worksheet, the link points to the corresponding user profile record of the child worksheet because this child worksheet contains only one record for that user profile.

Login Name*	Room	Jack	Cable	Floor	Building	Headset	Speaker	Mounting	Cord Length	Set Color	
johnmiller@avaya.com#Primary						false	false	d	0		

The following **Buttons** worksheet contains multiple records for johnmiller@avaya.com#Primary, the user profile, but the link points to the first record in the list.

Login Name*	Number*	Type*	Data1	Data2	Data3	Data4	Data5	Data6
johnmiller@avaya.com#Primary	1	call-appr						
johnmiller@avaya.com#Primary	2	call-appr						
johnmiller@avaya.com#Primary	3	call-appr						

Example of handling multiple communication profile sets for a user

In the exported Excel file, the system appends the login name with #profileSetName in all worksheets except the **Basic** and **Profile Set** worksheets. Appending the profile set name to the login name associates the communication profile set with the user record, for example, jmiller@avaya.com#profileSetName. When you export users in the Excel file, the association is automatic. When you provide data in a blank Excel template that you downloaded for import, you must make the association manually.

Note:

The **Profile Set** worksheet must contain all communication profile sets of a user, but only one communication profile set can be the default. The **Is Default** column is set to `true` only for the default profile.

In the **Profile Set** worksheet, the two communication profile sets for the user John Miller must contain the following information:

Login Name*	Name*	Is Default*
johnmiller@avaya.com	secondaryProfile	false
johnmiller@avaya.com	Primary	true

If a SIP e164 handle is associated with secondaryProfile of John Miller, the **Handle** worksheet must contain the following information:

Login Name*	Handle*	Type*	Sub Type	Domain
johnmiller@avaya.com#secondaryProfile	+1123	sip	e164	smgrdev.avaya.com

If a Session Manager communication profile is associated with secondaryProfile of John Miller, the **Session Manager Profile** worksheet must contain the following information:

Login Name*	Type*	Session Manager	Session Manager	Termination Application Sequence	Origination Application Sequence	Conference Factory Set	Survivability Server	Home Location*	Max. Simultaneous Devices	Block New Registration When Max Active	Enable Disable Call Log
johnmiller@avaya.com#secondary Profile	Session Manager	sm6						Pune	6	false	true

If a Engagement Development Platform communication profile is associated with Primary for John Miller, the **CE Profile** worksheet must contain the following:

Login Name*	Type*	Service Profile*
johnmiller@avaya.com#Primary	AUS	TempProfile

Hierarchy in communication profile worksheets

The table provides the parent-child relation of communication profile worksheets in the Excel template for bulk import and export of user.

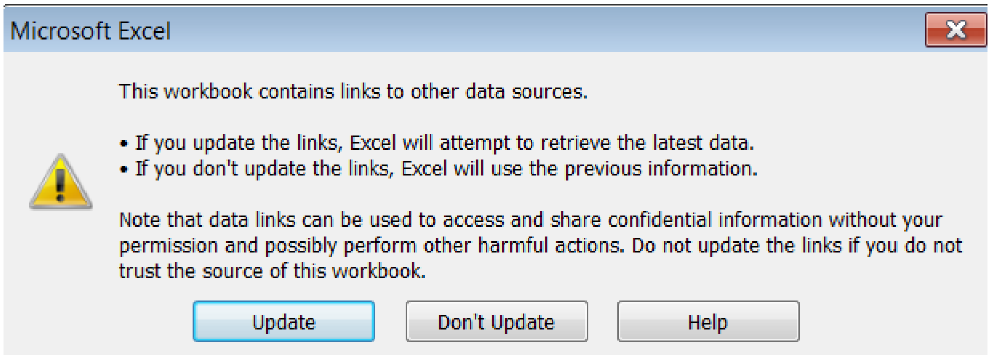
Element	Master worksheet	Child worksheets
Session Manager	Session Manager Profile	None
Communication Manager	CM Endpoint Profile	• Station Site Data • Buttons • Feature Buttons • Expansion Module Buttons • Soft Keys • Display Buttons • Station Abbr Dialing Data • Station Data Module • Station Hot Line Data • Native Name Data
Messaging	Messaging Profile	None
Conferencing	Conferencing Profile	None
IP Office	IP Office Endpoint Profile	None

Table continues…

Element	Master worksheet	Child worksheets
CS 1000	CS 1000 Endpoint Profile	None
Engagement Development Platform	CE Profile	None
CallPilot	CallPilot	None
Presence	Presence Profile	None

Microsoft Excel data link error

Microsoft Excel 2010 displays a data link error.


Microsoft Excel

This workbook contains links to other data sources.

- If you update the links, Excel will attempt to retrieve the latest data.
- If you don't update the links, Excel will use the previous information.

Note that data links can be used to access and share confidential information without your permission and possibly perform other harmful actions. Do not update the links if you do not trust the source of this workbook.

Related links

Proposed solution on page 322

Proposed solution

About this task

You can ignore Data link error that Microsoft Excel 2010 displays. However, perform the following procedure to avoid this error the next time you open an Excel file.

Procedure

1. On the Excel worksheet, close the warning message.
2. On the **Data** menu, click **Edit Links**.
3. On the Edit Links dialog box, click **Startup Prompt**.
4. Click **Don't display the alert and don’t update automatic links** and click **OK**.
5. Click **Close**.
6. Save the Excel file.
7. Close the Excel file and open the file again.

   The system does not display the data link error message now.

Related links

Proposed solution on page 322

Data entry warning in Microsoft Excel

The data type of the cell in Excel is text. If you provide a number in the cell, Excel displays the `Number Stored as Text` message. Ignore the warning and do not change the data type of the cell.

Related links

Proposed solution on page 323

Proposed solution

About this task

You can ignore data entry warning that Microsoft Excel 2007 or later displays. However, perform this procedure to turn off the warning message.

Procedure

1. Based on the version, do one of the following:
    - In Microsoft Office Excel 2007, click **Excel Options**.
    - In Microsoft Office Excel 2010, click **File** > **Options** > **Excel Options**.

    For other Microsoft Office Excel versions, use the appropriate options.
2. In Microsoft Office Excel 2010, in the left navigation pane, click **Formulas** and clear the **Numbers formatted as text or preceded by an apostrophe** check box.
3. Click **OK**.

Key features of bulk import and bulk export

- Supports import of user profiles from an XML file and Excel file, and import of global settings from an XML file. Also, supports the export of data to an XML file and Excel file.
- Supports the following error configurations:
    - Abort on first error. Stops the import of user records when the import user operation encounters the first error in the import file containing the user records.
    - Continue processing other records. Imports the next user record even if the import user operation encounters an error while importing a user record.
- Supports the following import types:
    - A *Partial Import* type helps import of users with specific user attributes.
    - A *Complete Import* helps import of users with all user attributes.
- Provides various configuration options if a record that you must import matches an existing record in the database. You can configure to skip, replace, merge, or delete a matching record that already exists and reimport data.
- Supports scheduling of bulk import jobs from System Manager Web Console.
- Displays import job details, such as job scheduled time, job end time, job status, job completion status in percentage, number of user records in the input file, number of user records in the

input file with warnings, and number of user records in the input file that failed to import. Also, provides the link to the Scheduler user interface.

- Supports cancellation and deletion of an import job.
- Maintains logs of records that fail to import and that require manual intervention.
- Supports download of failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and reimport the records into the database.

About bulk import of users

You can use the bulk import functionality to import users in bulk with their attributes from an XML file. The XML file must conform to XML schema definition. For more information, see XML Schema Definition for bulk import of users on page 348. See Sample XML for bulk import of users with all attributes on page 355 for the sample XML file for bulk import of user.

You can perform the following tasks with the bulk import functionality:

- Abort or continue the import process when the import user operation encounters first error in the user input file.
- Perform the following import types:
  - A *Partial* import type helps import of users with specific user attributes.
  - A *Complete* import type helps import of users with all user attributes.
- Skip import of the users that already exist in the database. Use this option to import new users from the XML file.
- Replace the users in the database with the new users from the file you imported. The system performs the following actions:
  - Replaces all items of user collection attributes such as CommprofileSet and Contactlist.
  - Removes the existing items.
  - Adds the new items from the XML.
  - Updates the single-value user attributes.

  For example, the user John Miller has StationA and EndpointB as existing commprofiles in default commprofileset and you import an XML file containing users with StationC and EndpointB with *Replace* option. After you import, John Miller has commprofiles StationC and EndpointB in the default commprofileset.

  Note:

  For CS1000 Endpoint Profile and CallPilot Messaging Profile, you cannot import both communication profile and user at the same time. You must add the user and then merge the profile.
- Update and merge the user attributes data from the imported file to the existing data. The system performs the following actions:
  - Merges items of user collection attributes such as CommprofileSet and Contactlist.

  - Retains and updates the existing items.
  - Adds the new items from the XML.
  - Updates the single-value user attributes.

  For example, the user John Miller has StationA and EndpointB as existing commprofiles in default commprofileset and you import an XML file containing users with StationC and EndpointB with *Replace* option. After you import, John Miller has commProfiles StationA, StationC, EndpointB in the default commprofileset.

- Delete the user records from the database that match the records in the input XML file.
- Schedule the bulk import job.
- View the details of an import job:
  - Job scheduled time
  - Job end time
  - Job status
  - Job completion status in percentage
  - Total number of user records in the input file
  - Total number of user records with warnings in the input file
  - Total number of user records that fail to import in the input file
  - The link to the Scheduler user interface
- Cancel or delete an import job.
- View logs of records that fail to import and require manual intervention.
- Download failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and import the records again to the database.

The following two XML schema definitions are available based on the complete and partial import types:

- XML schema definition for bulk import of users: See XML Schema Definition for bulk import of users on page 348. Use this XML schema definition to add and update (Merge/Replace) users. This schema addresses complete user attributes. For a sample XML that conforms to the XML schema definition, see Sample XML for bulk import of users with minimal attributes on page 355 and Sample XML for bulk import of users with all attributes on page 355.
- XML schema definition for partial import of users: See XML Schema Definition for partial import of user attributes on page 363. Use the XML schema definition to add and update (Merge/Replace) users. You must use this schema to import users with specific user attributes. For a sample XML that conforms to this XML schema definition, see Sample XML for partial import of user attributes on page 365.

To delete bulk users, a separate XML schema definition is defined. See XML Schema Definition for bulk deletion of users on page 367. For a sample XML that conforms to delete bulk users XML schema definition, see Sample XML for bulk deletion of users on page 368.

Configuration options for bulk import using Excel

You can bulk import only the supported user attribute data for users. The Excel file must be the downloaded Excel template file or exported Excel file.

The following configuration options are available for import of users by using the Excel file:

- Abort or continue the import process when the import user operation encounters first error in the user input file.
- Import users with specific or all user attributes that Excel supports.
- If a matching record already exists, you can:
  - Merge the user attribute data from the imported file to the existing data. For example, you can add a new handle to the existing user.
  - Delete the user records from the database that match the records in the input Excel file.
- Schedule the bulk import job.
- View the details of an import job:
  - Job scheduled time
  - Job end time
  - Job status
  - Job completion status in percentage
  - Total number of user records in the input file
  - Total number of user records with warnings in the input file
  - Total number of user records that fail to import in the input file
  - The link to the Scheduler user interface
- Cancel or delete an import job.
- View logs of records that fail to import and require manual intervention.

Downloading the Excel template file

About this task

To import or export by using an Excel file, you must use the Excel template file that System Manager supports. System Manager validates and displays a message if you use an unsupported Excel file.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **More Actions** > **Download Excel Template**.
4. In the Opening <Excel template file name>.xlsx dialog box, click **Save File**, and click **OK**.

Important:

Though the header fields in the Excel template are editable, do not change any header information in the worksheets. The import or export might fail if you modify the headers.

For the sample Excel template, see the Excel template for bulk import and export that you download from the User Management page.

About bulk export of users

In System Manager, you can export users in bulk from the System Manager database. While exporting in bulk, the system exports the data to an XML file.

You can export the following user attributes in bulk:

- Identity data
- Communication profile set
- Handles
- Communication profiles

  The supported communication profiles are CM Endpoint, CM Agent, Messaging, Session Manager, CS 1000 Endpoint, CallPilot Messaging, Conferencing, IP Office, Presence, Engagement Development Platform, and Work Assignment.

Note:

For security reasons, the system does not export the password fields in the XML file.

You can export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- Default access control list (ACLs)

The Export User process creates an archive file containing one or more XML files. While exporting users records, if the number of exported records exceed the limit of records that an XML file can hold, the system creates multiple XML files. The system packages the XML files in a zip file.

The XML file conforms to the XML schema definition that supports import of user. This schema addresses the complete user attributes, for more information, see XML Schema Definition for bulk import of users on page 348.

The system generates the XML file on the System Manager server. You can specify the location of the file you want to export while running the Export User job.

You can schedule an export user job. The job parameter provides an option to specify the schedule time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.

When you import the same file to a new system, you must provide the password for users with the *system administrator* role. For security reasons, the system does not export the **Password** fields to the XML file. Therefore, import of users with the *system administrator* role fails.

To import users with the *system administrator* role, in the XML file for the users, add the following XML tag after the `<username>` tag:

```
<userPassword> provide password for user </userPassword>
```

The system imports the other user records with non system administrator roles and automatically sets the password to `Avaya123$` for **Complete Merge/Replace** import type. For **Partial Merge/Replace** import type, if you do not specify the password, the existing password remains.

You can export user data in bulk from System Manager web console and by using the bulk export that you run from CLI. The utility is in the `$MGMT_HOME/bulkadministration/exportutility` directory, where *MGMT_HOME* is an environment variable that represents the System Manager HOME path.

Exporting users in bulk from web console

About this task

Important:

The system runs the export users job that you schedule only once. To export users the next time, you must create a new export job by using this procedure. You cannot reschedule an existing export job.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. On the User Management page, click one of the following:
   - **More Actions** > **Export All Users** to export user records for all users.
   - **More Actions** > **Export Selected Users** to export user records for the users that you select.

     Note:

     - If you select specific users from the list and click **Export All**, the system exports the records of all users instead of the selected records.
     - If you provide the criteria in **Advanced Search** and click **Export All**, the system exports only the records that match the criteria.
3. **(Optional)** On the Export Users page, in the User Attribute Options section, select one or more check boxes to export contacts and specific communication profiles.

   By default, the system exports basic attributes, communication profiles, and contacts.

   For more information, see Export Users field descriptions.
4. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.

   For more information, see Export Users field descriptions.

> ❗ **Important:**
>
> The export users job that you schedule runs only once. To export users the next time, you must create a new export job by using this procedure. You cannot reschedule an existing export job.

5. Click **Export** to complete the export operation.

   The system exports the user data to the XML and Excel file.

6. To view the data, in the **Export List** section, click the link in the **Download File** column.

   To use the exported excel file for operations such as reimporting, while exporting users from the Export Users webpage, clear the **Contacts** checkbox in User Attribute Options. Excel export or import operations does not support export or import of contacts that are associated with the user.

Related links

About bulk export of users on page 327
List of XML Schema Definitions and sample XMLs for bulk import on page 347
exportUpmGlobalsettings.sh command on page 343
Attribute details defined in Import user XSD on page 459
Attribute details defined in Delete User XSD on page 467
Attribute details defined in the CM Endpoint profile XSD on page 468
Attribute details defined in the Messaging communication profile XSD on page 491
Attribute details defined in the Session Manager communication profile XSD on page 499
Export Users field descriptions on page 511
Downloading the Excel template file on page 326
Microsoft Excel data link error on page 322
Bulk importing of users

Configuration options for bulk import of users

You can bulk import only the selected user attributes data for one or more users existing in the database. The XML file must conform to XML schema definition, for more information, see XML Schema Definition for partial import of users on page 363. For a sample XML file for import of user, see Sample XML for partial import of users on page 365.

The following configuration options are available for import of users:

- Abort or continue the import process when the import user operation encounters first error in the user input file.
- Perform one of the following import types:
  - The partial import type. Helps import of users with specific user attributes.
  - The complete import type. Helps import of users with all user attributes.
- If a matching record already exists, you can:
  - Replace the users in the database with the new users from the file you imported. For example, you can replace the existing contact list for a user with a new contact list.

  - Merge the user attributes data from the imported file to the existing data. For example, you can add a new contact in the list of contacts for the user and update the name of the user.
  - Delete the user records from the database that match the records in the input XML file.
- Schedule the bulk import job.
- View the details of an import job:
  - Job scheduled time
  - Job end time
  - Job status
  - Job completion status in percentage
  - Total number of user records in the input file
  - Total number of user records with warnings in the input file
  - Total number of user records that fail to import in the input file
  - The link to the Scheduler user interface
- Cancel or delete an import job.
- View logs of records that fail to import and require manual intervention.
- Download failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and import the records again to the database.

Bulk importing of partial user attributes for a user

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import** > **User Management** > **Users**.

   Also, to gain access to **Import users**, from the System Manager web console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import users page, in the **Select Import File Type** field, select one of the following file types:
   - XML
   - Excel

     Note:

     Use the Excel template that System Manager supports. If you use an unsupported template, the system displays a message `<file_name>.xlsx file is not a valid excel template for the current System Manager release. Use the Excel template that you downloaded or exported from the current System Manager release.`

4. Select one of the following error configuration options:
   - **Abort on first error**
   - **Continue processing other records**
5. Select **Partial** as the import type.
6. Select one of the following options to handle matching records:
   - To replace the existing attribute data of a matching user in the database with the new data from the imported file, click **Replace**.
   - To update and merge the user attributes data from the imported file to the existing data, click **Merge**.
7. To run the job, in the Job Schedule section, select one of the following:
   - To import the users immediately, click **Run immediately**.
   - To import the users at a specified time, click **Schedule later**, and set date and time.
8. Click **Import**.

Related links

About bulk import of users on page 324
List of XML Schema Definitions and sample XMLs for bulk import on page 347
Attribute details defined in Import user XSD on page 459
Attribute details defined in Delete User XSD on page 467
Attribute details defined in the CM Endpoint profile XSD on page 468
Attribute details defined in the Messaging communication profile XSD on page 491
Attribute details defined in the Session Manager communication profile XSD on page 499
Configuration options for bulk import of users on page 329

Making exported user data compatible for partial user import

Use this section to update user attributes partially. XML file format contains the user records that System Manager exports. You must update selected user attributes in the exported XML file and then import the XML file. You require this procedure because export users generate XML file conforming to this XML Schema Definition. For more information, see XML Schema Definition for bulk import of users on page 348. Partial import type uses a different XML schema definition, for more information, see XML Schema Definition for partial import of user attributes on page 363.

Before you begin

Export the users in bulk and generate the XML file.

About this task

For partial import of users, make the following changes in the user export XML file. You can generate the XML file by exporting users in bulk.

Procedure

1. 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 modify the XML file as instructed in Step b through Step e, the content 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 instances of:

    - `<tns:user>` with `<tns:userDelta>`
    - `</tns:user>` with `</tns:userDelta>`
    - `<tns:users>` with `<tns:deltaUserList>`
    - `</tns:users>` with `</tns:deltaUserList>`

Next steps

You can now make the updates in the XML file and import the changes to update the user attributes in the database.

About Bulk Import Encryption utility

System Manager Import User supports import of encrypted user password field and the plain text Communication Profile password field into the database. For importing a user XML file with encrypted password, System Manager provides BulkImportEncryptionUtil, a utility tool that encrypts the “userPassword” and “commPassword” fields in the user import input file.

The utility tool takes an XML file with plaintext password field values as input. This utility encrypts the password fields and generates an XML file with encrypted password field. You can use the XML file to import user.

BulkImportEncryptionUtil is a standalone Java program. You can run the utility on any machine that has Java installed on it.

Encrypting passwords in user import file using BulkImportEncryptionUtil running on Windows

Before you begin

JDK 1.6 is 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.

Procedure

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. At the command prompt, 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, the *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 ">
     ```

Related links

About Bulk Import Encryption utility on page 332

Encrypting passwords in user import file using BulkImportEncryptionUtil running on Linux

Before you begin

Install JDK 1.6 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.

Procedure

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. At the command prompt, 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, the *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 ">
     ```

Related links

About Bulk Import Encryption utility on page 332

Import user considerations

- If the comprofileset has associated handlelist or commprofilelist, you cannot merge or replace commprofileset attributes name and Isprimary.

  To move handlelist and commprofilelist from one commprofileset to another, perform the following:

  1. Perform Replace - Import file with no commprofileset.
  2. Perform Update (merge/replace) - Import file with the new commprofileset with associated handlelist and commprofiles.
- For security reasons, you do not export the **Password** fields in the XML file.

  When you import the same file to a new system, you must provide the password for users with the *system administrator* role. For security reasons, the system does not export the **Password** fields to the XML file. Therefore, import of users with the *system administrator* role fails.

  To import users with the *system administrator* role, in the XML file for the users, add the following XML tag after the `<username>` tag:

  ```
  <userPassword> provide password for user </userPassword>
  ```

  For **Complete Merge/Replace** import type, the system imports user records with nonSystem Administrator roles and automatically sets the password to `Avaya123$`. For **Partial Merge/Replace** import type, if you do not specify the password, the existing password remains.
- To enhance the performance of a file with large user records, split the file into smaller file sizes. For example, you can split a user import file of 15 Kb into three files of 5 Kb each. To speed up the import process, schedule three import jobs in parallel. System Manager does have the ability to process multiple files concurrently.

Scheduling a user import job

System Manager supports scheduling of bulk import jobs from the System Manager console. You can schedule a job to run immediately or at a later time.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import** > **User Management** > **Users**.

   Also, to gain access to **Import users**, from the System Manager web console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import users page, in the **Select Import File Type** field, select one of the following file types:
   - XML
   - Excel

Note:

Use the Excel template that System Manager supports. If you use an unsupported template, the system displays a message `<file_name>.xlsx file is not a valid excel template for the current System Manager release. Use the Excel template that you downloaded or exported from the current System Manager release.`

4. Select one of the following error configuration options:
   - **Abort on first error**
   - **Continue processing other records**
5. Select one of the following import options:
   - To skip users in the import file that match the existing user records in the database, click **Skip**.
   - To replace the users in the database with new users from the imported file, click **Replace**. Use this option to import new users and retain the existing users.

     If you select Excel file type, the system does not display the replace option
   - To update and merge the user attributes data from the imported file to the existing data, click **Merge**.
   - To delete the user records in the database that match the records in the imported file, click **Delete**.

     Note:

     For import by using Excel, the system deletes the user records permanently.
6. In the Job Schedule section:
   1. Click **Schedule later**.

      To run the user import job immediately, click **Run immediately**. When you select this option, the fields related to scheduling become unavailable.
   2. In the **Date** field, type the date.

      You can use the calendar icon to select a date.
   3. In the **Time** field, type the time in the HH:MM:SS format.
   4. In the **Time Zone** field, type the time zone.
7. Click **Import**.

   The page displays the scheduled job in the Manage Jobs section.

Aborting a user import job on first error

System Manager supports the following error configurations:

- Abort on first error: Aborts import of the user records when the import user operation encounters the first error in the import file containing the user records.

- Continue processing other records: Imports the next user record even if the import user operation encounters an error while importing a user record.

About this task

The user import process may encounter errors at the time of importing of users. Use this feature to configure actions when you encounter the first error. You can choose to abort the user import process or continue the import process.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import** > **User Management** > **Users**.

   Also, to gain access to **Import users**, from the System Manager web console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import users page, in the **Select Import File Type** field, select one of the following file types:
   - XML
   - Excel

   Note:

   Use the Excel template that System Manager supports. If you use an unsupported template, the system displays a message `<file_name>.xlsx file is not a valid excel template for the current System Manager release. Use the Excel template that you downloaded or exported from the current System Manager release.`
4. Click **Abort on first error** to choose error configuration options.
5. Select one of the following import options:
   - To skip users in the import file that match the existing user records in the database, click **Skip**.
   - To replace the users in the database with new users from the imported file, click **Replace**. Use this option to import new users and retain the existing users.

     If you select Excel file type, the system does not display the replace option
   - To update and merge the user attributes data from the imported file to the existing data, click **Merge**.
   - To delete the user records in the database that match the records in the imported file, click **Delete**.

   Note:

   For import by using Excel, the system deletes the user records permanently.
6. Choose or enter the appropriate information for remaining fields.
7. Click **Import**.

Canceling a user import job

You can cancel a job only when the job is in the PENDING EXECUTION or RUNNING state.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import** > **User Management** > **Users**.

   Also, to gain access to **Import users**, from the System Manager web console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import Users page, select the job from the table in the Manage Jobs section.
4. Click **Cancel job**.

Deleting a user import job

System Manager supports deleting of jobs. **Delete job** option removes the job information from the database.

About this task

You can delete a job only when the status of the job is SUCCESSFUL. To interrupt a job that is running or pending, use the **Cancel job** option.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import** > **User Management** > **Users**.

   Also, to gain access to **Import users**, from the System Manager web console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import Users page, select the job to delete from the table in the Manage Jobs section.
4. Click **Delete job**.

Viewing a user import job on the Scheduler page

You can view an import job on the Scheduler Web page. You can perform all operations on a job that Scheduler supports from the Scheduler page.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import** > **User Management** > **Users**.

   Also, to gain access to **Import users**, from the System Manager web console, click **Users** > **User Management**. Click **Manage Users** and select **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 **Job Name** column.

The Scheduler page displays the details of the job. You can perform operations on the job that the Scheduler supports for the job.

Viewing the details of a user import job

You can view the following details of an import job:

- Job name
- Job scheduled by
- Job scheduled start time
- Selected error configuration option
- Selected import type option
- Selected import option
- Job end time
- Job status
- Import file name
- Total number of user records in the import file
- Total number of user records successfully imported
- Total number of user records that failed to import
- Total number of warnings
- Percentage complete status

About this task

You can view the error message for each user record that fails to import. You can download the failed user records in an XML file format. You can modify the XML file and import the file again.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import** > **User Management** > **Users**.

   Also, to gain access to **Import users**, from the System Manager web console, click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Users**.
3. On the Import Users page, select a job to view from the table in the Manage Jobs section.
4. Click **View job**.

   The Job Detail page displays the details of the selected job.

Bulk import of global user settings

You can use the *Import Global Settings* functionality to import global settings in bulk from an XML file. The XML file must conform to XML schema definition, for more information, see XML Schema Definition for bulk import of global setting records on page 442. For sample XML file for import global settings, see Sample XML for bulk import of global setting records on page 449.

You can perform the following tasks with Import Global Settings:

- 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 to import new global user settings records and retain the existing users.
- Update and merge the global user settings attributes data from the imported file to the existing data in the attributes.
- Replace all the global user settings records in the database with the global user settings records from the imported file.
- Delete the global setting records from the database that match the records in the input XML file.
- Schedule the bulk import job.
- View the details of an import job:
  - Job scheduled time
  - Job end time
  - Job status
  - Job completion status in percentage
  - Total number of global settings records in the input file
  - The number of global settings records with warnings in the input file
  - The number of global settings records fail to import in the input file
  - The link to the Scheduler user interface
- Cancel or delete an import job.
- View logs of records that fail to import and require manual intervention.
- Download failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and import the records again to the database.

To add and update (Merge and Replace) global settings use XML Schema Definition for bulk import of global setting records on page 442.

To delete bulk global settings, use the XML schema definition for global settings delete, see XML Schema Definition for bulk deletion of global setting records on page 453. For a sample XML conforming to delete bulk global settings XML schema definition, see Sample XML for bulk deletion of users on page 368.

Bulk importing the global user settings

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.

3. On the Import Global Settings page, enter the complete path of the file in the **Select file** field.

   Also, you can click **Browse** to select a file.

4. Select one of the following error configuration options:
   - **Abort on first error**
   - **Continue processing other records**
5. Select one of the import options:
   - **Skip**
   - **Replace**
   - **Merge**
   - **Delete**
6. In the **Job Schedule** section, select one of the following options:
   - To run the import job immediately, click **Run immediately**.
   - To run the import job at a later time, click **Schedule later** and set the date and time.
7. Click **Import**.

Related links

About bulk import of users on page 324
List of XML Schema Definitions and sample XMLs for bulk import on page 347
Bulk import of global user settings on page 339

Bulk export of global user settings

In System Manager, you can export global settings in bulk from the System Manager database.

You can export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- Default access control list (ACLs)

The Export User process creates an archive file containing one or more XML files. While exporting the global settings records, if the number of exported records exceed the limit of records that an XML file can hold, the system creates multiple XML files. The system packages the XML files in a zip file.

The XML file conforms to the XML schema definition that supports import of global settings. This schema addresses the complete global settings attributes. For more information, see XML Schema Definition for bulk import of global setting records on page 442.

The system generates the XML file on the System Manager server. You can specify the location of the file you want to export while running the Export User job.

You can schedule an export global settings job. The job parameter provides an option to specify the schedule time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.

You can export user data in bulk from System Manager web console and by using the bulk export that you run from CLI. The utility is in the `$MGMT_HOME/bulkadministration/exportutility` directory, where *MGMT_HOME* is an environment variable that represents the System Manager HOME path.

Bulk exporting of global user settings

Before you begin

Start an SSH session.

About this task

In System Manager, you can export global settings from the System Manager database. The export global settings utility is located in the `$MGMT_HOME/bulkadministration/exportutility` directory, where MGMT_HOME is an environment variable that represents the home path for System Manager.

Procedure

1. Log in to System Manager using SSH as root.
2. To change the directory to `exportutility`, at the prompt, type `cd $MGMT_HOME/bulkadministration/exportutility`.

   MGMT_HOME is an environment variable that represents the home path for System Manager.
3. Type `# sh exportUpmGlobalsettings.sh … [OPTIONS]`.
4. **(Optional)** To modify the default values for optional parameters, change the `$MGMT_HOME/bulkadministration/exportutility/config/bulkexportconfig.properties` file.

   For example, `# sh exportUpmGlobalsettings.sh –f globalSettingExport –r 1000 –s 0 –e 1000 –o 1`.

Related links

About bulk export of users on page 327
List of XML Schema Definitions and sample XMLs for bulk import on page 347
exportUpmGlobalsettings.sh command on page 343
Bulk export of global user settings on page 341
exportUpmGlobalsettings.sh command on page 343

exportUpmGlobalsettings.sh command

Use the **exportUpmGlobalsettings** command to export global settings from the System Manager database.

Syntax

```
exportUpmGlobalsettings.sh -f globalSettingExport-r-d -s -e-t
```

-f The prefix of the file name for the file that you require to export.

-r The number of records per file.

-d The location of the file that you want to export.

-s The start index of record.

-e The number of records you want to export.

-t The job scheduling time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.

-o The global settings export filter. The default is 0. You can set one of the following values for the global settings export filter:

- **0** No Filter. 0 is considered as the 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

Note:

You can change the default values for optional arguments from the `bulkexportconfig.properties` file that is located in the `$MGMT_HOME/bulkadministration/exportutility` directory. MGMT_HOME is an environment variable that represents the home path for System Manager.

Scheduling a global user settings import job

About this task

System Manager supports scheduling of bulk import jobs from the System Manager console. With the scheduling utility, you can schedule an import job to run immediately or at a later time.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.

3. On the Import Global Settings page, enter the complete path of the file in the **Select file** field.

   Also, you can click **Browse** to select a file.

4. Select one of the following error configuration options:
   - **Abort on first error**
   - **Continue processing other records**

5. Select one of the import options:
   - **Skip**
   - **Replace**
   - **Merge**
   - **Delete**

6. In the **Job Schedule** section:

   a. Click **Schedule later**.

   To run the import job immediately, click **Run immediately**. After you select this option, the fields related to scheduling become unavailable.

   b. Enter the date in the **Date** field.

   You can use the calender icon to select a date.

   c. Enter time in the **Time** field in the HH:MM:SS format.

   d. From the **Time Zone** field, select a time zone.

7. Click **Import**.

   The system displays the scheduled job in the Manage Jobs section.

Viewing details of a global user settings import job

You can view the following details of an import job:

- Job name
- Job scheduled by
- Job scheduled start time
- Job end time
- Job status
- Import file name
- Total number of user records in the import file

- Total number of user records successfully imported
- Total number of user records that failed to import
- Percentage complete status

About this task

You can view the error message for each user record that fails to import. You can download the failed user records in an XML file format. You can modify the XML file and import the file again.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **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**.

   The Job Detail page displays the details of the selected job.

Viewing a global user settings import job on the Scheduler page

About this task

You can view and perform all operations on an import job that the scheduler supports from the Scheduler page.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.
3. On the Import Global Settings page, select a job from the table in the Manage Job section.
4. Click the link in the **Job Name** column.

   The Scheduler page displays the details of the job.

Aborting a global user settings import job on first error

System Manager supports the following error configurations:

- Abort on first error. Aborts importing of the global settings records when the import global settings operation encounters the first error in the import file that contains the global settings records.
- Continue processing other records. Imports the next global settings record even if the import operation encounters an error while importing a global settings record.

About this task

You can abort an import process when the import process encounters the first error in the input file while processing the global user settings records.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.
3. On the Import Global Settings page, enter the complete path of the file in the **Select file** field.

   Also, you can click **Browse** to select a file.
4. Select **Abort on first error** as the error configuration option.
5. Select one of the import options:
   - **Skip**
   - **Replace**
   - **Merge**
   - **Delete**
6. Choose or enter the appropriate information for the remaining fields.
7. Click **Import**.

Deleting a global user settings import job

System Manager supports deletion of an import job. The **Delete job** option removes the job information from the database. You can delete a job only when the job is in the *SUCCESSFUL* state.

To interrupt a job that is running or pending, use the **Cancel job** option.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **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 import job

You can cancel a job only when the job is in the PENDING EXECUTION or RUNNING state.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **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

The following is the list of XML Schema Definition and sample XML snippets for bulk import of users, global setting records, elements, endpoint profiles, Messaging profiles, CS 1000 profiles, CallPilot profiles, IP Office profiles, agent profiles, Session Manager profiles, Presence profiles, Engagement Development Platform, and Conferencing profiles:

XML Schema Definition for bulk import of users on page 348

Sample XML for bulk import of users with minimal attributes on page 355

Sample XML for bulk import of users with all attributes on page 355

XML Schema Definition for partial import of user attributes on page 363

Sample XML for partial import of user attributes on page 365

XML Schema Definition for bulk deletion of users on page 367

Sample XML for bulk deletion of users on page 368

XML Schema Definition for bulk import of elements on page 368

Sample XML for bulk import of elements on page 373

XML Schema Definition for bulk import of Session Manager profiles on page 374

Sample XML for bulk import of Session Manager profiles on page 376

XML Schema Definition for bulk import of endpoint profiles on page 377

Sample XML for bulk import of endpoint profiles on page 404

XML Schema Definition for bulk import of messaging profiles on page 408

Sample XML for bulk import of Messaging profiles on page 414

XML Schema Definitions for bulk import of agent profiles on page 415

XML Schema for CS1000 and CallPilot communication Profiles on page 420

Sample XML for the CS1000 and CallPilot Communication Profiles on page 421

XML Schema for IP Office Communication Profiles on page 422

Sample XML for the IP Office Communication Profiles on page 431

XML Schema for bulk import and export of Presence Profile on page 438

Sample XML for Presence Communication Profile on page 439

XML Schema for bulk import of Conferencing Profile on page 441

Sample XML for the Conferencing Communication Profile on page 442

XML Schema for bulk import of Engagement Development Platform Profile on page 404

Sample XML for bulk import of Engagement Development Platform Profile on page 403

XML Schema for bulk import of Work Assignment Profile on page 407

XML Schema Definition for bulk import of global setting records on page 442

Sample XML for bulk import of global setting records on page 449

XML Schema Definition for bulk deletion of global setting records on page 453

Sample XML for bulk deletion of global setting records on page 454

XML Schema Definition for bulk import of roles on page 454

Sample XML for bulk import of roles on page 457

Note:

You cannot use the following characters as is in the XML file. To use the characters in the import of XML files, make the following modifications:

- Less-than character (<) as &lt;
- Ampersand character (&) as &amp;
- Greater-than character (>) as &gt;
- Double-quote character (") as &quot;
- Apostrophe or single-quote character (') as &apos;

When you copy the XML schema from the document you must take care of the line breaks.

XML Schema Definition for bulk import of 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="2.0">
    <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"
maxOccurs="1"/>
                <xs:element name="user" type="tns:xmlUser" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:complexType name="xmlUser">
        <xs:sequence>
            <xs:element name="UserOrganizationDetails"
type="tns:UserOrganizationDetailsType"
                maxOccurs="1" minOccurs="0" />
            <xs:element name="UserProvisionRules" minOccurs="0">
                <xs:complexType>
```

```
                    <xs:sequence>
                        <xs:element name="UserProvisionRuleName" type="xs:string" 
minOccurs="0" maxOccurs="unbounded"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="authenticationType" type="xs:string"
                minOccurs="1" 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" minOccurs="1"
                maxOccurs="1" />
            <xs:element name="givenNameAscii" type="xs:string" minOccurs="0"
                maxOccurs="1" />
            <xs:element name="honorific" type="xs:string" minOccurs="0" />
            <xs:element name="loginName" minOccurs="1" maxOccurs="1">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:maxLength value="128" />
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="newLoginName" minOccurs="0" maxOccurs="1">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:maxLength value="128" />
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="employeeNo" type="xs:string"
                minOccurs="0" maxOccurs="1">
            </xs:element>
            <xs:element name="department" type="xs:string" minOccurs="0"
                maxOccurs="1">
            </xs:element>
            <xs:element name="organization" type="xs:string"
                minOccurs="0" maxOccurs="1">
            </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" minOccurs="1"
                maxOccurs="1" />
            <xs:element name="surnameAscii" type="xs:string" minOccurs="0"
                maxOccurs="1" />
            <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="localizedNames" type="tns:xmLocalizedNames" minOccurs="0"
maxOccurs="1"></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"
                maxOccurs="1">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="contactList"
                            type="tns:xmlContactList" maxOccurs="1" />
                    </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" maxOccurs="1" />
            <xs:element name="commProfileSet"
                type="tns:xmlCommProfileSetType" minOccurs="0"
                maxOccurs="unbounded" />

        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlSecurityIdentity">
        <xs:sequence>
            <xs:element name="identity" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="realm" type="xs:string" minOccurs="0"/>
            <xs:element name="type" type="xs:string" minOccurs="1" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlPresInfoTypeAccessType">
        <xs:sequence>
            <xs:element name="infoType" type="tns:xmlPresInfoTypeType" minOccurs="1" 
maxOccurs="1"/>
            <xs:element name="access" type="xs:string" minOccurs="0" maxOccurs="1"/>
        </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="xmlPresUserDefaultType">
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType"/>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresUserCLDefaultType">
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType"/>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresUserACLEntryType">
        <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:sequence>
            <xs:element name="label" type="xs:string" maxOccurs="1"/>
            <xs:element name="filter" type="xs:string" maxOccurs="1"/>
            <xs:element name="specFlags" type="xs:string" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <!-- Contact List entries -->
    <xs:complexType name="xmlContactList">
        <xs:sequence>
            <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="description" type="xs:string" minOccurs="0"/>
            <xs:element name="isPublic" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
            <xs:element name="members" type="tns:xmlContactListMember" minOccurs="0" 
maxOccurs="unbounded"/>
            <xs:element name="contactListType" type="xs:string" minOccurs="1" 
maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlContactListMember">
        <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:element name="isFavorite" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
            <xs:element name="isSpeedDial" type="xs:boolean" minOccurs="1"/>
            <xs:element name="speedDialEntry" type="xs:int" minOccurs="0"/>
            <xs:element name="isPresenceBuddy" type="xs:boolean" minOccurs="1" 
maxOccurs="1"/>
            <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:sequence>
            <xs:element name="address" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="altLabel" type="xs:string" minOccurs="0"/>
            <xs:element name="contactCategory" type="xs:string" minOccurs="1" 
maxOccurs="1"/>
            <xs:element name="contactType" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="label" type="xs:string" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlAddress">
        <xs:sequence>
            <xs:element name="addressType" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <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"/>
            <!-- Additional Attribute Support - The attribute room will be mapped to 
cubical.-->
            <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"/>
            <!-- Additional Attribute Support -->
            <xs:element name="businessphone" type="xs:string" minOccurs="0"/>
            <xs:element name="otherbusinessphone" type="xs:string" minOccurs="0"/>
            <xs:element name="fax" type="xs:string" minOccurs="0"/>
            <xs:element name="homephone" type="xs:string" minOccurs="0"/>
            <xs:element name="otherhomephone" type="xs:string" minOccurs="0"/>
            <xs:element name="mobilephone" type="xs:string" minOccurs="0"/>
            <xs:element name="othermobilephone" type="xs:string" minOccurs="0"/>
            <xs:element name="pager" type="xs:string" minOccurs="0"/>
            <xs:element name="pager2" type="xs:string" minOccurs="0"/>
            <!-- Additional Attribute Support - End -->
            <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: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" minOccurs="1" maxOccurs="1"/>
            <xs:element name="displayNameAscii" type="xs:string" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="dn" type="xs:string" minOccurs="0"/>
            <xs:element name="givenName" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="givenNameAscii" type="xs:string" minOccurs="0"
maxOccurs="1"/>
            <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"
maxOccurs="1"/>
            <xs:element name="preferredLanguage" type="xs:string" minOccurs="0"/>
            <xs:element name="isPublic" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
            <xs:element name="source" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="sourceUserKey" type="xs:string" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="suffix" type="xs:string" minOccurs="0"/>
            <xs:element name="surname" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="surnameAscii" type="xs:string" minOccurs="0" maxOccurs="1"/>
            <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:sequence>
            <xs:element name="handleName" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="handleType" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="handleSubType" type="xs:string" minOccurs="0"
maxOccurs="1"/>
            <xs:element name="domainName" type="xs:string" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlCommProfileType">
        <xs:sequence>
            <xs:element name="commProfileType" type="xs:string" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="commProfileSubType" type="xs:string" minOccurs="0"
maxOccurs="1"/>
            <xs:element name="jobId" type="xs:string" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlCommProfileSetType">
        <xs:sequence>
            <xs:element name="commProfileSetName" type="xs:string" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="isPrimary" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
            <xs:element name="handleList" minOccurs="0">
                <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: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:complexContent>
            <xs:extension base="ext:xmlCommProfileType">
                <xs:sequence>
                    <xs:element name="csEncryptionKeyId" type="xs:long" minOccurs="0" 
maxOccurs="1"/>
                    <xs:element name="servicePassword" type="xs:string" minOccurs="0" 
maxOccurs="1"/>
                    <xs:element name="serviceData" type="xs:string" minOccurs="0" 
maxOccurs="1"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlSecureStore">
        <xs:sequence>
            <xs:element name="secureStoreData" type="xs:base64Binary" minOccurs="1" 
maxOccurs="1"/>
            <xs:element name="passwordEncrypted" type="xs:boolean"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlLocalizedName">
        <xs:sequence>
            <xs:element name="locale" type="xs:string" minOccurs="1"
                maxOccurs="1">
            </xs:element>
            <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"></
xs:element>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmLocalizedNames">
        <xs:sequence>
            <xs:element name="localizedName" type="tns:xmlLocalizedName" minOccurs="0" 
maxOccurs="7"></xs:element>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="UserOrganizationDetailsType">
            <xs:sequence>
            <xs:element name="tenant" maxOccurs="1" minOccurs="1">
                    <xs:complexType>
                    <xs:attribute name="name" type="xs:string" use="required"/>
                       <xs:attribute name="createTenantIfNotAlreadyPresent"
                                           type="xs:boolean"
                                               use="required"/>
                    </xs:complexType>
                </xs:element>
                <xs:element name="organizationUnitLevelOne" type="xs:string"
                    maxOccurs="1" minOccurs="0">
                </xs:element>
                <xs:element name="organizationUnitLevelTwo" type="xs:string"
                    maxOccurs="1" minOccurs="0">
                </xs:element>
                <xs:element name="organizationUnitLevelThree" type="xs:string"
                    maxOccurs="1" minOccurs="0">
                </xs:element>
            </xs:sequence>
    </xs:complexType>

</xs:schema>
```

Sample XML for bulk import of 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 import of 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:This corresponds to the
         Console attribute-Endpoint Display Name.
        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 user,
        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 rfc3986.
........userinfo / loginname = *( unreserved / pct-encoded / sub-delims / ":")
        where <p>unreserved = ALPHA / DIGIT / "-" / "." / "_" / "~"
........pct-encoded = "%" HEXDIG HEXDIG
        sub-delims = "!" / "$" / "&amp;" / "’" / "(" / ")" / "*" / "+" / "," / ";" / "="
     ---employeeNo:Employee number of user.
     ---department:Department of employee.
     ---organization:Organization of employee.
     ---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 with 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:  (-12:0)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 _ . - % ! ~ * ( ) = + $ , ; and ? special characters are
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
     ---localizedNames:localized name of user.
     ---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 userss 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>
    <employeeNo>20060441</employeeNo>
    <department>UC</department>
    <organization>GCS</organization>
    <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>(-12:0)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>
    <localizedNames>
    <localizedName>
    <locale>English</locale>
    <name>John</name>
    </localizedName>
    </localizedNames>
    <!--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 or  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.
        ---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>
          <isPresence>Buddytrue</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
        For example, 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 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 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 inlcude 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.
        ---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 sip,smtp,ibm,and xmpp.
     ---handleSubType:This is an additional qualify on the handle type to help
        specify which private subsystem this handle belongs to.Possible values are
        e164,username,msrtc,googletalk,jabber,ibmsametime,lotousnotes,msexchageo.
     ---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="ns3:SessionManagerCommProfXML" xmlns:ns3="http://
xml.avaya.com/schema/import_sessionmanager">
                 <commProfileType>SessionManager</commProfileType>
                 <ns3:primarySM>SIP Entity 1</ns3:primarySM>
                 <ns3:secondarySM>SIP Entity 2</ns3:secondarySM>
                 <ns3:survivabilityServer>SIP Entity 2</ns3:survivabilityServer>
                 <ns3:terminationAppSequence>AppSeq1</ns3:terminationAppSequence>
                 <ns3:originationAppSequence>AppSeq2</ns3:originationAppSequence>
                 <ns3:homeLocation>Denver</ns3:homeLocation>
                 <ns3:confFactorySet>Factory Set 1</ns3:confFactorySet>
           </commProfile>
      </commProfileList>
-->
    </commProfileSet>

  </tns:user>
</tns:users>
```

XML Schema Definition for partial import of 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: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 partial import of 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>
    <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 deletion of 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 deletion of users

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:deleteUsers xmlns:tns="http://xml.avaya.com/schema/bulkdelete" xmlns:ns2="http://
xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/bulkdelete
UserProfileSchemaDefinitionForBulkDelete.xsd">
<tns:deleteType>permanent</tns:deleteType>
    <tns:user>
    <tns:loginName>jmiller@avaya.com</tns:loginName>
    </tns:user>
    <tns:user>
    <tns:loginName>david@avaya.com</tns:loginName>
    </tns:user>
</tns:deleteUsers>
```

XML Schema Definition for bulk import of 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 import of 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 import of 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">

<!--
    This is the XML schema for the "Session Manager Profile". It defines this
    profile inside of an XML document that defines a user record
    (see userimport.xsd)
-->

<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>
      <!--
       The following attributes are the names of objects that must
       already be administered in System Manager before performing
         the user import.

         The relative order here cannot be changed because it would
         break backwards compatibility with existing XML documents
         that could be used for an import.
      -->

      <!-- Name of the primary Session Manager (required) -->
      <xsd:element name="primarySM" type="xsd:string" minOccurs="1" />

      <!--  Name of the secondary Session Manager (optional) -->
          <xsd:element name="secondarySM" type="xsd:string" minOccurs="0" />

      <!-- Name of the Termination Application Sequence (optional) - administered
           under Session Manager /Application Configuration /Application Sequences
       -->
          <xsd:element name="terminationAppSequence" type="xsd:string"  minOccurs="0" />

          <!-- Name of the Origination Application Sequence (optional)
               - administered under
                 Session Manager /Application Configuration /Application Sequences --
>
          <xsd:element name="originationAppSequence" type="xsd:string" minOccurs="0" />

          <!-- Name of the Conference Factory Set (optional)
              - administered under
                Session Manager / Application Configuration / Conference Factories  -->
          <xsd:element name="confFactorySet" type="xsd:string" minOccurs="0" />

          <!-- Name of the Survivability Server (optional)
             - usually the name of a Branch Session Manager, but can be any non-CM
               SIP Entity -->
          <xsd:element name="survivabilityServer" type="xsd:string" minOccurs="0" />

          <!-- Name of the Home Location (required)
                - administered under Routing / Locations -->
          <xsd:element name="homeLocation" type="xsd:string"  minOccurs="1" />

          <!-- The maximum number of endpoints that can be simultaneously
                registered using this Session Manager Profile. (optional)
               - The value is an integer between 1 and 10 and
                 defaults to 1 if not specified.  -->
          <xsd:element name="maxSimultaneousDevices" minOccurs="0">
            <xsd:simpleType>
                      <xsd:restriction base="xsd:integer">
                          <xsd:minInclusive value="1" />
                         <xsd:maxInclusive value="10" />
                      </xsd:restriction>
                  </xsd:simpleType>
          </xsd:element>

        <!--
        If true, new registrations will be blocked for this Session Manager
        Profile if the maximum number of simultaneously registered endpoints
        (see "maxSimultaneousDevices" above) is currently registered.  If
          false, an existing registration will be terminated to allow a new
          registration for this Session Manager Profile. (optional)
          - the value defaults to false if not specified
        -->
          <xsd:element name="blockNewRegistrationWhenMaxActive" minOccurs="0">
                <xsd:simpleType>
                      <xsd:restriction base="xsd:boolean" />
                  </xsd:simpleType>
          </xsd:element>

    </xsd:sequence>

        </xsd:extension>
    </xsd:complexContent>
 </xsd:complexType>


</xsd:schema>
```

Sample XML for bulk import of 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) 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 -->
        <!-- A Session Manager Profile is defined to associate a maximum of two
            SIP phones,having the SIP handle, 5555555@domain.com, with...
            “Primary Session Manager” (‘Primary SM’)
            “Secondary Session Mananger” instance (‘Secondary SM’)
            “Termination Sequence” (‘Sequence to My CM’),
            “Origination Sequence” (‘Sequence to My CM’),
            “Conference Factory Set” (‘EngeeringDepartmentConferenceSet’)
            “Survivability Server” (“BSM” value below),
            “Home Location” (‘My Home’).
            If both phones are registered and a third phone tries to register
            using the same SIP handle, one of the two phones will have its
            registration terminated to allow the third phone to register.
        -->
<commProfileList>
                 <commProfile xsi:type="ns3:SessionManagerCommProfXML" xmlns:ns3="http://
xml.avaya.com/schema/import_sessionmanager">
                     <commProfileType>SessionManager</commProfileType>
                     <ns3:primarySM>Primary SM</ns3:primarySM>
                     <ns3:secondarySM>Secondary SM</ns3:secondarySM>
                     <ns3:terminationAppSequence>Sequence to My CM</
ns3:terminationAppSequence>
                     <ns3:originationAppSequence>Sequence to My CM</
ns3:originationAppSequence>
                                 <ns3:confFactorySet>EngeeringDepartmentConferenceSet</
ns3:confFactorySet>
                     <ns3:survivabilityServer>BSM</ns3:survivabilityServer>
                     <ns3:homeLocation>My Home</ns3:homeLocation>
                     <ns3:maxSimultaneousDevices>3</ns3:maxSimultaneousDevices>
                     <ns3:blockNewRegistrationWhenMaxActive>false</
ns3:blockNewRegistrationWhenMaxActive>
                 </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 import of 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"/>
                <xs:element name="prefHandleId" type="xs:string" maxOccurs="1" 
minOccurs="0"/>
                <!-- '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"/>

                <!-- Extension Range which will be used to create Station using available 
extension within given range -->
                <xs:element name="extensionRange" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|([0-9]+([\.\-]
[0-9]+)*:[0-9]+([\.\-][0-9]+)*)"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- 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]+)*)|[nN][eE][xX][tT]"/>
                        </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"/>

                <!-- Whether the endpoint name on CM should be overridden with the value 
in User. -->
                <xs:element name="overRideEndpointName" type="xs:boolean" maxOccurs="1" 
minOccurs="0"/>

                <!-- true/false for Enhanced Callr-Info display for 1-line phones -->
                <xs:element name="enhCallrInfodisplay" 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: CM 5.2 - Path Number between 1-2000, time of day 
table, t1-t999, or blank. -->
                <!-- Valid values: CM 6.0 - Path Number between 1-9999, 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="([1-9]{0})|(t[1-9][0-9]{0,2})|([1-9][0-9]
{0,3})"/>
                        </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: CM 5.2 - Path Number between 1-2000, time of day 
table, t1-t999, or blank. -->
                <!-- Valid values: CM 6.0 - Path Number between 1-9999, 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="([1-9]{0})|(t[1-9][0-9]{0,2})|([1-9][0-9]
{0,3})"/>
                        </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 250 when TN is ON in special application and 1 to 
100 o.w. -->
                <xs:element name="tn" maxOccurs="1" minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:int">
                            <xs:minInclusive value="1" />
                            <xs:maxInclusive value="250" />
                        </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="xmobileType" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="EC500"/>
                            <xs:enumeration value="DECT"/>
                            <xs:enumeration value="IPDECT"/>
                            <xs:enumeration value="PHS"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="mappingMode" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="termination"/>
                            <xs:enumeration value="origination"/>
                            <xs:enumeration value="both"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="configurationSet" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                              <xs:pattern value="|[1-9]|[0-9][1-9]"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="mobilityTrunkGroup" 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="dialPrefix" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                              <xs:pattern value="([0-9]*#){0,4}"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="cellPhoneNumber" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                              <xs:pattern value="[0-9]{0,15}"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="musicSource" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:int">
                            <xs:minInclusive value="1" />
                            <xs:maxInclusive value="250" />
                          </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="unicode2"/>
                            <xs:enumeration value="unicode3"/>
                            <xs:enumeration value="unicode4"/>
                            <xs:enumeration value="user-defined"/>
                          </xs:restriction>
                    </xs:simpleType>
                </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="1" />
                            <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" />

                <!--
                    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.
                -->
                <xs:element name="mediaComplexExt" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="([1-9]{0})|[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 
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>
                <!--
                    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
                        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)(*)(#)(~mwWps)]{0,24}"/>
                        </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>

                <!--
                    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.
                -->
                <xs:element name="lwcActivation" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="lwcLogExternalCalls" type="xs:boolean" 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 - 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.
                    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
                -->
                <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
                                        if the user is not a served user of either an fp-
mwi or qsig-mwi message center.
                 -->
                <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**********
                    When a DCP 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 data base must be manually updated. If the Emergency
                    Location Extension field 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 entries             Usage
                    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.
                    once             Enter once and 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.
                                    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.
                    no                 Enter no to require administration in order to
move the DCP telephone.
                    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.
                    error             Error is a display-only value. 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.
                -->
                <xs:element name="automaticMoves" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
```

```
                            <xs:enumeration value="always"/>
                            <xs:enumeration value="no"/>
                            <xs:enumeration value="once"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <!--
                    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 entries                    Usage
                    as-on-local                   Type as-on-local to achieve the following
results:
                                            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).
                                            If the administrator populates the IP Address
Mapping screen with
                                            emergency numbers, the value as-on-local
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 value as-on-
local 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
Extension 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).

                    block                          Enter block to prevent 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 Avaya S8XXX 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                    Enter cesid to allow 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.
                                            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 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                    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 Station
                    screen is different from the Emergency Location 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).
                -->
                <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.
                                        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 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
                 -->
                <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" />

                <!-- Provides extended local calls / imsFeatureSequencing
                Extended Local Calls (ELC) /imsFeatureSequencing allows DCP and H.323
stations to use SIP sequenced applications.  The feature works by routing calls
                involving those stations over SIP IMS trunks.  In other words, CM is
applying the half-call model to those stations.
                That also has the side effect that features which work differently under
the half-call model than under the usual (full-call) model
                also work differently for ELC stations.
                The Extended Local Calls feature is administrable per station.  We're
allowing stations that always use SIP IMS trunks to coexist on
                the same server with stations that dont always use SIP IMS trunks.  In
other words, ELC is changing a previous marketing rule that
                the full-call model (CM-ES) and the half-call model (CM-FS) functions
can't co-exist on the same server.  As noted above, that also
                has the side effect that features which work differently under the half-
call model than under the full-call model now also can work
                differently for two different SIP stations on the same CM
server.
                 -->
                <xs:element name="imsFeatureSequencing" 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
                    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 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 0-3-->
                <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:string">
                            <xs:pattern value="[1-5]|[0-9]{0}"/>
                        </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>

                <!-- true/false to enable/disable Mute on Off Hook in Shared Control Mode
feature. -->
                <xs:element name="muteOnOffHookInSCMode" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <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>

                <!-- Enter a Group ID between 0-999, or blank -->
                <xs:element name="ipPhoneGroupId" maxOccurs="1" minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]|[0-9][0-9]|[0-9][0-9][0-9]|[0-9]
{0}"/>
                        </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>


                <xs:element name="endptId" maxOccurs="1" minOccurs="0" > <!-- 00 to 62 -->
                    <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" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[1-9]{0}|[1-9]|[1-9][0-9]|[1-9]([0-9]){2}|
[1]([0-9]){3}|2000"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
            </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>

        <!-- Enter numeric cord length (0-99) -->
        <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:element name="listId" type="xs:int" maxOccurs="1" minOccurs="0" />
    </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>
        <!-- CM dependant field - 100 or 250 depends on system params -->
        <xs:element name="tn" maxOccurs="1" minOccurs="1" ><!--  *******Must
present******  -->
            <xs:simpleType>
                  <xs:restriction base="xs:int">
                    <xs:minInclusive value="1" />
                    <xs:maxInclusive value="250" />
                  </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>

<!-- If displayName,givenName or surname contains characters of multiple scripts then 
locale tag should be present.
       If displayName tag is present then it overwrites native name.
       If displayname is not present then combination of givenName and surname gets 
copied in native name.
       Please find below locale for multiscript language
       Language               Locale
       Japanese                       ja, ja-jp
       Simplified Chinese         zh-cn
       Traditional Chinese     zh-tw -->
<xs:complexType name="xmlNativeNameData">
    <xs:sequence>
        <xs:element name="locale" maxOccurs="1" minOccurs="0">
           <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="ja-jp"/>
                    <xs:enumeration value="ja"/>
                    <xs:enumeration value="zh-cn"/>
                    <xs:enumeration value="zh-tw"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="name" maxOccurs="1" minOccurs="0" >
            <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 import of Engagement Development Platform profiles

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:ns2="http://xml.avaya.com/schema/import_ce" xmlns:ns3="http://
xml.avaya.com/schema/import_csm_b5800" xmlns:ns4="http://xml.avaya.com/schema/import1"
xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ns6="http://xml.avaya.com/schema/
import_mmcs" xmlns:ns7="http://xml.avaya.com/schema/import_sessionmanager"
xmlns:ns8="http://xml.avaya.com/schema/mock" xmlns:ns9="http://xml.avaya.com/schema/
import_csm_mm" xmlns:ns10="http://xml.avaya.com/schema/import_csm_cm" xmlns:ns11="http://
xml.avaya.com/schema/import_csm_agent" xmlns:ns12="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">
    <tns:user>
        <authenticationType>basic</authenticationType>
        <description></description>
        <displayName>saurabh, tyagi</displayName>
        <displayNameAscii>saurabh, tyagi</displayNameAscii>
        <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>tyagi</givenName>
        <givenNameAscii>tyagi</givenNameAscii>
        <honorific></honorific>
        <loginName>saurabhtyagi@avaya.com</loginName>
        <employeeNo></employeeNo>
        <department></department>
        <organization></organization>
        <middleName></middleName>
        <preferredLanguage>hu</preferredLanguage>
        <source>local</source>
        <status>provisioned</status>
        <surname>saurabh</surname>
        <surnameAscii>saurabh</surnameAscii>
        <userName>saurabhtyagi</userName>
        <userPassword></userPassword>
        <roles>
            <role>End-User</role>
        </roles>
        <ownedContactLists>
            <contactList>
                <name>list-saurabhtyagi_avaya.com</name>
                <isPublic>false</isPublic>
                <contactListType>general</contactListType>
            </contactList>
        </ownedContactLists>
        <commProfileSet>
            <commProfileSetName>Primary</commProfileSetName>
            <isPrimary>true</isPrimary>
            <commProfileList>
                <commProfile xsi:type="ns2:CeCommProfXML" xmlns:ns2="http://xml.avaya.com/
schema/import_ce">
                    <commProfileType>AUS</commProfileType>
                    <ns2:serviceProfile>ce_service_profile</ns2:serviceProfile>
                </commProfile>
            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema Definition for bulk import of Engagement Development Platform 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_ce"
            elementFormDefault="qualified">

<!-- This is the XML schema for the "CE Profile".  It
     defines this profile inside of an XML document that defines
     a user record (see userimport.xsd) -->

<xsd:import namespace="http://xml.avaya.com/schema/import"
            schemaLocation="userimport.xsd"/>

<xsd:complexType name="CeCommProfXML">
    <xsd:complexContent>
        <xsd:extension base="smgr:xmlCommProfileType">

    <xsd:sequence>
      <!--
       The following attributes are the names of objects that must
       already be administered in System Manager before performing
         the user import.

         The relative order here cannot be changed because it would
         break backwards compatibility with existing XML documents
         that could be used for an import.
      -->

      <!--  Name of the secondary Session Manager (optional) -->
          <xsd:element name="serviceProfile" type="xsd:string" minOccurs="1" />

    </xsd:sequence>

        </xsd:extension>
    </xsd:complexContent>
 </xsd:complexType>

</xsd:schema>
```

Sample XML for bulk import of Engagement Development Platform 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>
            <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>
                        s
                    </ipt:coverageAfterForwarding>
                    <ipt:directIpIpAudioConnections>
                        true
                    </ipt:directIpIpAudioConnections>
                    <ipt:ipAudioHairpinning>
                        false
                    </ipt:ipAudioHairpinning>
                    <!-- <ipt:primeAppearancePreference>
                        </ipt:primeAppearancePreference>  -->
                </commProfile>
            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
</codeblock>
```

XML Schema for bulk import and export of Work Assignment 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_workassignment"
                elementFormDefault="qualified">
                 <!-- This is the XML schema for the "Work Assignment Profile".  It
                 defines this profile inside of an XML document that defines
                a user record (see userimport.xsd) -->
                <xsd:import namespace="http://xml.avaya.com/schema/import"
             schemaLocation="userimport.xsd" />
                <xsd:complexType name="WorkAssignmentCommProfXML">
                  <xsd:complexContent>
                  <xsd:extension base="smgr:xmlCommProfileType" >
                  <xsd:sequence>
                  <xsd:element name="strategyName" type="xsd:string" minOccurs="0"
maxOccurs="1" />
                 <xsd:element name="workAssignmentResourceDetails" minOccurs="0"
maxOccurs="unbounded">
                <xsd:complexType>
                <xsd:sequence>
                <xsd:element name="associatedHandleName" type="xsd:string" minOccurs="1"
maxOccurs="1" />
        <xsd:element name="accountName" type="xsd:string" minOccurs="0" maxOccurs="1" />
             <xsd:element name="accountAddress" type="xsd:string" minOccurs="0"
maxOccurs="1" />
           <xsd:element name="sourceName" type="xsd:string" minOccurs="0" maxOccurs="1" />
           <xsd:element name="sourceAddress" type="xsd:string" minOccurs="0"
maxOccurs="1" />
        <xsd:element name="channelAttribute" type="xsd:string" minOccurs="0"
maxOccurs="1" />
            </xsd:sequence>
          </xsd:complexType>
          </xsd:element>
          <xsd:element name="workAssignmentAgentAttributes" minOccurs="0"
maxOccurs="unbounded">
           <xsd:complexType>
         <xsd:sequence>
         <xsd:element name="categoryName" type="xsd:string" minOccurs="1" maxOccurs="1" />
         <xsd:element name="attributeName" type="xsd:string" minOccurs="1"
maxOccurs="1" />
         </xsd:sequence>
          </xsd:complexType>
          </xsd:element>
       </xsd:sequence>
       </xsd:extension>
       </xsd:complexContent>
    </xsd:complexType>
 </xsd:schema>
```

XML Schema Definition for bulk import of 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. Name as it appears under
                        'Applications/Application Management/Entities
                    -->
                    <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]{1,50}" />
                            </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="0">
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern value="[0-9]{0,15}" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>
                    <xs:element name="deleteOnUnassign" type="xs:boolean"
                        maxOccurs="1" minOccurs="0" />

                    <!-- follows overrriding  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.
                    -->
                    <xs:element name="communityID" maxOccurs="1" minOccurs="0">
                    <!-- MM/CMM field -->
                        <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]{0,50}" />
                            </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>
            <!--
                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]{0}|[0-9]{3,10}" />
                    </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 import of 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>
        <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>newest messages first
</ipt:tuiMessageOrder>
                        <ipt:intercomPaging>paging is off
</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 import of agent 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_agent" xmlns:csm="http://
xml.avaya.com/schema/import_csm_agent">
<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="xmlAgentProfile">
    <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="useExistingAgent" type="xs:boolean" maxOccurs="1" 
minOccurs="0"/>

                <!-- Extension Range which will be used to create Agent using available 
extension within given range -->
                <xs:element name="extensionRange" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|([0-9]+([\.\-]
[0-9]+)*:[0-9]+([\.\-][0-9]+)*)"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Agent Login ID extension number that need to be assigned to the 
user. -->
                <xs:element name="loginIdExtension" maxOccurs="1" minOccurs="1">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|[nN][eE][xX][tT]"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Template name to be used to create agent. Values defined in Template 
will be used if not provided. -->
                <xs:element name="template" 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]{0,4}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="aas" type="xs:boolean" maxOccurs="1" minOccurs="0"/>
                <xs:element name="audix" type="xs:boolean" maxOccurs="1" minOccurs="0"/>

                <xs:element name="password" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]{0,9}" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="portExtension" 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 the agent should be deleted if it unassigned from the user. 
-->
                <xs:element name="deleteOnUnassign" type="xs:boolean" maxOccurs="1" 
minOccurs="0"/>
```

```
                <!-- CM dependent field for max value -->
                <xs:element name="tn" maxOccurs="1" minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:int">
                            <xs:minInclusive value="1" />
                            <xs:maxInclusive value="250" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <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>

                <!--Coverage path = Enter path number between 1-9999, time of day table 
t1-t999, or blank - CM Dependent-->
                <xs:element name="coveragePath" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="(t[1-9][0-9]{0,2})|([1-9]{0})|([1-9][0-9]
{0,3})"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <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>

                <xs:element name="lwcLogExternalCalls" type="xs:boolean" maxOccurs="1" 
minOccurs="0" />
                <xs:element name="audixNameforMessaging" type="xs:string" maxOccurs="1" 
minOccurs="0" />
                <xs:element name="hearsServiceObservingTone" type="xs:boolean" 
maxOccurs="1" minOccurs="0" />
                <xs:element name="loginIDforISDNSIPDisplay" type="xs:boolean" 
maxOccurs="1" minOccurs="0" />

                <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="none"/>
                            <xs:enumeration value="station"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="miaAcrossSkills" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
```

```
                            <xs:enumeration value="n"/>
                            <xs:enumeration value="y"/>
                            <xs:enumeration value="system"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="acwAgentConsideredIdle" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="n"/>
                            <xs:enumeration value="y"/>
                            <xs:enumeration value="system"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="auxWorkReasonCodeType" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="forced"/>
                            <xs:enumeration value="requested"/>
                            <xs:enumeration value="system"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="logoutReasonCodeType" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="forced"/>
                            <xs:enumeration value="requested"/>
                            <xs:enumeration value="system"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="maximumTimeAgentInAcwBeforeLogoutSec" maxOccurs="1" 
minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                              <xs:pattern value="|[3-9][0-9]{1}|[1-9][0-9]{1,3}|(none)|
(system)"/>

                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="forcedAgentLogoutTimeHr" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="|[0-9]|[1][0-9]{1}|[2][0-3]{1}"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="forcedAgentLogoutTimeSec" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                              <xs:pattern value="|(00)|(15)|(30)|(45)"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>
                <xs:element name="directAgentSkill" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="|[1-9]|[1-9][0-9]{0,2}|[1-7][0-9]{3}|
8000"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="callHandlingPreference" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="greatest-need"/>
                            <xs:enumeration value="percent-allocation"/>
                            <xs:enumeration value="skill-level"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="serviceObjective" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="directAgentCallsFirst" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="localCallPreference" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="skills" type="csm:xmlAgentLoginIdSkillsData"
maxOccurs="unbounded" minOccurs="0" />

                <xs:element  name="nativeName" type="csm:xmlNativeNameData" maxOccurs="1"
minOccurs="0"/>

                <!--

                private String NativeNameScripts;

                 -->
            </xs:sequence>
        </xs:extension>
   </xs:complexContent>
</xs:complexType>

<xs:complexType name="xmlAgentLoginIdSkillsData">
    <xs:sequence>
    <!--
        private AgentLoginIdData agentLoginId;

     -->
        <xs:element name="number" type="xs:string" maxOccurs="1" minOccurs="1" />
        <xs:element name="skillNumber" maxOccurs="1" minOccurs="1">
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="[1-9][0-9]{0,2}|[1-7][0-9]{3}|8000"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="reserveLevel" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="|a|m|n|[1-2]"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="skillLevel" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="|[1-9]|[1-9][0-6]{1}"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="percentAllocation" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="|[1-9]|[1-9][0-9]{1}|100"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>


    </xs:sequence>
</xs:complexType>

<!-- If displayName,givenName or surname contains characters of multiple scripts then
locale tag should be present.
       If displayName tag is present then it overwrites native name.
       If displayname is not present then combination of givenName and surname gets
copied in native name.
       Please find below locale for multiscript language
       Language              Locale
       Japanese                ja, ja-jp
       Simplified Chinese        zh-cn
       Traditional Chinese    zh-tw-->
<xs:complexType name="xmlNativeNameData">
    <xs:sequence>
        <xs:element name="locale" maxOccurs="1" minOccurs="0">
           <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="ja-jp"/>
                    <xs:enumeration value="ja"/>
                    <xs:enumeration value="zh-cn"/>
                    <xs:enumeration value="zh-tw"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="name" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:maxLength value="27"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:sequence>
</xs:complexType>

</xs:schema>
```

XML Schema for CS 1000 and CallPilot Communication Profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     xmlns:one="http://xml.avaya.com/schema/import"
     targetNamespace="http://xml.avaya.com/schema/import1"
     elementFormDefault="qualified"
     xmlns:abc="http://xml.avaya.com/schema/import1">
<xsd:import namespace="http://xml.avaya.com/schema/import"
            schemaLocation="userimport.xsd"/>
<xsd:complexType name="AccountCommProfileType">
```

```
    <xsd:complexContent>
        <xsd:extension base="one:xmlCommProfileType" >
            <xsd:sequence>
               <xsd:element name="serviceDetails" type="xsd:string" minOccurs="0"/>
               <xsd:element name="element" type="xsd:string" minOccurs="0"/>
               <xsd:element name="target" type="xsd:string" minOccurs="0"/>
               <xsd:element name="template" type="xsd:string" minOccurs="0"/>
               <xsd:element name="serviceType" type="xsd:string" minOccurs="0"/>
               <xsd:element name="accountDetails" type="xsd:string" minOccurs="0"/>
               <xsd:element name="accountProperties" type="abc:AccountPropertyType"
minOccurs="0" maxOccurs="unbounded"/>
            </xsd:sequence>
        </xsd:extension>
    </xsd:complexContent>
</xsd:complexType>

<xsd:complexType name="AccountPropertyType">
   <xsd:sequence>
      <xsd:element name="propertyName" type="xsd:string"/>
      <xsd:element name="propertyValue" type="xsd:string"/>
    </xsd:sequence>
</xsd:complexType>
</xsd:schema>
```

Sample XML for CS 1000 and CallPilot Communication Profiles

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<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">
    <tns:user>
        <authenticationType>basic</authenticationType>
        <description></description>
        <displayName>singleUser, singleUser</displayName>
        <displayNameAscii>singleUser, singleUser</displayNameAscii>
        <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>singleUser</givenName>
        <honorific></honorific>
        <loginName>singleuser@avaya.com</loginName>
        <employeeNo></employeeNo>
        <department></department>
        <organization></organization>
        <middleName></middleName>
        <preferredLanguage>en_US</preferredLanguage>
        <source>local</source>
        <sourceUserKe>Ynone</sourceUserKe>Y
        <status>provisioned</status>
        <surname>singleUser</surname>
        <userName>singleuser</userName>
        <userPassword></userPassword>
        <roles>
            <role>End-User</role>
        </roles>
        <ownedContactLists>
            <contactList>
                <name>list-singleuser_avaya.com</name>
                <description></description>
                <isPublic>false</isPublic>
                <contactListType>general</contactListType>
            </contactList>
        </ownedContactLists>
        <commProfileSet>
```

```
            <commProfileSetName>Primary</commProfileSetName>
            <isPrimar>Ytrue</isPrimar>Y
            <commProfileList>
                <commProfile xsi:type="ns3:AccountCommProfileType" xmlns:ns3="http://
xml.avaya.com/schema/import1">
                    <commProfileType>accountCommProfile</commProfileType>
                    <ns3:serviceDetails>DN=8054(Marped), TN=004 0 00 12, TYPE=M2602</
ns3:serviceDetails>
                    <ns3:element>CS1K Mock Element Manager</ns3:element>
                    <ns3:target>Target1</ns3:target>
                    <ns3:template>Premium</ns3:template>
<ns3:serviceType>com.nortel.ems.services.account.Telephony</ns3:serviceType>
                    <ns3:properties>
                        <ns3:property name="prefEsn">343-8054</ns3:propert>Y
                        <ns3:property name="prefDn">8054</ns3:propert>Y
                    </ns3:properties>
                    <ns3:isPublished>true</ns3:isPublished>
                </commProfile>
            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema for IP Office Communication 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_b5800" xmlns:csm="http://
xml.avaya.com/schema/import_csm_b5800">

    <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="xmlB5800UserProfile">
        <xs:complexContent>
            <xs:extension base="one:xmlCommProfileType">
                <xs:sequence>
                    <!--
                        IPOffice/B5800/B5800L Device Name as it appears under
'Applications/Application
                        Management/Entities
                    -->
                    <xs:element name="deviceName" type="xs:string" maxOccurs="1"
                        minOccurs="1" />

                    <!--
                        Template name to be used to create station. Values defined in
                        Template will be used if not provided.
                    -->
                    <xs:element name="userTemplate" type="xs:string"
                        maxOccurs="1" minOccurs="0" />

                    <xs:element name="useExistingExt" type="xs:boolean"
                        maxOccurs="1" minOccurs="0" />

                    <!-- 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>
                    <xs:element name="modulePort" type="xs:string"
                        maxOccurs="1" minOccurs="0" />

                    <!-- Specifies the type of the extn  -->
                    <xs:element name="extensionType" maxOccurs="1"
                        minOccurs="1">
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:enumeration value="Analog" />
                                <xs:enumeration value="IPDECT" />
                                <xs:enumeration value="SIPDECT" />
                                <xs:enumeration value="Sip" />
                                <xs:enumeration value="Digital" />
                                <xs:enumeration value="H323" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>

                    <xs:element name="deleteExtOnUserDelete" type="xs:boolean"
                        maxOccurs="1" minOccurs="0" />

                    <xs:element name="data" type="csm:xmlB5800UserProfileData"
                        maxOccurs="1" minOccurs="0" />
                </xs:sequence>

            </xs:extension>

        </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="xmlB5800UserProfileData">
        <xs:sequence>
            <xs:element name="ws_object" type="csm:xmlB5800UserConfig">
            </xs:element>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlB5800UserConfig">
        <xs:sequence>
            <xs:element name="Extension" type="csm:xmlB5800ExtensionInfo">
            </xs:element>
            <xs:element name="User" type="csm:xmlB5800UserInfo">
            </xs:element>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlB5800ExtensionInfo">
        <xs:sequence>
            <xs:element name="Id" type="xs:int" minOccurs="0" />
            <xs:element name="SubId" type="xs:string" minOccurs="0" />
            <xs:element name="Extension" type="xs:string" minOccurs="0" />
            <xs:element name="TypeInfo" type="xs:int" minOccurs="0" />
            <xs:element name="CallerDisplayType" type="xs:int" minOccurs="0" />
            <xs:element name="MessageLampType" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnClassification" type="xs:int" minOccurs="0" />
            <xs:element name="LineType" type="xs:int" minOccurs="0" />
            <xs:element name="MinFlashPulseWidth" type="xs:int" minOccurs="0" />
            <xs:element name="MaxFlashPulseWidth" type="xs:int" minOccurs="0" />
            <xs:element name="UseSystemFlashHook" type="xs:boolean" minOccurs="0" />
            <xs:element name="ResetVolumeAfterCalls" type="xs:boolean" minOccurs="0" />
            <xs:element name="DisconnectPulseWidth" type="xs:int" minOccurs="0" />
            <xs:element name="HookPersistency" type="xs:int" minOccurs="0" />
            <xs:element name="Mac" type="xs:string" minOccurs="0" />
            <xs:element name="SilenceSuppression" type="xs:boolean" minOccurs="0" />
            <xs:element name="VoicePktSize" type="xs:int" minOccurs="0" />
            <xs:element name="VoiceCompression" type="xs:int" minOccurs="0" />
            <xs:element name="voip" type="csm:xmlVoip" minOccurs="0" />
            <xs:element name="RenegotiationSupported" type="xs:boolean" minOccurs="0" />
            <xs:element name="RenegotiateBeforeConnect" type="xs:boolean" minOccurs="0" />
            <xs:element name="UseVocoder" type="xs:boolean" minOccurs="0" />
            <xs:element name="EarlyH245Supported" type="xs:boolean" minOccurs="0" />
            <xs:element name="RFC2833" type="xs:boolean" minOccurs="0" />
            <xs:element name="MediaWait" type="xs:boolean" minOccurs="0" />
            <xs:element name="MediaOnOverlap" type="xs:boolean" minOccurs="0" />
            <xs:element name="PauseRequired" type="xs:boolean" minOccurs="0" />
            <xs:element name="PauseOnEndRequired" type="xs:boolean" minOccurs="0" />
            <xs:element name="ParallelH245" type="xs:boolean" minOccurs="0" />
            <xs:element name="AnnexFSupported" type="xs:boolean" minOccurs="0" />
            <xs:element name="PhoneType" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIAudio_setting" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIHeadset_setting" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIContrast" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIRedial_time" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPISpeaker_volume" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIHandsfree_settings" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIRingtone_volume" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIDoor_phone" type="xs:boolean" minOccurs="0" />
            <xs:element name="ExtnAPIHandset_volume" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIRingtone_speed" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIHeadset_volume" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIHeadset_config" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIAlpha_keypad_layout" type="xs:int" minOccurs="0" />
            <xs:element name="ExtnAPIDirect_dial_enabled" type="xs:boolean"
minOccurs="0" />
            <xs:element name="ExtnAPIHandsfree_enabled" type="xs:boolean" minOccurs="0" />
            <xs:element name="T38Fax" type="csm:xmlT38Fax" minOccurs="0" />
            <xs:element name="SipExtn" type="csm:xmlSipExtn" minOccurs="0" />
            <xs:element name="DisableSpeaker" type="xs:boolean" minOccurs="0" />
            <xs:element name="VPNExtn" type="xs:boolean" minOccurs="0" />
            <xs:element name="IPAvayaLicenseReserved" type="xs:boolean" minOccurs="0" />
            <xs:element name="IPEndpointsLicenseReserved" type="xs:boolean"
minOccurs="0" />
            <xs:element name="IsExtnCentralized" type="xs:boolean" minOccurs="0" />
            <xs:element name="CentralizedDDINumber" type="xs:string" minOccurs="0" />
            <xs:element name="ExtnDS" type="csm:xmlExtnDS" minOccurs="0" />
            <xs:element name="SpecificBstType" type="xs:int" minOccurs="0" />
            <xs:element name="Location" type="xs:string" minOccurs="0" />
            <xs:element name="PhonePassword" type="xs:string" minOccurs="0" />
            <xs:element name="Module" type="xs:string" minOccurs="0" />
            <xs:element name="Port" type="xs:string" minOccurs="0" />
            <xs:element name="AllowRemoteExtn" type="xs:string" minOccurs="0" />
            <xs:element name="FallbackAsRemoteWorker" type="xs:string" minOccurs="0" />
            <xs:element name="RingVoltageBoost" type="xs:string" minOccurs="0" />
            <xs:element name="RemoteLineNumber" type="xs:string" minOccurs="0" />
            <xs:element name="D100Extn" type="csm:xmlD100Extn" minOccurs="0" />
        </xs:sequence>
        <xs:attribute name="GUID" type="xs:string" />
    </xs:complexType>

    <xs:complexType name="xmlB5800UserInfo">
        <xs:sequence>
            <xs:element name="EUAuth" type="csm:xmlEUAuth" minOccurs="0" />
            <xs:element name="UserRightsView" type="xs:string" minOccurs="0" />
            <xs:element name="UsingView" type="xs:boolean" minOccurs="0" />
            <xs:element name="UserRightsTimeProfile" type="xs:string" minOccurs="0" />
            <xs:element name="OutOfHoursUserRights" type="xs:string" minOccurs="0" />
            <xs:element name="Name" type="xs:string" minOccurs="0" />
            <xs:element name="KName" type="xs:string" minOccurs="0" />
            <xs:element name="Password" type="xs:string" minOccurs="0" />
            <xs:element name="FullName" type="xs:string" minOccurs="0" />
            <xs:element name="Extension" type="xs:string" minOccurs="0" />
            <xs:element name="Priority" type="xs:int" minOccurs="0" />
            <xs:element name="OutsideCallSeq" type="xs:int" minOccurs="0" />
            <xs:element name="InsideCallSeq" type="xs:int" minOccurs="0" />
            <xs:element name="RingbackCallSeq" type="xs:int" minOccurs="0" />
            <xs:element name="NoAnswerTime" type="xs:int" minOccurs="0" />
            <xs:element name="ForwardOnBusy" type="xs:boolean" minOccurs="0" />
            <xs:element name="BookConferenceWithPM" type="xs:boolean" minOccurs="0" />
            <xs:element name="DisableForwardOnInt" type="xs:boolean" minOccurs="0" />
            <xs:element name="DisableForwardUncondOnInt" type="xs:boolean"
minOccurs="0" />
            <xs:element name="DisableForwardBusyNoAnsOnInt" type="xs:boolean"
minOccurs="0" />
            <xs:element name="VoicemailReception2" type="xs:string" minOccurs="0" />
            <xs:element name="VoicemailReception3" type="xs:string" minOccurs="0" />
            <xs:element name="DSSKeys" type="csm:xmlDSSKeys" minOccurs="0" />
            <xs:element name="InhibitOffSwitchForwarding" type="xs:boolean"
minOccurs="0" />
            <xs:element name="IsNoUser" type="xs:boolean" minOccurs="0" />
            <xs:element name="IsRealUser" type="xs:boolean" minOccurs="0" />
            <xs:element name="IsRemoteManager" type="xs:boolean" minOccurs="0" />
            <xs:element name="IsVoiceEmailModeAlert" type="xs:boolean" minOccurs="0" />
            <xs:element name="IsVoiceEmailModeCopy" type="xs:boolean" minOccurs="0" />
            <xs:element name="IsVoiceEmailModeForward" type="xs:boolean" minOccurs="0" />
            <xs:element name="IsVoiceEmailModeOff" type="xs:boolean" minOccurs="0" />
            <xs:element name="MaxTwinnedCalls" type="xs:int" minOccurs="0" />
            <xs:element name="PhoneManagerCallStatusOptions" type="xs:long"
minOccurs="0" />
            <xs:element name="PhoneManagerCloseOptions" type="xs:int" minOccurs="0" />
            <xs:element name="PhoneManagerCanChange" type="xs:boolean" minOccurs="0" />
            <xs:element name="PhoneManagerConfigureOptions" type="xs:int" minOccurs="0" />
            <xs:element name="PhoneManagerOptions" type="xs:int" minOccurs="0" />
            <xs:element name="PhoneManagerOptionsOriginal" type="xs:int" minOccurs="0" />
            <xs:element name="PhoneType" type="xs:int" minOccurs="0" />
            <xs:element name="PhoneTypeIndex" type="xs:int" minOccurs="0" />
            <xs:element name="PopupAnswering" type="xs:boolean" minOccurs="0" />
            <xs:element name="PopupExternal" type="xs:boolean" minOccurs="0" />
            <xs:element name="PopupInternal" type="xs:boolean" minOccurs="0" />
            <xs:element name="PopupOutlook" type="xs:boolean" minOccurs="0" />
            <xs:element name="PopupRinging" type="xs:boolean" minOccurs="0" />
            <xs:element name="PopupOptions" type="xs:int" minOccurs="0" />
            <xs:element name="RingDelay" type="xs:int" minOccurs="0" />
            <xs:element name="ShowAccountCodes" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowAllCalls" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowCallStatus" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowCostOfCall" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowIncoming" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowMessages" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowMissed" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowOutgoing" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShowSpeedDials" type="xs:boolean" minOccurs="0" />
            <xs:element name="StartInCompactMode" type="xs:boolean" minOccurs="0" />
            <xs:element name="StayInCompactModeOnIncommingCall" type="xs:boolean"
minOccurs="0" />
            <xs:element name="StayInCompaceModeOnOutgoingCall" type="xs:boolean"
minOccurs="0" />
            <xs:element name="T3AllowThirdPartyFwd" type="xs:boolean" minOccurs="0" />
            <xs:element name="T3ProtectFromThirdPartyFwd" type="xs:boolean"
minOccurs="0" />
            <xs:element name="TwinnedDialDelay" type="xs:int" minOccurs="0" />
            <xs:element name="TwinnedEligibleForForwarded" type="xs:boolean"
minOccurs="0" />
            <xs:element name="TwinnedEligibleForGroup" type="xs:boolean" minOccurs="0" />
            <xs:element name="TwinnedMobileNumber" type="xs:string" minOccurs="0" />
            <xs:element name="TwinnedTimeProfile" type="xs:string" minOccurs="0" />
            <xs:element name="TwinningNumber" type="xs:string" minOccurs="0" />
            <xs:element name="TwinningType" type="xs:int" minOccurs="0" />
            <xs:element name="TwinningUser" type="xs:string" minOccurs="0" />
            <xs:element name="IsTwinSlave" type="xs:string" minOccurs="0" />
            <xs:element name="IsTwinMaster" type="xs:string" minOccurs="0" />
            <xs:element name="InternalTwinning" type="xs:boolean" minOccurs="0" />
            <xs:element name="MobilityTwinning" type="xs:boolean" minOccurs="0" />
            <xs:element name="TwinnedMobileAnswerGuard" type="xs:string" minOccurs="0" />
            <xs:element name="AutoRecMailBox" type="xs:string" minOccurs="0" />
            <xs:element name="ManualRecMailBox" type="xs:string" minOccurs="0" />
            <xs:element name="PAServicesEnabled" type="xs:string" minOccurs="0" />
            <xs:element name="AutoRecModeIn" type="xs:string" minOccurs="0" />
            <xs:element name="AutoRecModeOut" type="xs:string" minOccurs="0" />
            <xs:element name="DenyAutoIntercomCalls" type="xs:string" minOccurs="0" />
            <xs:element name="MobileCallControl" type="xs:boolean" minOccurs="0" />
            <xs:element name="SpecificBstType" type="xs:string" minOccurs="0" />
            <xs:element name="ForwardOnNoAnswer" type="xs:boolean" minOccurs="0" />
            <xs:element name="ForwardUnconditional" type="xs:boolean" minOccurs="0" />
            <xs:element name="ForwardHuntGroupCalls" type="xs:boolean" minOccurs="0" />
            <xs:element name="ForwardNumber" type="xs:string" minOccurs="0" />
            <xs:element name="ForwardBusyNumber" type="xs:string" minOccurs="0" />
            <xs:element name="DoNotDisturb" type="xs:boolean" minOccurs="0" />
            <xs:element name="DNDExceptions" type="xs:string" minOccurs="0" />
            <xs:element name="OutgoingCallBar" type="xs:boolean" minOccurs="0" />
            <xs:element name="IncomingCallBar" type="xs:boolean" minOccurs="0" />
            <xs:element name="OffHookStation" type="xs:boolean" minOccurs="0" />
            <xs:element name="BusyOnHeld" type="xs:boolean" minOccurs="0" />
            <xs:element name="FollowMeNumber" type="xs:string" minOccurs="0" />
            <xs:element name="CallWaitingOn" type="xs:boolean" minOccurs="0" />
            <xs:element name="VoicemailOn" type="xs:boolean" minOccurs="0" />
            <xs:element name="VoicemailHelp" type="xs:boolean" minOccurs="0" />
            <xs:element name="VoicemailCode" type="xs:string" minOccurs="0" />
            <xs:element name="VoicemailEmail" type="xs:string" minOccurs="0" />
            <xs:element name="VoicemailEmailReading" type="xs:boolean" minOccurs="0" />
            <xs:element name="VoicemailReception" type="xs:string" minOccurs="0" />
            <xs:element name="VoicemailEmailMode" type="xs:int" minOccurs="0" />
            <xs:element name="VoicemailRingback" type="xs:boolean" minOccurs="0" />
            <xs:element name="ShortCodes" type="csm:xmlShortCodes" minOccurs="0" />
            <xs:element name="DialInOn" type="xs:boolean" minOccurs="0" />
            <xs:element name="DialInTimeProfile" type="xs:string" minOccurs="0" />
            <xs:element name="DialInFirewallProfile" type="xs:string" minOccurs="0" />
            <xs:element name="SourceNumbers" type="xs:string" minOccurs="0" />
            <xs:element name="DialInQuotaTime" type="xs:int" minOccurs="0" />
            <xs:element name="LoginCode" type="xs:string" minOccurs="0" />
            <xs:element name="LoginIdleTime" type="xs:string" minOccurs="0" />
            <xs:element name="WrapUpTime" type="xs:int" minOccurs="0" />
            <xs:element name="TwinMaster" type="xs:string" minOccurs="0" />
            <xs:element name="SecTwinCallEnabled" type="xs:boolean" minOccurs="0" />
            <xs:element name="CanIntrude" type="xs:boolean" minOccurs="0" />
            <xs:element name="CannotBeIntruded" type="xs:boolean" minOccurs="0" />
            <xs:element name="XDirectory" type="xs:boolean" minOccurs="0" />
            <xs:element name="ForceLogin" type="xs:boolean" minOccurs="0" />
            <xs:element name="ForceAuthCode" type="xs:boolean" minOccurs="0" />
            <xs:element name="ForceAccountCode" type="xs:boolean" minOccurs="0" />
            <xs:element name="SystemPhone" type="xs:int" minOccurs="0" />
            <xs:element name="AbsentMsg" type="xs:int" minOccurs="0" />
            <xs:element name="AbsentSet" type="xs:int" minOccurs="0" />
            <xs:element name="AbsentText" type="xs:string" minOccurs="0" />
            <xs:element name="T3HuntGroupMembershipStatus" type="xs:string"
minOccurs="0" />
            <xs:element name="T3HuntGroupServiceStatus" type="xs:string" minOccurs="0" />
            <xs:element name="T3HuntGroupNightServiceStatus" type="xs:string"
minOccurs="0" />
            <xs:element name="T3DirectoryEntries" type="xs:string" minOccurs="0" />
            <xs:element name="MonitorGroup" type="xs:string" minOccurs="0" />
            <xs:element name="DisplayLocale" type="xs:string" minOccurs="0" />
            <xs:element name="Locale" type="xs:string" minOccurs="0" />
            <xs:element name="PMType" type="xs:int" minOccurs="0" />
            <xs:element name="InboundAutoRecord" type="xs:int" minOccurs="0" />
            <xs:element name="OutboundAutoRecord" type="xs:int" minOccurs="0" />
            <xs:element name="AutoRecordTimeProfile" type="xs:string" minOccurs="0" />
            <xs:element name="RemoteWorker" type="xs:boolean" minOccurs="0" />
            <xs:element name="CanAcceptCollectCalls" type="xs:boolean" minOccurs="0" />
            <xs:element name="UserRights" type="xs:string" minOccurs="0" />
            <xs:element name="Secretaries" type="xs:string" minOccurs="0" />
            <xs:element name="TransferReturnTime" type="xs:string" minOccurs="0" />
            <xs:element name="AnswerCallWaiting" type="xs:boolean" minOccurs="0" />
            <xs:element name="RingingLinePreference" type="xs:boolean" minOccurs="0" />
            <xs:element name="IdleLinePreference" type="xs:boolean" minOccurs="0" />
            <xs:element name="CoverageTime" type="xs:int" minOccurs="0" />
            <xs:element name="AutoVRL" type="xs:int" minOccurs="0" />
            <xs:element name="ManualVRL" type="xs:int" minOccurs="0" />
            <xs:element name="DelayedRingPreference" type="xs:boolean" minOccurs="0" />
            <xs:element name="AnswerPreSelect" type="xs:boolean" minOccurs="0" />
            <xs:element name="ReserveLastCA" type="xs:boolean" minOccurs="0" />
            <xs:element name="CallTracingOn" type="xs:boolean" minOccurs="0" />
            <xs:element name="DisplayCharges" type="xs:boolean" minOccurs="0" />
            <xs:element name="MarkUpFactor" type="xs:int" minOccurs="0" />
            <xs:element name="reset_longest_idle_info" type="xs:int" minOccurs="0" />
            <xs:element name="NoAnswerStatus" type="xs:int" minOccurs="0" />
            <xs:element name="PBXAddress" type="xs:string" minOccurs="0" />
            <xs:element name="SIPName" type="xs:string" minOccurs="0" />
            <xs:element name="SIPDisplayName" type="xs:string" minOccurs="0" />
            <xs:element name="SIPContact" type="xs:string" minOccurs="0" />
            <xs:element name="SIPAnonymous" type="xs:boolean" minOccurs="0" />
            <xs:element name="AbbreviatedRing" type="xs:boolean" minOccurs="0" />
            <xs:element name="CustomerServiceRep" type="xs:boolean" minOccurs="0" />
            <xs:element name="ACWTime" type="xs:int" minOccurs="0" />
            <xs:element name="AutoACW" type="xs:boolean" minOccurs="0" />
            <xs:element name="UMSWebServices" type="xs:boolean" minOccurs="0" />
            <xs:element name="DisableVMOnFU" type="xs:boolean" minOccurs="0" />
            <xs:element name="DTMFCallCtrl" type="xs:boolean" minOccurs="0" />
            <xs:element name="LoggedOutTwinning" type="xs:int" minOccurs="0" />
            <xs:element name="OneXClient" type="xs:boolean" minOccurs="0" />
            <xs:element name="MobilityFeatures" type="xs:boolean" minOccurs="0" />
            <xs:element name="TwinnedBridgeAppearances" type="xs:boolean" minOccurs="0" />
            <xs:element name="TwinnedCoverageAppearances" type="xs:boolean"
minOccurs="0" />
            <xs:element name="TwinnedLineAppearances" type="xs:boolean" minOccurs="0" />
            <xs:element name="PersonalDirectory" type="xs:string" minOccurs="0" />
            <xs:element name="ForwardToVoicemail" type="xs:boolean" minOccurs="0" />
            <xs:element name="CoverageGroup" type="xs:string" minOccurs="0" />
            <xs:element name="CanChangeHGOOSGroup" type="xs:string" minOccurs="0" />
            <xs:element name="CanChangeHGONGroup" type="xs:string" minOccurs="0" />
            <xs:element name="IncludeForwardInMenu" type="xs:boolean" minOccurs="0" />
            <xs:element name="CallLoggingCentralised" type="xs:string" minOccurs="0" />
            <xs:element name="AttentionRing" type="xs:string" minOccurs="0" />
            <xs:element name="CoverageRing" type="xs:string" minOccurs="0" />
            <xs:element name="LogMissedCallsForHG" type="xs:string" minOccurs="0" />
            <xs:element name="DisableForwardToVoicemail" type="xs:int" minOccurs="0" />
            <xs:element name="AnnouncementsOn" type="xs:boolean" minOccurs="0" />
            <xs:element name="FollowAnnouncementsOn" type="xs:boolean" minOccurs="0" />
            <xs:element name="LoopAnnouncementsOn" type="xs:boolean" minOccurs="0" />
            <xs:element name="SyncAnnouncementsOn" type="xs:boolean" minOccurs="0" />
            <xs:element name="FirstAnnTime" type="xs:int" minOccurs="0" />
            <xs:element name="SecondAnnTime" type="xs:int" minOccurs="0" />
            <xs:element name="BetweenAnnTime" type="xs:int" minOccurs="0" />
            <xs:element name="PostAnnTone" type="xs:int" minOccurs="0" />
            <xs:element name="PortalServices" type="xs:int" minOccurs="0" />
            <xs:element name="WorkingHoursUserRightsGroup" type="xs:string"
minOccurs="0" />
            <xs:element name="T3SelfAdmin" type="xs:string" minOccurs="0" />
            <xs:element name="MobileCallback" type="xs:boolean" minOccurs="0" />
            <xs:element name="Receptionist" type="xs:boolean" minOccurs="0" />
            <xs:element name="SoftPhone" type="xs:boolean" minOccurs="0" />
            <xs:element name="OneXTelecommuter" type="xs:boolean" minOccurs="0" />
            <xs:element name="AssignedPackage" type="xs:int" minOccurs="0" />
            <xs:element name="AutoRecMode" type="xs:int" minOccurs="0" />
            <xs:element name="CallLogTimeout" type="xs:string" minOccurs="0" />
            <xs:element name="UserCLI" type="xs:string" minOccurs="0" />
            <xs:element name="FlareEnabled" type="xs:boolean" minOccurs="0" />
            <xs:element name="FlareMode" type="xs:int" minOccurs="0" />
            <xs:element name="AutoIntDeny" type="xs:boolean" minOccurs="0" />
            <xs:element name="TUIUser" type="csm:xmlTUIUser" minOccurs="0" />
            <xs:element name="UserPasswordStatus" type="xs:int" minOccurs="0" />
            <xs:element name="BlockForwarding" type="xs:boolean" minOccurs="0" />
            <xs:element name="ParkAndPageInfo" type="csm:xmlParkAndPageInfo"
minOccurs="0" />
            <xs:element name="MobileVoIPClientEnabled" type="xs:boolean" minOccurs="0" />
            <xs:element name="SendMobilityEmail" type="xs:boolean" minOccurs="0" />
            <xs:element name="IPOCCAgent" type="xs:boolean" minOccurs="0" />
            <xs:element name="AgentType" type="xs:string" minOccurs="0" />
            <xs:element name="WebCollaboration" type="xs:boolean" minOccurs="0" />
            <xs:element name="ConferencePIN" type="xs:string" minOccurs="0" />
        </xs:sequence>
        <xs:attribute name="GUID" type="xs:string" />
    </xs:complexType>

    <xs:complexType name="xmlDSSKeys">
        <xs:sequence>
            <xs:element minOccurs="0" maxOccurs="unbounded" name="DSSKey"
                type="csm:xmlDSSKey"/>

        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlDSSKey">
        <xs:sequence>
            <xs:element name="KeyType" type="xs:int" minOccurs="0"/>
            <xs:element name="Label" type="xs:string" minOccurs="0" />
            <xs:element name="ActionObject" type="xs:string" minOccurs="0" />
            <xs:element name="Data" type="xs:string" minOccurs="0" />
            <xs:element name="RingDelay" type="xs:int" minOccurs="0" />
            <xs:element name="IdlePos" type="xs:string" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="Key" type="xs:int" />
    </xs:complexType>


    <xs:complexType name="xmlShortCodes">
        <xs:sequence>
            <xs:element minOccurs="0" maxOccurs="unbounded" name="ShortCode"
                type="csm:xmlShortCode"  />

        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlShortCode">
        <xs:sequence>
            <xs:element name="Code" type="xs:string" minOccurs="0" />
            <xs:element name="TelephoneNumber" type="xs:string" minOccurs="0" />
            <xs:element name="LineGroupId" type="xs:int" minOccurs="0" />
            <xs:element name="Feature" type="xs:string" minOccurs="0" />
            <xs:element name="Locale" type="xs:string" minOccurs="0" />
            <xs:element name="ForceAccountCode" type="xs:boolean" minOccurs="0" />
            <xs:element name="ForceAuthCode" type="xs:boolean" minOccurs="0" />
        </xs:sequence>
        <xs:attribute name="GUID" type="xs:string" />
    </xs:complexType>

    <xs:complexType name="xmlVoip">
        <xs:sequence>
            <xs:element name="GatekeeperPrimaryIPAddress" type="xs:string"
minOccurs="0" />
            <xs:element name="GatekeeperSecondaryIPAddress" type="xs:string"
minOccurs="0" />
            <xs:element name="IPAddress" type="xs:string" minOccurs="0" />
            <xs:element name="EnableFaststart" type="xs:boolean" minOccurs="0" />
            <xs:element name="FaxTransportSupport" type="xs:boolean" minOccurs="0" />
            <xs:element name="FaxTransportMethod" type="xs:int" minOccurs="0" />
            <xs:element name="CodecLockdown" type="xs:boolean" minOccurs="0" />
            <xs:element name="LocalHoldMusic" type="xs:boolean" minOccurs="0" />
            <xs:element name="LocalTones" type="xs:boolean" minOccurs="0" />
            <xs:element name="RSVPEnabled" type="xs:boolean" minOccurs="0" />
            <xs:element name="OOB_DTMF" type="xs:boolean" minOccurs="0" />
            <xs:element name="AllowDirectMedia" type="xs:boolean" minOccurs="0" />
            <xs:element name="H450Support" type="xs:int" minOccurs="0" />
            <xs:element name="AnnexlSupport" type="xs:boolean" minOccurs="0" />
            <xs:element name="InputGain" type="xs:int" minOccurs="0" />
            <xs:element name="OutputGain" type="xs:int" minOccurs="0" />
            <xs:element name="MediaSecurity" type="xs:int" minOccurs="0" />
            <xs:element name="RTP_Authentication" type="xs:boolean" minOccurs="0" />
            <xs:element name="RTP_Encryption" type="xs:boolean" minOccurs="0" />
            <xs:element name="RTCP_Authentication" type="xs:boolean" minOccurs="0" />
            <xs:element name="RTCP_Encryption" type="xs:boolean" minOccurs="0" />
            <xs:element name="SRTP_Window_Size" type="xs:string" minOccurs="0" />
            <xs:element name="Crypto_Suite_SHA_80" type="xs:boolean" minOccurs="0" />
            <xs:element name="Crypto_Suite_SHA_32" type="xs:boolean" minOccurs="0" />
            <xs:element name="CodecSelection" type="xs:string" minOccurs="0" />
            <xs:element name="SupplementaryServices" type="xs:int" minOccurs="0" />
            <xs:element name="DTMFSupport" type="xs:int" minOccurs="0" />
            <xs:element name="ReinviteSupported" type="xs:boolean" minOccurs="0" />
            <xs:element name="IsMediaSecurityCustom" type="xs:boolean" minOccurs="0" />
            <xs:element name="UseAdvancedCodecPrefs" type="xs:boolean" minOccurs="0" />
            <xs:element name="AdvancedCodecPrefs" type="csm:xmlAdvancedCodecPrefs"
minOccurs="0" />
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlSipExtn">
        <xs:sequence>
            <xs:element name="ForceAuthentication" type="xs:boolean" minOccurs="0" />
            <xs:element name="Rel100Supported" type="xs:string" minOccurs="0" />
            <xs:element name="T38Fax" type="csm:xmlT38Fax" minOccurs="0" />
            <xs:element name="SIP3rdPartyAutoAnswer" type="xs:string" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlExtnDS">
        <xs:sequence>
            <xs:element name="AdmmUseHandsetConfig" type="xs:boolean" minOccurs="0" />
            <xs:element name="AdmmType" type="xs:int" minOccurs="0" />
            <xs:element name="AdmmIpei" type="xs:int" minOccurs="0" />
            <xs:element name="AdmmAnonymous" type="xs:boolean" minOccurs="0" />

        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlT38Fax">
```

```
        <xs:sequence>
            <xs:element name="Defaulted" type="xs:string" minOccurs="0" />
            <xs:element name="T38FaxVersion" type="xs:string" minOccurs="0" />
            <xs:element name="RedundancyLowSpeed" type="xs:string" minOccurs="0" />
            <xs:element name="RedundancyHighSpeed" type="xs:string" minOccurs="0" />
            <xs:element name="NSFOveride" type="xs:string" minOccurs="0" />
            <xs:element name="NSFCountryCode" type="xs:string" minOccurs="0" />
            <xs:element name="NSFVendorCode" type="xs:string" minOccurs="0" />
            <xs:element name="TxNetworkTimeout" type="xs:string" minOccurs="0" />
            <xs:element name="ScanLineFixup" type="xs:string" minOccurs="0" />
            <xs:element name="TopEnhancement" type="xs:string" minOccurs="0" />
            <xs:element name="DisableT30ECM" type="xs:string" minOccurs="0" />
            <xs:element name="DisableT30MR" type="xs:string" minOccurs="0" />
            <xs:element name="DisableEFlagsForFirstDis" type="xs:string" minOccurs="0" />
            <xs:element name="EflagStartTimer" type="xs:string" minOccurs="0" />
            <xs:element name="EflagStopTimer" type="xs:string" minOccurs="0" />
            <xs:element name="FaxTransport" type="xs:string" minOccurs="0" />
            <xs:element name="TCFMethod" type="xs:int" minOccurs="0" />
            <xs:element name="MaxFaxRate" type="xs:int" minOccurs="0" />
            <xs:element name="G711FaxEcanEnabled" type="xs:string" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlD100Extn">
        <xs:sequence>
            <xs:element name="ForceAuthentication" type="xs:boolean" minOccurs="0" />
            <xs:element name="RemoteLineNumber" type="xs:int" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlTUIUser">
        <xs:sequence>
            <xs:element name="TUIFeaturesMenuControls" type="xs:boolean" minOccurs="0" />
            <xs:element name="TUIFeaturesMenu" type="xs:boolean" minOccurs="0" />
            <xs:element name="TUIBasicCallFunctions" type="xs:boolean" minOccurs="0" />
            <xs:element name="TUIAdvancedCallFunctions" type="xs:boolean" minOccurs="0" />
            <xs:element name="TUIHotDeskFunctions" type="xs:boolean" minOccurs="0" />
            <xs:element name="TUIPasscodeChange" type="xs:boolean" minOccurs="0" />
            <xs:element name="TUIPhoneLock" type="xs:boolean" minOccurs="0" />
            <xs:element name="TUISelfAdmin" type="xs:boolean" minOccurs="0" />
            <xs:element name="TUIVoiceMailControls" type="xs:boolean" minOccurs="0" />
            <xs:element name="TUIForwarding" type="xs:boolean" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlParkAndPageInfo">
        <xs:sequence>
            <xs:element name="ParkAndPage" type="csm:xmlParkAndPage" minOccurs="0" 
maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlParkAndPage">
        <xs:sequence>
            <xs:element name="ParkAndPageId" type="xs:string" minOccurs="0" />
            <xs:element name="PagingNumber" type="xs:string" minOccurs="0" />
            <xs:element name="CentrexTransferNumber" type="xs:string" minOccurs="0" />
            <xs:element name="PNPFallBackNumber" type="xs:string" minOccurs="0" />
            <xs:element name="RetryTimeout" type="xs:string" minOccurs="0" />
            <xs:element name="RetryCount" type="xs:string" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlAdvancedCodecPrefs">
        <xs:sequence>
```

```
      <xs:element name="CodecPref" type="xs:string" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

 <xs:complexType name="xmlEUAuth">
  <xs:sequence>
   <xs:element type="xs:string" name="EUAEnable"/>
   <xs:element type="xs:string" name="EUAName"/>
   <xs:element type="xs:string" name="EUAPassword"/>
   <xs:element type="xs:string" name="EUAFullName"/>
   <xs:element type="xs:string" name="EUAExtension"/>
   <xs:element type="xs:string" name="EUALocale"/>
   <xs:element type="xs:string" name="EUADoNotDisturb"/>
   <xs:element type="xs:string" name="EUADNDExceptions"/>
   <xs:element type="xs:string" name="EUAVoicemailOn"/>
   <xs:element type="xs:string" name="EUAVoicemailCode"/>
   <xs:element type="xs:string" name="EUAVoicemailEmail"/>
   <xs:element type="xs:string" name="EUAVoicemailEmailMode"/>
   <xs:element type="xs:string" name="EUAMobilityTwinning"/>
   <xs:element type="xs:string" name="EUATwinnedMobileNumber"/>
   <xs:element type="xs:string" name="EUALoginCode"/>
   <xs:element type="xs:string" name="EUADenyAutoIntercomCalls"/>
   <xs:element type="xs:string" name="EUAPersonalDirectory"/>
   <xs:element type="xs:string" name="EUAShortCodes"/>
   <xs:element type="xs:string" name="EUABlockForwarding"/>
   <xs:element type="xs:string" name="EUAForwardNumber"/>
   <xs:element type="xs:string" name="EUAForwardBusyNumber"/>
   <xs:element type="xs:string" name="EUAForwardOnBusy"/>
   <xs:element type="xs:string" name="EUAForwardOnNoAnswer"/>
   <xs:element type="xs:string" name="EUADSSKeys"/>
   <xs:element type="xs:string" name="EUAVoicemailRingback"/>
   <xs:element type="xs:string" name="EUAConferencePIN"/>
  </xs:sequence>
 </xs:complexType>

</xs:schema>
```

Sample XML for the IP Office Communication 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>
  <givenName>test09</givenName>
  <loginName>test09@avaya.com</loginName>
  <middleName />
  <surname>test09</surname>
  <userPassword/>
  <commPassword />
  <commProfileSet>
   <commProfileSetName>Primary</commProfileSetName>
   <isPrimary>true</isPrimary>
   <commProfileList>
    <commProfile xsi:type="csm:xmlB5800UserProfile" xmlns:csm="http://xml.avaya.com/
schema/import_csm_b5800">
     <commProfileType>IP Office</commProfileType>
     <csm:deviceName>Sanjeet_IPO</csm:deviceName>
     <csm:useExistingExt>true</csm:useExistingExt>
     <csm:extension>207</csm:extension>
     <csm:extensionType>Digital</csm:extensionType>
     <csm:deleteExtOnUserDelete>true</csm:deleteExtOnUserDelete>
     <csm:data>
```

```
            <csm:ws_object>
              <csm:Extension>
                <csm:Id>1</csm:Id>
                <csm:SubId>0</csm:SubId>
                <csm:Extension>207</csm:Extension>
                <csm:TypeInfo>15</csm:TypeInfo>
                <csm:CallerDisplayType>1</csm:CallerDisplayType>
                <csm:MessageLampType>4</csm:MessageLampType>
                <csm:ExtnClassification>0</csm:ExtnClassification>
                <csm:LineType>6</csm:LineType>
                <csm:MinFlashPulseWidth>2</csm:MinFlashPulseWidth>
                <csm:MaxFlashPulseWidth>50</csm:MaxFlashPulseWidth>
                <csm:UseSystemFlashHook>true</csm:UseSystemFlashHook>
                <csm:ResetVolumeAfterCalls>false</csm:ResetVolumeAfterCalls>
                <csm:DisconnectPulseWidth>80</csm:DisconnectPulseWidth>
                <csm:HookPersistency>100</csm:HookPersistency>
                <csm:Mac>000000000000</csm:Mac>
                <csm:SilenceSuppression>false</csm:SilenceSuppression>
                <csm:VoicePktSize>160</csm:VoicePktSize>
                <csm:VoiceCompression>0</csm:VoiceCompression>
                <csm:voip>
                  <csm:GatekeeperPrimaryIPAddress>0.0.0.0</csm:GatekeeperPrimaryIPAddress>
                  <csm:GatekeeperSecondaryIPAddress>0.0.0.0</
csm:GatekeeperSecondaryIPAddress>
                  <csm:IPAddress>0.0.0.0</csm:IPAddress>
                  <csm:EnableFaststart>false</csm:EnableFaststart>
                  <csm:FaxTransportSupport>false</csm:FaxTransportSupport>
                  <csm:FaxTransportMethod>3</csm:FaxTransportMethod>
                  <csm:CodecLockdown>false</csm:CodecLockdown>
                  <csm:LocalHoldMusic>false</csm:LocalHoldMusic>
                  <csm:LocalTones>false</csm:LocalTones>
                  <csm:RSVPEnabled>false</csm:RSVPEnabled>
                  <csm:OOB_DTMF>true</csm:OOB_DTMF>
                  <csm:AllowDirectMedia>true</csm:AllowDirectMedia>
                  <csm:H450Support>2</csm:H450Support>
                  <csm:AnnexlSupport>false</csm:AnnexlSupport>
                  <csm:InputGain>0</csm:InputGain>
                  <csm:OutputGain>0</csm:OutputGain>
                  <csm:MediaSecurity>0</csm:MediaSecurity>
                  <csm:RTP_Authentication>true</csm:RTP_Authentication>
                  <csm:RTP_Encryption>true</csm:RTP_Encryption>
                  <csm:RTCP_Authentication>true</csm:RTCP_Authentication>
                  <csm:RTCP_Encryption>false</csm:RTCP_Encryption>
                  <csm:SRTP_Window_Size>64</csm:SRTP_Window_Size>
                  <csm:Crypto_Suite_SHA_80>true</csm:Crypto_Suite_SHA_80>
                  <csm:Crypto_Suite_SHA_32>false</csm:Crypto_Suite_SHA_32>
                  <csm:CodecSelection>SystemDefault</csm:CodecSelection>
                  <csm:SupplementaryServices>2</csm:SupplementaryServices>
                  <csm:DTMFSupport>2</csm:DTMFSupport>
                  <csm:ReinviteSupported>true</csm:ReinviteSupported>
                  <csm:IsMediaSecurityCustom>false</csm:IsMediaSecurityCustom>
                </csm:voip>
                <csm:RenegotiationSupported>true</csm:RenegotiationSupported>
                <csm:RenegotiateBeforeConnect>false</csm:RenegotiateBeforeConnect>
                <csm:UseVocoder>false</csm:UseVocoder>
                <csm:EarlyH245Supported>false</csm:EarlyH245Supported>
                <csm:RFC2833>false</csm:RFC2833>
                <csm:MediaWait>false</csm:MediaWait>
                <csm:MediaOnOverlap>false</csm:MediaOnOverlap>
                <csm:PauseRequired>false</csm:PauseRequired>
                <csm:PauseOnEndRequired>false</csm:PauseOnEndRequired>
                <csm:ParallelH245>false</csm:ParallelH245>
                <csm:AnnexFSupported>false</csm:AnnexFSupported>
                <csm:PhoneType>47</csm:PhoneType>
                <csm:ExtnAPIAudio_setting>0</csm:ExtnAPIAudio_setting>
                <csm:ExtnAPIHeadset_setting>0</csm:ExtnAPIHeadset_setting>
                <csm:ExtnAPIContrast>0</csm:ExtnAPIContrast>
                <csm:ExtnAPIRedial_time>0</csm:ExtnAPIRedial_time>
                <csm:ExtnAPISpeaker_volume>0</csm:ExtnAPISpeaker_volume>
                <csm:ExtnAPIHandsfree_settings>0</csm:ExtnAPIHandsfree_settings>
                <csm:ExtnAPIRingtone_volume>0</csm:ExtnAPIRingtone_volume>
                <csm:ExtnAPIDoor_phone>false</csm:ExtnAPIDoor_phone>
                <csm:ExtnAPIHandset_volume>0</csm:ExtnAPIHandset_volume>
                <csm:ExtnAPIRingtone_speed>0</csm:ExtnAPIRingtone_speed>
                <csm:ExtnAPIHeadset_volume>0</csm:ExtnAPIHeadset_volume>
                <csm:ExtnAPIHeadset_config>0</csm:ExtnAPIHeadset_config>
                <csm:ExtnAPIAlpha_keypad_layout>0</csm:ExtnAPIAlpha_keypad_layout>
                <csm:ExtnAPIDirect_dial_enabled>false</csm:ExtnAPIDirect_dial_enabled>
                <csm:ExtnAPIHandsfree_enabled>false</csm:ExtnAPIHandsfree_enabled>
                <csm:DisableSpeaker>false</csm:DisableSpeaker>
                <csm:VPNExtn>false</csm:VPNExtn>
                <csm:IPAvayaLicenseReserved>false</csm:IPAvayaLicenseReserved>
                <csm:IPEndpointsLicenseReserved>false</csm:IPEndpointsLicenseReserved>
                <csm:IsExtnCentralized>false</csm:IsExtnCentralized>
                <csm:CentralizedDDINumber>||||</csm:CentralizedDDINumber>
                <csm:SpecificBstType>-1</csm:SpecificBstType>
                <csm:Location>1</csm:Location>
                <csm:PhonePassword />
                <csm:Module></csm:Module>
                <csm:Port></csm:Port>
                <csm:AllowRemoteExtn>false</csm:AllowRemoteExtn>
                <csm:FallbackAsRemoteWorker>0</csm:FallbackAsRemoteWorker>
                <csm:RingVoltageBoost>0</csm:RingVoltageBoost>
                <csm:RemoteLineNumber>-1</csm:RemoteLineNumber>
              </csm:Extension>
              <csm:User>
                <csm:EUAuth>
                  <csm:EUAEnable>0</csm:EUAEnable>
                  <csm:EUAName>0</csm:EUAName>
                  <csm:EUAPassword>0</csm:EUAPassword>
                  <csm:EUAFullName>0</csm:EUAFullName>
                  <csm:EUAExtension>0</csm:EUAExtension>
                  <csm:EUALocale>0</csm:EUALocale>
                  <csm:EUADoNotDisturb>0</csm:EUADoNotDisturb>
                  <csm:EUADNDExceptions>0</csm:EUADNDExceptions>
                  <csm:EUAVoicemailOn>0</csm:EUAVoicemailOn>
                  <csm:EUAVoicemailCode>0</csm:EUAVoicemailCode>
                  <csm:EUAVoicemailEmail>0</csm:EUAVoicemailEmail>
                  <csm:EUAVoicemailEmailMode>0</csm:EUAVoicemailEmailMode>
                  <csm:EUAMobilityTwinning>0</csm:EUAMobilityTwinning>
                  <csm:EUATwinnedMobileNumber>0</csm:EUATwinnedMobileNumber>
                  <csm:EUALoginCode>0</csm:EUALoginCode>
                  <csm:EUADenyAutoIntercomCalls>0</csm:EUADenyAutoIntercomCalls>
                  <csm:EUAPersonalDirectory>0</csm:EUAPersonalDirectory>
                  <csm:EUAShortCodes>0</csm:EUAShortCodes>
                  <csm:EUABlockForwarding>0</csm:EUABlockForwarding>
                  <csm:EUAForwardNumber>0</csm:EUAForwardNumber>
                  <csm:EUAForwardBusyNumber>0</csm:EUAForwardBusyNumber>
                  <csm:EUAForwardOnBusy>0</csm:EUAForwardOnBusy>
                  <csm:EUAForwardOnNoAnswer>0</csm:EUAForwardOnNoAnswer>
                  <csm:EUADSSKeys>0</csm:EUADSSKeys>
                  <csm:EUAVoicemailRingback>0</csm:EUAVoicemailRingback>
                  <csm:EUAConferencePIN>0</csm:EUAConferencePIN>
                </csm:EUAuth>
                <csm:UserRightsView />
                <csm:UsingView>false</csm:UsingView>
                <csm:UserRightsTimeProfile />
                <csm:OutOfHoursUserRights />
                <csm:Name>test09</csm:Name>
                <csm:KName />
                <csm:Password>test09</csm:Password>
                <csm:FullName />
                <csm:Extension>207</csm:Extension>
                <csm:Priority>1</csm:Priority>
                <csm:OutsideCallSeq>0</csm:OutsideCallSeq>
                <csm:InsideCallSeq>0</csm:InsideCallSeq>
                <csm:RingbackCallSeq>0</csm:RingbackCallSeq>
                <csm:NoAnswerTime>15</csm:NoAnswerTime>
                <csm:ForwardOnBusy>false</csm:ForwardOnBusy>
                <csm:BookConferenceWithPM>false</csm:BookConferenceWithPM>
                <csm:DisableForwardOnInt>false</csm:DisableForwardOnInt>
                <csm:DisableForwardUncondOnInt>false</csm:DisableForwardUncondOnInt>
                <csm:DisableForwardBusyNoAnsOnInt>false</csm:DisableForwardBusyNoAnsOnInt>
                <csm:VoicemailReception2 />
                <csm:VoicemailReception3 />
                <csm:DSSKeys>
                  <csm:DSSKey Key="1">
                    <csm:KeyType>0</csm:KeyType>
                    <csm:Label />
                    <csm:ActionObject>39</csm:ActionObject>
                    <csm:Data>a=</csm:Data>
                    <csm:RingDelay>0</csm:RingDelay>
                    <csm:IdlePos />
                  </csm:DSSKey>
                  <csm:DSSKey Key="2">
                    <csm:KeyType>0</csm:KeyType>
                    <csm:Label />
                    <csm:ActionObject>39</csm:ActionObject>
                    <csm:Datab>=</csm:Data>
                    <csm:RingDelay>0</csm:RingDelay>
                    <csm:IdlePos />
                  </csm:DSSKey>
                  <csm:DSSKey Key="3">
                    <csm:KeyType>0</csm:KeyType>
                    <csm:Label />
                    <csm:ActionObject>39</csm:ActionObject>
                    <csm:Data>c=</csm:Data>
                    <csm:RingDelay>0</csm:RingDelay>
                    <csm:IdlePos />
                  </csm:DSSKey>
                </csm:DSSKeys>
                <csm:InhibitOffSwitchForwarding>false</csm:InhibitOffSwitchForwarding>
                <csm:IsNoUser>false</csm:IsNoUser>
                <csm:IsRealUser>true</csm:IsRealUser>
                <csm:IsRemoteManager>false</csm:IsRemoteManager>
                <csm:IsVoiceEmailModeAlert>false</csm:IsVoiceEmailModeAlert>
                <csm:IsVoiceEmailModeCopy>false</csm:IsVoiceEmailModeCopy>
                <csm:IsVoiceEmailModeForward>false</csm:IsVoiceEmailModeForward>
                <csm:IsVoiceEmailModeOff>true</csm:IsVoiceEmailModeOff>
                <csm:MaxTwinnedCalls>1</csm:MaxTwinnedCalls>
                <csm:PhoneManagerCallStatusOptions>4294967295</
csm:PhoneManagerCallStatusOptions>
                <csm:PhoneManagerCloseOptions>0</csm:PhoneManagerCloseOptions>
                <csm:PhoneManagerCanChange>true</csm:PhoneManagerCanChange>
                <csm:PhoneManagerConfigureOptions>81664</csm:PhoneManagerConfigureOptions>
                <csm:PhoneManagerOptions>98120</csm:PhoneManagerOptions>
                <csm:PhoneManagerOptionsOriginal>98120</csm:PhoneManagerOptionsOriginal>
                <csm:PhoneType>47</csm:PhoneType>
                <csm:PhoneTypeIndex>47</csm:PhoneTypeIndex>
                <csm:PopupAnswering>false</csm:PopupAnswering>
                <csm:PopupExternal>false</csm:PopupExternal>
                <csm:PopupInternal>false</csm:PopupInternal>
                <csm:PopupOutlook>false</csm:PopupOutlook>
                <csm:PopupRinging>false</csm:PopupRinging>
                <csm:PopupOptions>0</csm:PopupOptions>
                <csm:RingDelay>0</csm:RingDelay>
                <csm:ShowAccountCodes>true</csm:ShowAccountCodes>
                <csm:ShowAllCalls>true</csm:ShowAllCalls>
                <csm:ShowCallStatus>true</csm:ShowCallStatus>
                <csm:ShowCostOfCall>true</csm:ShowCostOfCall>
                <csm:ShowIncoming>true</csm:ShowIncoming>
                <csm:ShowMessages>true</csm:ShowMessages>
                <csm:ShowMissed>true</csm:ShowMissed>
                <csm:ShowOutgoing>true</csm:ShowOutgoing>
                <csm:ShowSpeedDials>true</csm:ShowSpeedDials>
                <csm:StartInCompactMode>false</csm:StartInCompactMode>
                <csm:StayInCompactModeOnIncommingCall>false</
csm:StayInCompactModeOnIncommingCall>
                <csm:StayInCompaceModeOnOutgoingCall>false</
csm:StayInCompaceModeOnOutgoingCall>
                <csm:T3AllowThirdPartyFwd>false</csm:T3AllowThirdPartyFwd>
                <csm:T3ProtectFromThirdPartyFwd>false</csm:T3ProtectFromThirdPartyFwd>
                <csm:TwinnedDialDelay>2</csm:TwinnedDialDelay>
                <csm:TwinnedEligibleForForwarded>false</csm:TwinnedEligibleForForwarded>
                <csm:TwinnedEligibleForGroup>false</csm:TwinnedEligibleForGroup>
                <csm:TwinnedMobileNumber />
                <csm:TwinnedTimeProfile />
                <csm:TwinningNumber />
                <csm:TwinningType>0</csm:TwinningType>
                <csm:TwinningUser />
                <csm:IsTwinSlave>false</csm:IsTwinSlave>
                <csm:IsTwinMaster>false</csm:IsTwinMaster>
                <csm:InternalTwinning>false</csm:InternalTwinning>
                <csm:MobilityTwinning>false</csm:MobilityTwinning>
                <csm:TwinnedMobileAnswerGuard>0</csm:TwinnedMobileAnswerGuard>
                <csm:AutoRecMailBox>207 test21</csm:AutoRecMailBox>
                <csm:ManualRecMailBox>207 test21</csm:ManualRecMailBox>
                <csm:PAServicesEnabled>false</csm:PAServicesEnabled>
                <csm:AutoRecModeIn>2</csm:AutoRecModeIn>
                <csm:AutoRecModeOut>2</csm:AutoRecModeOut>
                <csm:DenyAutoIntercomCalls>false</csm:DenyAutoIntercomCalls>
                <csm:MobileCallControl>false</csm:MobileCallControl>
                <csm:SpecificBstType>47</csm:SpecificBstType>
                <csm:ForwardOnNoAnswer>false</csm:ForwardOnNoAnswer>
                <csm:ForwardUnconditional>false</csm:ForwardUnconditional>
                <csm:ForwardHuntGroupCalls>false</csm:ForwardHuntGroupCalls>
                <csm:ForwardNumber />
                <csm:ForwardBusyNumber />
                <csm:DoNotDisturb>false</csm:DoNotDisturb>
                <csm:DNDExceptions />
                <csm:OutgoingCallBar>false</csm:OutgoingCallBar>
                <csm:IncomingCallBar>false</csm:IncomingCallBar>
                <csm:OffHookStation>false</csm:OffHookStation>
                <csm:BusyOnHeld>false</csm:BusyOnHeld>
                <csm:FollowMeNumber />
                <csm:CallWaitingOn>false</csm:CallWaitingOn>
                <csm:VoicemailOn>true</csm:VoicemailOn>
                <csm:VoicemailHelp>false</csm:VoicemailHelp>
                <csm:VoicemailCode />
                <csm:VoicemailEmail />
                <csm:VoicemailEmailReading>false</csm:VoicemailEmailReading>
                <csm:VoicemailReception />
                <csm:VoicemailEmailMode>0</csm:VoicemailEmailMode>
                <csm:VoicemailRingback>false</csm:VoicemailRingback>
                <csm:ShortCodes>
                  <csm:ShortCode>
                    <csm:Code>*DSS1</csm:Code>
                    <csm:TelephoneNumber>99/a=</csm:TelephoneNumber>
                    <csm:LineGroupId>0</csm:LineGroupId>
                    <csm:Feature>26</csm:Feature>
                    <csm:Locale />
                    <csm:ForceAccountCode>false</csm:ForceAccountCode>
                    <csm:ForceAuthCode>false</csm:ForceAuthCode>
                  </csm:ShortCode>
                  <csm:ShortCode>
                    <csm:Code>*DSS2</csm:Code>
                    <csm:TelephoneNumber>99/b=</csm:TelephoneNumber>
                    <csm:LineGroupId>0</csm:LineGroupId>
                    <csm:Feature>26</csm:Feature>
                    <csm:Locale />
                    <csm:ForceAccountCode>false</csm:ForceAccountCode>
                    <csm:ForceAuthCode>false</csm:ForceAuthCode>
                  </csm:ShortCode>
                  <csm:ShortCode>
                    <csm:Code>*DSS3</csm:Code>
                    <csm:TelephoneNumber>99/c=</csm:TelephoneNumber>
                    <csm:LineGroupId>0</csm:LineGroupId>
                    <csm:Feature>26</csm:Feature>
                    <csm:Locale />
                    <csm:ForceAccountCode>false</csm:ForceAccountCode>
                    <csm:ForceAuthCode>false</csm:ForceAuthCode>
                  </csm:ShortCode>
                </csm:ShortCodes>
                <csm:DialInOn>false</csm:DialInOn>
                <csm:DialInTimeProfile />
                <csm:DialInFirewallProfile />
                <csm:SourceNumbers>V207|</csm:SourceNumbers>
                <csm:DialInQuotaTime>0</csm:DialInQuotaTime>
                <csm:LoginCode />
                <csm:LoginIdleTime />
                <csm:WrapUpTime>2</csm:WrapUpTime>
                <csm:TwinMaster />
                <csm:SecTwinCallEnabled>false</csm:SecTwinCallEnabled>
                <csm:CanIntrude>false</csm:CanIntrude>
                <csm:CannotBeIntruded>true</csm:CannotBeIntruded>
                <csm:XDirectory>false</csm:XDirectory>
                <csm:ForceLogin>false</csm:ForceLogin>
                <csm:ForceAuthCode>false</csm:ForceAuthCode>
                <csm:ForceAccountCode>false</csm:ForceAccountCode>
                <csm:SystemPhone>0</csm:SystemPhone>
                <csm:AbsentMsg>0</csm:AbsentMsg>
                <csm:AbsentSet>0</csm:AbsentSet>
                <csm:AbsentText />
                <csm:T3HuntGroupMembershipStatus />
                <csm:T3HuntGroupServiceStatus />
                <csm:T3HuntGroupNightServiceStatus />
                <csm:T3DirectoryEntries />
                <csm:MonitorGroup />
                <csm:DisplayLocale>   </csm:DisplayLocale>
                <csm:Locale />
                <csm:PMType>0</csm:PMType>
                <csm:InboundAutoRecord>0</csm:InboundAutoRecord>
                <csm:OutboundAutoRecord>0</csm:OutboundAutoRecord>
                <csm:AutoRecordTimeProfile />
                <csm:RemoteWorker>false</csm:RemoteWorker>
                <csm:CanAcceptCollectCalls>false</csm:CanAcceptCollectCalls>
                <csm:UserRights />
                <csm:Secretaries />
                <csm:TransferReturnTime />
                <csm:AnswerCallWaiting>true</csm:AnswerCallWaiting>
                <csm:RingingLinePreference>true</csm:RingingLinePreference>
                <csm:IdleLinePreference>true</csm:IdleLinePreference>
                <csm:CoverageTime>10</csm:CoverageTime>
                <csm:AutoVRL>0</csm:AutoVRL>
                <csm:ManualVRL>0</csm:ManualVRL>
                <csm:DelayedRingPreference>false</csm:DelayedRingPreference>
                <csm:AnswerPreSelect>false</csm:AnswerPreSelect>
                <csm:ReserveLastCA>false</csm:ReserveLastCA>
                <csm:CallTracingOn>false</csm:CallTracingOn>
                <csm:DisplayCharges>true</csm:DisplayCharges>
                <csm:MarkUpFactor>100</csm:MarkUpFactor>
                <csm:reset_longest_idle_info>0</csm:reset_longest_idle_info>
                <csm:NoAnswerStatus>0</csm:NoAnswerStatus>
                <csm:PBXAddress />
                <csm:SIPName>207</csm:SIPName>
                <csm:SIPDisplayName>test21</csm:SIPDisplayName>
                <csm:SIPContact>207</csm:SIPContact>
                <csm:SIPAnonymous>false</csm:SIPAnonymous>
                <csm:AbbreviatedRing>true</csm:AbbreviatedRing>
                <csm:CustomerServiceRep>false</csm:CustomerServiceRep>
                <csm:ACWTime>-1</csm:ACWTime>
                <csm:AutoACW>false</csm:AutoACW>
                <csm:UMSWebServices>false</csm:UMSWebServices>
                <csm:DisableVMOnFU>false</csm:DisableVMOnFU>
                <csm:DTMFCallCtrl>false</csm:DTMFCallCtrl>
                <csm:LoggedOutTwinning>0</csm:LoggedOutTwinning>
                <csm:OneXClient>false</csm:OneXClient>
                <csm:MobilityFeatures>false</csm:MobilityFeatures>
                <csm:TwinnedBridgeAppearances>false</csm:TwinnedBridgeAppearances>
                <csm:TwinnedCoverageAppearances>false</csm:TwinnedCoverageAppearances>
                <csm:TwinnedLineAppearances>false</csm:TwinnedLineAppearances>
                <csm:PersonalDirectory />
                <csm:ForwardToVoicemail>false</csm:ForwardToVoicemail>
                <csm:CoverageGroup />
                <csm:CanChangeHGOOSGroup />
                <csm:CanChangeHGONGroup />
                <csm:IncludeForwardInMenu>true</csm:IncludeForwardInMenu>
                <csm:CallLoggingCentralised>0</csm:CallLoggingCentralised>
                <csm:AttentionRing>true</csm:AttentionRing>
                <csm:CoverageRing>0</csm:CoverageRing>
                <csm:LogMissedCallsForHG />
                <csm:DisableForwardToVoicemail>0</csm:DisableForwardToVoicemail>
                <csm:AnnouncementsOn>false</csm:AnnouncementsOn>
                <csm:FollowAnnouncementsOn>true</csm:FollowAnnouncementsOn>
                <csm:LoopAnnouncementsOn>true</csm:LoopAnnouncementsOn>
                <csm:SyncAnnouncementsOn>false</csm:SyncAnnouncementsOn>
                <csm:FirstAnnTime>10</csm:FirstAnnTime>
                <csm:SecondAnnTime>20</csm:SecondAnnTime>
                <csm:BetweenAnnTime>20</csm:BetweenAnnTime>
                <csm:PostAnnTone>2</csm:PostAnnTone>
                <csm:PortalServices>0</csm:PortalServices>
                <csm:WorkingHoursUserRightsGroup />
                <csm:T3SelfAdmin>false</csm:T3SelfAdmin>
                <csm:MobileCallback>false</csm:MobileCallback>
                <csm:Receptionist>true</csm:Receptionist>
                <csm:SoftPhone>false</csm:SoftPhone>
                <csm:OneXTelecommuter>false</csm:OneXTelecommuter>
                <csm:AssignedPackage>1</csm:AssignedPackage>
                <csm:AutoRecMode>2</csm:AutoRecMode>
                <csm:CallLogTimeout>00:00</csm:CallLogTimeout>
                <csm:UserCLI />
                <csm:FlareEnabled>false</csm:FlareEnabled>
                <csm:FlareMode>0</csm:FlareMode>
                <csm:AutoIntDeny>false</csm:AutoIntDeny>
                <csm:TUIUser>
                  <csm:TUIFeaturesMenuControls>false</csm:TUIFeaturesMenuControls>
                  <csm:TUIFeaturesMenu>true</csm:TUIFeaturesMenu>
                  <csm:TUIBasicCallFunctions>true</csm:TUIBasicCallFunctions>
                  <csm:TUIAdvancedCallFunctions>true</csm:TUIAdvancedCallFunctions>
                  <csm:TUIHotDeskFunctions>true</csm:TUIHotDeskFunctions>
                  <csm:TUIPasscodeChange>true</csm:TUIPasscodeChange>
                  <csm:TUIPhoneLock>true</csm:TUIPhoneLock>
                  <csm:TUISelfAdmin>true</csm:TUISelfAdmin>
                  <csm:TUIVoiceMailControls>true</csm:TUIVoiceMailControls>
                  <csm:TUIForwarding>true</csm:TUIForwarding>
                </csm:TUIUser>
                <csm:UserPasswordStatus>1</csm:UserPasswordStatus>
                <csm:BlockForwarding>false</csm:BlockForwarding>
                <csm:ParkAndPageInfo>
                  <csm:ParkAndPage>
                    <csm:ParkAndPageId>1</csm:ParkAndPageId>
                    <csm:PagingNumber />
                    <csm:CentrexTransferNumber />
                    <csm:PNPFallBackNumber />
                    <csm:RetryTimeout>15</csm:RetryTimeout>
                    <csm:RetryCount>0</csm:RetryCount>
                  </csm:ParkAndPage>
                  <csm:ParkAndPage>
                    <csm:ParkAndPageId>2</csm:ParkAndPageId>
                    <csm:PagingNumber />
                    <csm:CentrexTransferNumber />
                    <csm:PNPFallBackNumber />
                    <csm:RetryTimeout>15</csm:RetryTimeout>
                    <csm:RetryCount>0</csm:RetryCount>
                  </csm:ParkAndPage>
                  <csm:ParkAndPage>
                    <csm:ParkAndPageId>3</csm:ParkAndPageId>
                    <csm:PagingNumber />
                    <csm:CentrexTransferNumber />
                    <csm:PNPFallBackNumber />
                    <csm:RetryTimeout>15</csm:RetryTimeout>
                    <csm:RetryCount>0</csm:RetryCount>
                  </csm:ParkAndPage>
                </csm:ParkAndPageInfo>
                <csm:MobileVoIPClientEnabled>false</csm:MobileVoIPClientEnabled>
                <csm:SendMobilityEmail>false</csm:SendMobilityEmail>
                <csm:IPOCCAgent>false</csm:IPOCCAgent>
                <csm:AgentType>0</csm:AgentType>
                <csm:WebCollaboration>false</csm:WebCollaboration>
                <csm:ConferencePIN />
              </csm:User>
            </csm:ws_object>
          </csm:data>
        </commProfile>
      </commProfileList>
    </commProfileSet>
  </tns:user>
</tns:users>
```

XML Schema for bulk import and export of Presence Profile

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:complexType name="XmlPsCommProfile">
<xsd:complexContent>
<xsd:extension base="one:xmlCommProfileType" >
<xsd:sequence>
<xsd:element name="primarySipEntityId" type="xsd:long"/>
<xsd:element name="secondarySipEntityId" type="xsd:long" minOccurs="0"/>
</xsd:sequence>
</xsd:extension>
</xsd:complexContent>
</xsd:complexType>
```

Sample XML for Presence Communication Profile

```
<?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>pm_0displayName</displayName>
<displayNameAscii>pm_0displayNameAscii</displayNameAscii>
<dn>dn</dn>
<isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
<isEnabled>true</isEnabled>
<isVirtualUser>false</isVirtualUser>
<givenName>pm_0givenName</givenName>
<honorific>honorific</honorific>
<loginName>pm_0@pres.avaya.com</loginName>
<middleName>pm_0middleName</middleName>
<managerName>pm_0managerName</managerName>
<preferredGivenName>pm_0preferredGivenName</preferredGivenName>
<preferredLanguage>en-US</preferredLanguage>
<source>local</source>
<sourceUserKey>sourceUserKey</sourceUserKey>
<status>AUTHPENDING</status>
<suffix>suffix</suffix>
<surname>pm_0surname</surname>
<title>pm_0title</title>
<userName>pm_0userName</userName>
<userPassword>-6396392681329505585</userPassword>
<commPassword>-6396392681329505585</commPassword>
<userType>AGENT</userType>
<address>
<addressType>OFFICE</addressType>
<name>pm_0contact_address</name>
<building>pm_0building</building>
<localityName>pm_0localityName</localityName>
<postalCode>pm_0postalCode</postalCode>
<room>pm_0room</room>
<stateOrProvince>pm_0stateOrProvince</stateOrProvince>
<country>pm_0country</country>
<street>pm_0street</street>
<postalAddress>pm_0postalAddress</postalAddress>
<isPrivate>true</isPrivate>
</address>
<securityIdentity>
<identity>pm_0identity1</identity>
<realm>pm_0realm1</realm>
<type>pm_0type1</type>
</securityIdentity>
<ownedContactLists>
<contactList>
<name>pm_0ContactList_1</name>
<description>pm_0Decription_ContactList_default_1</description>
<isPublic>false</isPublic>
<members>
<memberContact>pm_0_0Contact_1</memberContact>
<speedDialContactAddress>
<address>12345</address>
<altLabel>pm_0altLabel1</altLabel>
<contactCategory>OFFICE</contactCategory>
<contactType>PHONE</contactType>
<label>pm_0labe2</label>
</speedDialContactAddress>
<isFavorite>true</isFavorite>
```

```
<isSpeedDial>true</isSpeedDial>
<speedDialEntry>22222</speedDialEntry>
<isPresenceBuddy>true</isPresenceBuddy>
<label>pm_0labe3</label>
<altLabel>pm_0altLabe4</altLabel>
<description>pm_0description1</description>
<priorityLevel>1</priorityLevel>
</members>
<contactListType>CONTACTCENTER</contactListType>
</contactList>
</ownedContactLists>
<ownedContacts>
<contact>
<company>pm_0company1</company>
<description>pm_0description1</description>
<displayName>pm_0_0Contact_1</displayName>
<displayNameAscii>pm_0displayNameAscii1</displayNameAscii>
<dn>pm_0dn1</dn>
<givenName>pm_0givenName1</givenName>
<initials>initials1</initials>
<middleName>pm_0middleName1</middleName>
<preferredGivenName>pm_0preferredGivenName1</preferredGivenName>
<preferredLanguage>English</preferredLanguage>
<isPublic>false</isPublic>
<source>local</source>
<sourceUserKey>pm_0sourceUserKey1</sourceUserKey>
<suffix>pm_0suffix1</suffix>
<surname>pm_0surname1</surname>
<title>pm_0title1</title>
<ContactAddress>
<address>12345</address>
<altLabel>pm_0altLabel1</altLabel>
<contactCategory>OFFICE</contactCategory>
<contactType>PHONE</contactType>
<label>pm_0label1</label>
</ContactAddress>
<addresses>
<addressType>OFFICE</addressType>
<name>pm_0_Add_Name</name>
<building>pm_0_Building_Name</building>
<localityName>pm_0_locality</localityName>
<postalCode>411014</postalCode>
<room>pm_0_Room_5B</room>
<stateOrProvince>Maharashtr<A/stateOrProvince>
<country>Indi<A/country>
<street>pm_0_Street</street>
<postalAddress>pm_0_POAdd</postalAddress>
<isPrivate>true</isPrivate>
</addresses>
</contact>
</ownedContacts>
<presenceUserDefault>
<infoTypeAccess>
<infoType>
<label>All</label>
<filter>ALL</filter>
<specFlags>FULL</specFlags>
</infoType>
<access>BLOCK</access>
</infoTypeAccess>
</presenceUserDefault>
<presenceUserACL>
<infoTypeAccess>
<infoType>
<label>All</label>
```

```
<filter>ALL</filter>
<specFlags>FULL</specFlags>
</infoType>
<access>BLOCK</access>
</infoTypeAccess>
<watcherDisplayName>pm_0_0Contact_1</watcherDisplayName>
</presenceUserACL>
<presenceUserCLDefault>
<infoTypeAccess>
<infoType>
<label>Telephony</label>
<filter>CLASS(phone)</filter>
<specFlags></specFlags>
</infoType>
<access>ALLOW</access>
</infoTypeAccess>
</presenceUserCLDefault>
<commProfileSet>
<commProfileSetName>commProfileSetNamepm_0</commProfileSetName>
<isPrimary>true</isPrimary>
<handleList>
<handle>
<handleName>smtp_pm_0@ahmadexserver.com</handleName>
<handleType>smtp</handleType>
<handleSubType>msexchange</handleSubType>
<domainName>__foreign__</domainName>
</handle>
</handleList>
<commProfileList>
<commProfile xsi:type="ext:XmlPsCommProfile"
xmlns:ext="http://xml.avaya.com/schema/presence">
<commProfileType>PS</commProfileType>
<ext:primarySipEntityId>32768</ext:primarySipEntityId>
</commProfile>
</commProfileList>
</commProfileSet>
</tns:user>
</tns:users>
```

XML Schema for Conferencing Communication Profile

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
      xmlns:one="http://xml.avaya.com/schema/import"
      targetNamespace="http://xml.avaya.com/schema/import_mmcs"
      elementFormDefault="qualified"
      xmlns:abc="http://xml.avaya.com/schema/import_mmcs">

<!--
    This is the XML schema for the Avaya Aura Conferencing Profile. It
     defines this profile inside of an XML document that defines a user record
  (see userimport.xsd)
-->

<xsd:import namespace="http://xml.avaya.com/schema/import"
                       schemaLocation="userimport.xsd"/>
   <xsd:complexType name="MmcsCommProfileType">
      <xsd:complexContent>
         <xsd:extension base="one:xmlCommProfileType" >
            <xsd:sequence>
               <xsd:element name="template" type="xsd:string"/>
               <xsd:element name="securityCode" type="xsd:string"/>
               <xsd:element name="moderatorPin" type="xsd:string"/>
               <xsd:element name="eventConfCode" type="xsd:string"/>
               <xsd:element name="location" type="xsd:string" minOccurs="0"/>
               <xsd:element name="autoGeneratedCodeLength" minOccurs="0">
                 <xsd:simpleType>
                   <xsd:restriction base="xsd:int">
                     <xsd:minInclusive value="6"/>
                     <xsd:maxInclusive value="8"/>
                   </xsd:restriction>
                 </xsd:simpleType>
               </xsd:element>
            </xsd:sequence>
         </xsd:extension>
      </xsd:complexContent>
   </xsd:complexType>
</xsd:schema>
```

Sample XML for bulk import of Conferencing Profile

```
<?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)

<!-- 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” or E.164) -->
                <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>

                  <commProfile xsi:type="ns2:MmcsCommProfileType" xmlns:ns2="http://
xml.avaya.com/schema/import_mmcs">
                  <commProfileType>mmcsCommProfile</commProfileType>
                  <ns2:template>event_1000</ns2:template>
                  <ns2:securityCode></ns2:securityCode>
                  <ns2:moderatorPin></ns2:moderatorPin>
                  <ns2:eventConfCode>777</ns2:eventConfCode>
                  <ns2:location>Location1</ns2:location>
                  <ns2:autoGeneratedCodeLength>6</ns2:autoGeneratedCodeLength>
               </commProfile>
           </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema Definition for bulk import of 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.
                    ---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. 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 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 inlcude 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 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 import of 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 inlcude 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 deletion of 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 deletion of 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 import of 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 Resource
                                        Attributes. 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">
                                ResourceType: String Value for 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 import of roles

```
&lt;?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 Import user XSD

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
authenticationType	The type of authentication the user undergoes at runtime to gain access to the system.	Mandatory	Possible values: • BASIC • ENTERPRISE
description	A description of the user. A human readable description of this user instance.	Optional	
displayName	The localized name of the user to be used when displaying. Typically, the value is the localized full name. This value might be provisioned from the enterprise directory entry of the user. If the value does not exist, you can use synchronization rules to populate the value for other fields. For example: Surname, GivenName, or LoginName.	Optional	
displayNameAscii	The name that corresponds to the console attribute Endpoint Display Name. The full text name of the user represented in ASCII. The attribute used for displaying (e.g. endpoints) the unsupported localized text.	Optional	
dn	The distinguished name (DN) of the user. DN is a sequence of relative distinguished names (RDN) connected by commas. RDN is an attribute with an associated value in the form of attribute=value, typically expressed in a UTF-8 string format. Use DN for identifying the user and for authentication subject mapping. You can change DN.	Optional	
isDuplicatedLoginAllowed	A boolean that indicates whether this user is allowed a duplicate concurrent logins. true indicates that the user can have duplicate logins.	Optional	Default value is true.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
isEnabled	A boolean that indicates whether or not the user is active. Users with AuthenticationType=Basic fails if the value is false. This attribute can be used to disable access between login attempts. You cannot revoke login for a running session. 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.	Optional	Default value is false.
isVirtualUser	A boolean that indicates whether or not the record is being used for a non-human entity such as an application, service, and software agent. You require this attribute where the entity behaves 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, for example, a trust certificate must not be treated as a virtual user. A virtual user can represent an Avaya or an 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.	Optional	Default value is false.
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	The unique login name that you provide for the user. The format for the login name is username@domain. The login	Mandatory	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	name is an alphanumeric value and supports the ASCII characters "_", ".", and "-".		
middleName	The middle name of the user.	Optional	
managerName	The name of the manager of the user. This is a free formed field and does not require the user's manager to be a user of the solution. The attribute supports the reporting needs.	Optional	
preferredGivenName	The preferred first name of the user.	Optional	
preferredLanguage	The preferred written or spoken language. The format uses the ISO standard Language (ISO-639) and region (ISO-3166) codes If a preferred language is not available, the locale of the client must be used. If the value is blank, en_US must be used as default.	Optional	Possible values: • English (United States) - en_US • Chinese (Simplified) - zh_CN • Japanese (Japan) - ja_JP • Korean (Korea) - ko_KR • French (France) - fr_FR • German (Germany) - de_DE • Italian (Italy) - it_IT • Russian (Russia) - ru_RU • English (United Kingdom) - en_GB • Spanish (Mexico) - es_MX • Portugese (Brazil) - pt_BR • French (Canada) - fr_CA • English (Canada) - en_CA
source	A free format text field that identifies the entity that created	Optional	User Management populates the source

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	this user record. The format of this field must be a IP Address/ Port or a name representing an enterprise LDAP or Avaya.		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, the key is objectGUID.	Optional	By default, the value is none.
status	The information that helps provisioning activities such as correcting or completing the provisioning of a user. 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: AUTHPENDING; PENDINGAUTHZ; PROVISIONED
suffix	The text appended to a name. For example, Jr., III.	Optional	
surname	The last name or the family name of the user.	Mandatory	
timeZone	The preferred time zone of the user. For example: America/ New_York, Europe/Dublin. The application consuming this information must know how to translate e.g. in Java it is TimeZone.getTimeZone("Europe/Moscow"); In the absence of a value, the system uses the local services timezone. **Note:** You must consider daylight saving time (DST) and summer time adjustments while using the suggested values for **timeZone**. Typically, you add 1 hour to the offset. **Note:** You cannot use the following characters as is in the xml. Make the following modifications	Optional	(-12:0)International Date Line West (-11:0)Midway Island, Samoa (-10:0)Hawaii (-9:0)Alaska (-8:0)Pacific Time (US & Canada); Tijuana (-7:0)Mountain Time (US & Canada); Chihuahua, La Paz (-7:0)Arizona (-6:0)Central Time (US & Canada); Guadalajara, Mexico City (-6:0)Central America; Saskatchewan (-5:0)Indiana (East); Bogota, Lima, Quito

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	while using them in the import xml files: • less-than character (<) as < &lt; • ampersand character (&) as &amp; • greater-than character (>) as &gt; • double-quote character (") as &quot; • apostrophe or single-quote character (') as &apos;		(-5:0)Eastern Time (US & Canada) (-4:0)Caracas, La Paz (-4:0)Atlantic Time (Canada); Santiago, Manaus (-3:30)Newfoundland (-3:0)Georgetown (-3:0)Brasilia, Greenland, Buenos Aires, Montevideo (-2:0)Mid-Atlantic (-1:0)Azores (-1:0)Cape Verde Is. (0:0)Monrovia, Reykjavik (0:0)GMT : Dublin, Edinburgh, Lisbon, London, Casablanca (+1:0)West Central Africa (+1:0)Amsterdam, Berlin, Rome, Belgrade, Prague, Brussels, Sarajevo (+2:0)Harare, Pretoria (+2:0)Amman, Athens, Minsk, Beirut, Cairo, Jerusalem, Helsinki, Windhoek (+3:0)Baghdad, Kuwait, Riyadh, Nairobi, Tbilisi (+3:0)Moscow, St. Petersburg, Volgograd (+3:30)Tehran (+4:0)Abu Dhabi, Muscat, Caucasus Standard Time

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			(+4:0)Baku, Tbilisi, Yerevan (+4:30)Kabul (+5:0)Islamabad, Karachi, Tashkent, Ekaterinburg (+5:30)Chennai, Kolkata, Mumbai, New Delhi, Sri Jayawardenepura (+5:45)Kathmandu (+6:0)Astana, Dhaka, Almaty, Novosibirsk (+6:30)Rangoon (+7:0)Bangkok, Hanoi, Jakarta, Krasnoyarsk (+8:0)Beijing, Hong Kong, Singapore; Taipei (+8:0)Perth; Irkutsk, Ulaan Bataar (+9:0)Seoul, Osaka, Sapporo, Tokyo (+9:0)Yakutsk (+9:30)Darwin, Adelaide (+10:0)Brisbane, Guam, Port Moresby (+10:0)Canberra, Melbourne, Sydney, Hobart, Vladivostok (+11:0)Magadan, Solomon Is., New Caledonia (+12:0)Auckland, Wellington (+12:0)Fiji, Kamchatka, Marshall Is. (+13:0)Nuku'alofa
title	The job function of a person in their organizational context.	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
userName	The username portion of the loginName field. 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 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 and non SIP. This attribute is shared across different communication profiles and thus different communication services.	Optional	
userType	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	The text name of a role. This value must be available in the System Manager database.	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 loginName, Kerberos account name, or X509 certificate name.	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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	The system creates a default contactlist per user.
ownedContacts	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.	Optional	
presenceUserDefault	The 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 can be one User Default rule per presentity (User), or none.	Optional	
presenceUserACL	The personal rules defined by presentities themselves on who can monitor their presence information. There might be several entries in the list for a given presentity, each entry corresponding to one watcher.	Optional	
presenceUserCLDefault	The personal rule that is set by presentities to define how much presence information can be shown to watchers that belong to the contact list of the user. There can be one User Contact List Default rule per presentity (Person) or none.	Optional	
commProfileSet	The default Commprofile set of the user. A commprofile set can exist without any handles or commprofiles referencing it. That is, you can create a commprofile set without creating 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	Optional	A user has a default commprofile set.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	CommProfile uniqueness constraint include type, commprofile_set_id.		
employeeNo	The employee number of the user.	Optional	
department	The department which the employee belongs to.	Optional	
organization	The organization which the employee belongs to.	Optional	
localizedNames	The localized name of the user.	Optional	

Attribute details defined in Delete User XSD

Attribute	Attribute description	Mandatory/Optional	Validation constraints
deleteType	Defines the delete type of the user. If the user selects: • soft: The system does not delete the user record permanently. You can recover the user record. • permanent: The system permanently deletes all attributes associated with the user and the links to public contacts and shared addresses.	Mandatory	Possible values: • soft • permanent
loginName	A unique system login name assigned to the user in the format username@domain or username.	Mandatory	
id	A unique identifier for a user record. The id attribute is included in the XSD for future enhancement. This is not used in System Manager the current release.	Optional	

Attribute details defined in the CM Endpoint profile XSD

Attribute details defined in the CM Endpoint profile XSD

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
CM Name cmName	The name of the Communication Managersystem as it appears in the Applications/Application Management/Entities.	Mandatory	
Use Existing Extension useExistingExtension	Select **true** if you want to use an already created extension. Select **false** if you want to use an available extension.	Optional	
Template Name template	The template name that is used to create the endpoint. Values defined in the template will be used if you do not provide other values.	Optional	
Set Type setType	The set type of the endpoint.	Optional	
Port port	The valid port value.	Optional	01 to 64 First and second numbers are the cabinet numbers having values A to E. The third character is the carrier having values between 01 to 20. Fourth and fifth characters are the slot number between 01 to 32. Sixth and seventh characters are the circuit number having values 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 has a non-IP set, or that the extension had a non-IP set, and is

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) endpoints, 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 has an IP set. This is autopopulated for certain IP endpoint set types. You can enter the value for a DCP set with softphone permissions. This changes to the s00000 type when the set registers.
Delete endpoint is unassigned deleteOnUnassign	Specifies whether the endpoint must be deleted if it is unassigned from the user.	Optional	
Lock messages feature. lockMessages	Select to enable the lock messages feature.	Optional	Select true or false to enable or disable the lock messages feature respectvely.
Coverage Path 1 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 1-9999, time of day table between 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 1-9999, time of day table between t1-t999, or blank.
Hunt To Station huntToStation	The extension the system must hunt to for this telephone when the telephone is busy. A endpoint hunting chain can be created by assigning a hunt-to	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	endpoint to a series of telephones.		
Tenant Number tn	Provides partitioning of attendant groups and endpoints and trunk groups. Typically this is used for multiple tenants in a building or multiple departments within a company or an organization.	Mandatory	Valid values: 1 to 250
Class of Restriction cor	This is used for multiple tenants in a building or multiple departments within a company or an organization.	Mandatory	Valid values: 0 to 995
Class of Service cos	Class of Service lets you define a group of users and control the groups' access to features.	Mandatory	Valid values: 0 to 15
speakerphone	Controls the behavior of speakerphones.	Optional	Valid values : none, 1-way, 2-way
Display Language displayLanguage	The language that displays on the endpoint.	Optional	Time of day is displayed in the 24- hour format (00:00 - 23:59) for all languages except English, which is displayed in the 12-hour format (12:00 a.m. to 11:59 p.m.). unicode: Displays English messages in a 24-hour format . If you do not install the Unicode file, the endpoint displays messages in English by default.
Personalized Ringing Pattern personalizedRingingPattern	The personalized ringing pattern for the endpoint. Personalized Ringing allows the users of some telephones to have one of the eight ringing		L = 530 Hz, M = 750 Hz, and H = 1060 Hz Valid Entries Usage: 1. MMM (standard ringing) 2. HHH

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	patterns for incoming calls. For virtual endpoints, this field dictates the ringing pattern on its mapped to physical telephone.		3. LLL 4. LHH 5. HHL 6. HLL 7. HLH 8. LHL
Message Lamp Extension messageLampExt	The Message Lamp Extension associated with the current extension.	Mandatory	
muteButtonEnabled	Select to enable the mute button on the endpoint.		
Media Complex Extension mediaComplexExt	When used with Multi-media Call Handling, this field indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to either place a voice or a data call. Voice conversion, coverage, and forwarding apply as if the call were made to the 1-number.	Optional	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 endpoint extension: For the 4600 series IP Telephones, enter the corresponding H.323 endpoint. For IP Softphone, enter the corresponding H.323 endpoint. If you enter a value in this field, you can register this endpoint on either a road-warrior or elecommuter/Avaya IP Agent application. Blank: Leave this field blank for single-connect IP applications.
IP Softphone ipSoftphone	Specifies whether the endpoint is an IP soft phone.	Optional	
Servivable GK Node Name survivableGkNodeName	Survivable GK Node Name identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call	Optional	Valid Entry Usage: Valid IP node name, any valid, previously-administered IP node name.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the H.248 gateways. When you enter a valid IP node name in 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 endpoints register with Communication Manager, this list is sent to the registration confirm message. The IP endpoint can use the IP address of this Survivable Gatekeeper as the call controller of last resort to register with. Survivable GK Node Name is available only if the endpoint is an H.323 endpoint (46xxor 96xx set types).		
Survivable class of restriction survivableCOR	Sets the level of restriction for endpoints to be used with the survivable dial plan to limit certain users to certain types of calls. You can list the restriction levels from the most restrictive to least restrictive. Each level assumes the calling ability of the ones above it. This field is used by the PIM module in Integrated Management to communicate with the Communication Manager	Optional	Valid Entries: Usage emergency - This endpoint can only be used to place emergency calls. Internal - This endpoint can only make intra-switch calls. This is the default value. local - This endpoint can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	administration tables and to obtain the class of service information. PIM module builds a managed database to send to Standard Local Survivability (SLS) on the H.248 gateways. Survivable COR is valid for all analog and IP endpoint types.		toll - This endpoint can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables. unrestricted - This endpoint 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 survivableTrunkDest	This field does not allow certain telephones to receive incoming trunk calls when the media gateway is in survivable mode. This field is used by the PIM module in 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. Survivable Trunk Destination is available for all analog and IP endpoint types.	Optional	Valid Entry Usage: true - Allows this endpoint to be an incoming trunk destination while the media gateway is running in the survivability mode. This is the default value. false - Prevents this endpoint from receiving incoming trunk calls when the endpoint in survivable mode.
Voice Mail Number voiceMailNumber	Enter the complete Voice Mail Dial Up number.	Optional	String
offPremisesStation	Analog telephones only.	Optional	Valid entries Usage: • true - Enter true if this telephone is not located in the same building as the system. If you enter true, you

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			must complete the R Balance Network. - false - Enter false if the telephone is located in the same building as the system.
dataOption	If a second line on the telephone is administered on the I-2 channel, enter `analog`. Else, enter the data module if applicable, or enter `none`.	Optional	Valid entries: analog, none.
Message Waiting Indicator messageWaitingIndicator	If you select led or neon, then you must enable messageLampExt, else leave this field blank.	Optional	Valid entries: led, neon, none.
remoteOfficePhone	Select **true** to use this endpoint as an endpoint in a remote office configuration.	Optional	Valid entries: - 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.
lwcActivation	Select true to allow internal telephone users to leave short LWC messages for this extension. If the system has hospitality, select true for guest-room telephones for the designated extensions to receive failed wakeup messages, and to receive LWC messages that indicate the wakeup	Optional	Boolean

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	calls failed. Select true if LWC Reception is audix.		
activeStationRinging	Active endpoint ringing	Optional	Valid entries: • single • continuous • if-busy-single • silent
idleActiveRinging	Defines how a call rings to the telephone when it is on-hook.	Optional	Valid entries • continuous - Select continuous to cause all calls to this telephone to ring continuously. • if-busy-single - Select 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. • silent-if-busy - Select silent-if-busy to cause calls to ring silently when this endpoint is busy. • single - Select single to cause calls to this telephone to receive one ring cycle and then ring silently.
switchhookFlash	Set this field to true when the **Type** field is set to H. 323.	Optional	Boolean
ignoreRotaryDigits	If you set this field to true, the short switch-hook flash (50 to 150) from a 2500-type set is ignored.	Optional	Boolean

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
h320Conversion	H.320 Conversion — Valid entries are true and false (default). This field is optional for non-multimedia complex voice endpoints and for basic multimedia complex voice endpoints. H.320 Conversion is mandatory for enhanced multimedia complex voice endpoints. Since the system can only handle a limited number of conversion calls, you must limit the number of telephones with H.320 conversion. Enhanced multimedia complexes must have this flag set to true.	Optional	Boolean
serviceLinkMode	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 ends 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 resource. Service Link Mode can	Optional	Valid entries: as-needed permenant

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	be administered as either as-needed or permanent: • 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 endpoint and for a period of 10 seconds after the last multimedia call on the endpoint 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 reestablish. • 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 endpoint's first multimedia call and will remain in a connected state until the user		

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	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 endpoint or a multimedia call that has been early answered.		
multimediaMode	There are two multimedia modes, Basic and Enhanced.	Optional	Basic - A basic multimedia complex consists of a BRIconnected multimedia-equipped PC and a non-BRI-connected multifunction telephone set. Enhanced - An enhanced multimedia complex consists of a BRI-connected multimediaequipped PC and a non-BRIconnected multifunction telephone.
mwiServedUserType	Controls the auditing or interrogation of a served user's message waiting indicator (MWI).	Optional	Valid entries: 1. fp-mwi - Select this option if the endpoint is a served user of an fp-mwi message center. 2. qsig-mwi - Select this option if the endpoint is a served user of a qsig-mwi message center. 3. sip adjuncts - Select this option if the endpoint is a served user of a sip adjunct message center.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			4. blank - Leave this field 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.
audixName	The AUDIX associated with the endpoint. 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	Valid entries: 1. always - Select always to move the DCP telephone anytime without additional administration by unplugging the telephone from one location and plugging it into a new location. 2. once - Select once to unplug and plug the DCP telephone 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. Use once when you want to move a large number of DCP telephones so that each extension is removed from the move list. Use once to prevent automatic maintenance replacement.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			3. no - Enter no to require administration in order to move the DCP telephone. 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. 5. Error - Error is a display-only value. 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.
remoteSoftphoneEmergencyCalls	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.	Optional	Valid entries: 1. As-on-local: As-on-local sends the extension entered in the Emergency Location Extension field on the Endpoint screen to the Public Safety Answering Point (PSAP) 2. Block - Block prevents the completion of emergency calls. 3. Cesid - Cesid allows Communication Manager to send the CESID information supplied by the IP

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			Softphone to the PSAP. 4. Option - Option allows the user to select the option (extension, block, or cesid) that the user selected during registration.
emergencyLocationExt	This field allows the system to properly identify the location of a caller who dials a 911 emergency call from this endpoint. 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. The entry can be a UDP extension. The default entry is blank. A blank entry typically is 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 Endpoint 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 Endpoint screen is	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	different from the Emergency Location 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 in 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 endpoint extension is displayed, overriding the administered LoginID for ISDN Display. This 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 endpoint.	Optional	
autoSelectAnyIdleAppearance	Enables or disables automatic selection of any idle appearance of transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being	Optional	Boolean

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	transferred or conferenced has. If that attempt fails, Optional Boolean Communication Manager selects the first idle appearance coverageMsgRetrieval.		
coverageMsgRetrieval	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.	Optional	Boolean
autoAnswer	In EAS environments, the auto answer setting for the Agent LoginID can override a endpoint's setting when an agent logs in.	Optional	Valid entries: 1. all: All ACD and non-ACD calls ended to an idle endpoint 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. 2. acd: Only ACD split / skill calls and direct agent calls to auto answer. Non-ACD calls ended to an endpoint ring audibly. For analog endpoints, the endpoint is off-hook and idle, only the ACD split/skill calls

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			and direct agent calls auto answer; non-ACD calls receive busy treatment. If the endpoint is active on an ACD call and a non-ACD call arrives, the Agent receives call-waiting tone. 3. none: All calls ended to this endpoint receive an audible ringing treatment. 4. icom: Allows a telephone user 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. Data restriction cannot be assigned if Auto Answer is administered as all or acd. If enabled, whisper page to this endpoint 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. false - The Alerting Appearance Preference is set and the user connects to the ringing call appearance.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
callWaitingIndication	Enable or disable call waiting for this endpoint.	Optional	
attCallWaitingIndication	Attendant call waiting allows attendantoriginated or attendant-extended calls to a busy single-line telephone to wait and sends distinctive call-waiting tone to the single-line user. Select to enable or disable attendant call waiting	Optional	Boolean
distinctiveAudibleAlert	Select true so that the telephone can receive the three 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: 1. true: Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only. 2. false: Last idle call appearance is used for incoming priority calls and outgoing call originations.
adjunctSupervision	Enable or disable Adjunct Supervision.	Optional	Valid entries: 1. true: Analog disconnect signal is sent automatically to the port after a call ends. Analog devices such as answering machines and speakerphones use this signal to

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			turn the devices off after a call ends. 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 endpoint when a call is queued for the endpoint.
perStationCpnSendCallingNumber	Send Calling Number	Optional	Valid entries: 1. y: All outgoing calls from the endpoint will deliver the Calling Party Number (CPN) information as Presentation Allowed. 2. n: No CPN information is sent for the call. 3. r: Outgoing non-DCS network calls from the endpoint will deliver the Calling Party Number information as Presentation Restricted.
busyAutoCallbackWithoutFlash	Appears on the Endpoint 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	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	Busy Auto Callback without Flash field then defaults to true for all analog telephones that allow Analog Automatic Callback. Set this field to true to provide automatic callback for a calling analog endpoint without flashing the hook.		
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 originate from an endpoint with Client Room Class of Service. For endpoints with an audix endpoint type, AUDIX Voice Power ports, or ports for any other type of messaging that needs display information, Display Client Redirection must be enabled. Set this field to true to redirect information for a call originating from a Client Room and ending to this endpoint displays.	Optional	Boolean
selectLastUsedAppearance		Optional	Valid entries: 1. True: Indicates that an endpoint's line selection is not to be moved from the currently selected line button to a different, non-alerting line button. If you select true, the

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			line selection on an on-hook endpoint 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. 2. false: The line selection on an on-hook endpoint with no alerting calls can be moved to a different line button, which might be serving a different extension.
coverageAfterForwarding	Specifies whether an unanswered forwarded call is provided coverage treatment.	Optional	
directIpIpAudioConnections	Select to allow or deny 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	
endpointSiteData	This is applicable for Site Data fields		
room	This is a Site Data field.	Optional	Max length 10
jack	This is a Site Data field.	Optional	Max length 5
cable	This is a Site Data field.	Optional	Max length 5
floor	This is a Site Data field.	Optional	
building	This is a Site Data field.	Optional	
headset	This is a Site Data field.	Optional	
speaker	This is a Site Data field.	Optional	
mounting	This is a Site Data field.	Optional	Valid values d, w.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
cordLength	This is a Site Data field.	Optional	Valid range from 0 to 99.
setColor	This is a Site Data field.	Optional	
abbrList	This is applicable for Station Abbreviated Dialing Data fields.	Optional	
listType	This is a Station Abbreviated Dialing Data field.	Mandatory	Valid values enhanced, group, personal, system.
number	This is a Station Abbreviated Dialing Data field.	Mandatory	A number.
buttons	This is applicable for button data.	Optional	
Number	This is a button data field.	Mandatory	
Type	This is a button data field.	Optional	
data1	This is a button data field.	Optional	
data2	This is a button data field.	Optional	
data3	This is a button data field.	Optional	
data4	This is a button data field.	Optional	
data5	This is a button data field.	Optional	
data6	This is a button data field.	Optional	
endpointDataModule	This is a Station Data module field.	Optional	
dataExtension	This is a Station Data module field.	Mandatory	
name	This is a Station Data module field.	Optional	Max length 29
Class of restriction cor	This is a Station Data module field.	Mandatory	Valid range from 0 to 995.
Class of Service Cos	This is a Station Data module field.	Mandatory	Valid range from 0 to 15.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
itc	This is a Station Data module field.	Mandatory	Valid values: 1. restricted 2. unrestricted
Tenant Number	This is a Station Data module field.	Mandatory	Valid range from 1 to 100.
listType	This is a Station Data module field.	Optional	Valid values: 1. enhanced 2. group 3. personal 4. system
listId	This is a Station Data module field.	Optional	
specialDialingOption	This is a Station Data module field.	Optional	Valid values: 1. default 2. hot-line
specialDialingAbbrDialCode	This is a Station Data module field.	Optional	
hotLineDestAbbrevList	This is a Station Hot Line Data field.	Optional	Valid range 1 to 3
hotLineAbbrevDialCode	This is a Station Hot Line Data field.	Optional	Numeric string
nativeName	This is a Native Name Data field.	Optional	
locale	This is a Native Name Data field. **Note:** If the **displayName**, **givenName**, or **surname** contains characters of multiple scripts then the locale tag should be present. The locale for the multiscript languages are: • Japanese: **ja**	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	- Simplified Chinese: **zh-cn** - Traditional Chinese: **zh-tw** - Korean: **ko-kr** - Vietnamese: **vi-vn** The locale tag is case sensitive. You can use the preferredLanguage tag to specify the locale if displayName, nativeName, and Name are in multibytes. If the locale tag is present in the xml, locale tag is preferred over the preferredLanguage tag.		
Name	This is a Native Name Data field.	Mandatory	Max length 27
Enable Reachability for Domain Control SIP Stations	The system enables Reachability on SIP endpoint.	Optional	
			If you select **Calculate Route Pattern** check box, the system: - Populates the **Sip Trunk** field - Makes **Sip Trunk** field read-only.
		Optional	

Attribute details defined in the Messaging communication profile XSD

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
Messaging System Name messagingName	The name of Messaging System	Mandatory	
Use Existing Mailbox number useExisting	true if already created mailbox number is to be used. false if available	Optional	

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	mailbox number is to be used.		
Messaging Template messagingTemplate	Specifies the messaging template of a subscriber.	Optional	
Password password	Specifies the default password the subscriber must use to log in to his or her mailbox.	Mandatory	The password must be from 3 to 15 digits and adhere to system policies that you set on the Avaya Aura® Messaging server.
deleteOnUnassign		Optional	
Class of service 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 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 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 subscriber sends or receives an e-mail.	Optional	
Common Name 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	Optional	Valid values 0 to 9 number values of length 10

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	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.		
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	
telephoneNumber	This is field of Messaging specific data. 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. If the subscriber name is entered in multibyte character format, then this field specifies the ASCII translation of the subscriber name.	Optional	

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
expirePassword	This is field of Messaging specific data. Specifies whether your password expires or not.	Optional	You can choose one of the following: • yes: for password to expire • no: if you do not want your password to expire
mailBoxLocked	This is field of Messaging specific data. 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: • no: to unlock your mailbox • yes: to lock your mailbox and prevent access to it
personalOperatorMailbox	This is field of Messaging specific data. 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.	Optional	
personalOperatorSchedule	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.	Optional	
tuiMessageOrder	This is field of Messaging specific data. Specifies the order in which the subscriber hears the voice messages.	Optional	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.

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
			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.
intercomPaging	This is field of Messaging specific data. Specifies the intercom paging settings for a subscriber.	Optional	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.
voiceMailEnabled	This is field of Messaging specific data.	Optional	

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	Specifies whether a subscriber can receive messages, e-mail messages and callanswer 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.		
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. Specifies additional, useful information about		Max length 51

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	a subscriber. Entries in this field are for convenience and are not used by the messaging system.		
miscellaneous4	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
cmmSpecific	This is field of Messaging specific data. Specifies the number of the switch on which this subscriber's extension is administered.	Optional	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.
accountCode	This is field of CMM data. 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	Optional	

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	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 about a subscriber. Entries in this field are for convenience and are not used by the messaging system.	Optional	Max length 11
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	Mandator y/Optional	Validation Constraints
Primary Session Manager primarySM	The name of the Session Manager instance that must be used as the home server for a communication profile. As a home server, the primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura® network.	Mandatory	-
Secondary Session Manager secondarySM	If a secondary Session Manager instance is specified, this Session Manager provides continued service to SIP devices associated with this communication profile when the primary Session Manager is unavailable.	Optional	-
Survivability Server survivabilityServer	For local survivability, you can specify the name of a survivability server, a SIP entity, to provide survivability communication services for devices associated with a communication profile if the local connectivity to Session Manager instances in the Aura Core is lost. If you specify a Branch Session Manager, and the termination and origination application sequences contain a Communication Manager application, sequencing	Optional	-

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	to this application continues, locally, to the Communication Manager remote survivability server resident with the Branch Session Manager. **Note:** If a termination or origination application sequence contains a Communication Manager application, the Communication Manager associated with the application must be the main Communication Manager for the Communication Manager remote survivability server resident with Branch Session Manager.		
Max. Simultaneous Devices maxSimultaneousDevices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.		
Block New Registration When Maximum Registrations Active blockNewRegistrationWhenMaxActive	Set the value to true or false. If you do not set the attribute, by default, the system sets the attribute to false. If you set to true and if an endpoint tries to register using this communication profile when the maximum number of allowed simultaneous registrations reaches, the		

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	endpoint cannot register with Session Manager The endpoint does not have the SIP service. If the value is set to false, the default, the endpoint can register only after the system cancels the registration of the oldest endpoint. The stopped endpoint does not have the SIP service.		
Origination Application Sequence originationAppSequence	An Application Sequence that is invoked when calls are routed from this user. ✱ **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.	Optional	-
Termination Application Sequence terminationAppSequence	An Application Sequence that is invoked when calls are routed to this user. ✱ **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication	Optional	-

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	Manager must be the same in both the sequences.		
Home Location homeLocation	The home location that you set from **Routing** > **Locations** to support mobility for a user. When this user calls numbers that are not associated with an administered user, dial-plan rules that are set in**Routing** > **Dial Patterns** will be applied to complete the call based on this home location regardless of the physical location of the SIP device used to make the call.	Mandatory	-
Conference Factory Set confFactorySet	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.	Optional	-

Attribute details defined in the Avaya Aura® Conferencing profile XSD

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
User Template template	Specify the name of the User Template. User Templates are created in Avaya Aura Conferencing Provisioning Client. The following default templates always exist:	Mandatory	-

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	executive, desktop_user_with_video, desktop_user_no_video, desktop_user_low_priority, guest_user_no_video, event_1000, event_2000, event_3000.		
Location location	Specify location for the user. Location is a mandatory field. However, Conferencing can get the value of location from the **Location** field in Conferencing Profile. Conferencing can also get the value of location from the **Home Location** field in Session Manager Profile if Session Manager profile is configured and the location in Conferencing Profile is not configured.	Mandatory	-
Participant Security Code securityCode	The participant code for the chairperson bridge.	Mandatory if the autoGeneratedCodeLength parameter is not set.	-
Moderator Security Code moderatorPin	The unique participant code that you use to login to a conference as a moderator.	Mandatory if the autoGeneratedCodeLength parameter is not set.	-
Auto Generated Participant and Moderator Security Codes Length autoGeneratedCodeLength	This parameter shows that Participant and Moderator Security Codes must be auto-generated and must specify the length of such auto-generated codes.	Optional	The value can be integers between 6 and 8.
Presenter Security Code eventConfCode	Specify Presenter Security Code. In an Event Conference, when you enter the Presenter Security Code, the system assigns you	Mandatory if the User Template supports event conferencing.	-

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	the presenter role. Event Conference Host sets the Presenter Security Code. Presenter Security Code is mandatory if User Template contains Conferencing Class Of Service, supporting event conferencing.		

Import Users field descriptions

Use this page to bulk import users and their attributes from a valid XML or Excel file.

File Selection

Name	Description
Select Import File Type	The type of the file from where you import the users. The options are: • XML • Excel
Select File	The path and name of the XML or Excel file from which you import the users. If you select the Excel file option, use the template that System Manager supports. You can download the template from **User Management** > **Manage Users** > **More Actions** > **Download Excel Template**.

Button	Description
Browse	Displays a dialog box to select the file from which you import the users.

General

Name	Description
Select Error Configuration	The options are: • **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. • **Continue processing other records**: Imports the next user record even if the import user operation encounters an error while importing a user record.

Table continues…

Name	Description
Select Import Type	The options are: - **Complete**: Imports users with all the user attributes. - **Partial**: Imports users with specific user attributes. **Select Import Type** is available only for imports using the XML file.
If a matching record already exists	The options are: - **Skip**: Skips a matching user record that already exists in the system during an import operation. Currently, with this option you can add a new communication profile to a communication profile set but you cannot update an existing communication profile in a communication profile set. **Note:** This option is not available if you select the **Partial** option in **Select Import Type**. - **Replace**: Re-imports or replaces all the data for a user including access control lists, contact lists, and so on. With this option, you can replace a user and the associated data of the user. **Note:** **Replace** is available only for imports using the XML file. - **Merge**: 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 last name. - **Delete**: Deletes the user records from the database that match the records in the input file. **Note:** 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.

Job Schedule

Name	Description
Schedule Job	The options for configuring the schedule of the job: • **Run immediately**: Use this option to run the import job immediately. • **Schedule later**: Use this option to run the job at the specified date and time.
Date	The date on which you run the import users job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date. This field is available when you select the **Schedule later** option for scheduling a job.
Time	The 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 **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Button	Description
Import	Imports or schedules the import operation based on the option you selected.

Manage Job

Name	Description
Select check box	Use this check box to select a job.
Scheduled Time	The time and date of scheduling the job.
Status	The current status of the job. The following are the different status of a job: 1. PENDING EXECUTION: The job is in queue. 2. RUNNING: The job execution is in progress. 3. SUCCESSFUL: The job execution is completed. 4. INTERRUPTED: The job execution is cancelled. 5. PARTIAL FAILURE: The job execution has partially failed. 6. FAILED: The job execution has failed.

Table continues…

Name	Description
Job Name	A link to the Scheduler user interface. You can also cancel the job from the Scheduler user interface.
% Complete	The job completion status in percentage.
User Records	The total user records in the input file.
Warnings	The number of user records in the input file with warnings.
Errors	The number of user records in the input file that failed to import.

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

Import Users – Job Details field descriptions

The Import Users-Job Details page displays the details of the selected job.

Name	Description
Name	The import job that the end user initiates.
Scheduled by	The name of the user who initiates or schedules the import job
Scheduled at	The start time of the import job.
Error Configuration	The value that was configured for error while scheduling the Import Job. The values are **Abort on first error** and **Continue processing other records**.

Table continues…

Name	Description
Import Type	The value configured for the **Import Type** field while scheduling the import job. The values are **Complete** and **Partial**.
Import Option	The value that was configured for the **If a matching record already exists** field while scheduling the import job. The values are **Skip**, **Merge**, **Replace**, and **Delete**.
End	The end date and time of the job.
Status	The status of the job.
File	The name of the file that is used to import the user records.
Count	The total number of user records in the input file.
Success	The total number of user records that are successfully imported.
Fail	The total number of user records that failed to import.
Warning	The total number of user records that successfully imported, however, there are warnings generated for the user records.
Message	A message that indicates whether the import is successful or failure.
Completed	The percentage completion of the import.

Name	Description
Line Number	The line number in the file where the error occurred.
Login Name	The login name of the user record that failed to be imported.
Error Message	A brief description of the error.

Button	Description
Download	Exports and saves the user import error records in an XML file to the specified destination. **Note:** This button is not available if there are no error records for user Import Jobs or if the import job type is set to **Abort on first error**.
Cancel	Returns to the Import Users page.

To enable the **Download** button, on the User bulk import configuration page, set the **Enable Error File Generation** attribute to **True**.

To navigate to the User bulk import configuration page from the System Manager console, click **Services** > **Configurations** > **Settings** > **SMGR** > **User BulkImport profile**.

Import Global Settings field descriptions

Use this page to bulk import shared addresses, public contacts, and presence access control list (ACLs) from a valid XML file. These imported items are also called global user settings.

File Selection

Name	Description
Select File	The path and name of the XML file from which you must import the global settings records.

Button	Description
Browse	Opens a dialog box to select the file from which you must import the global user settings.

General

Name	Description
Select Error Configuration	The options are: • **Abort on first error**: Stops importing the global user settings records when User Management encounters the first error in the import file containing the global user settings records. • **Continue processing other records**: Imports the next global user settings record even if User Management encounters an error while importing a global user settings record.
If a matching record already exists	The options are: • **Skip**: 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. • **Merge**: 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. • **Replace**: 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. • **Delete**: Deletes the global setting records from the database that matches the records in the input XML file.

Job Schedule

Name	Description
Schedule Job	The settings for configuring the schedule of the job: • **Run immediately**: Use this option to run the import job immediately. • **Schedule later**: Use this option to run the job at the specified date and time.
Date	The date when you must 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 **Schedule later** option for scheduling a job.
Time	The 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 **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Button	Description
Import	Imports or schedules the import operation based on the option you selected.

Manage Jobs

Name	Description
Select check box	Use this check box to select a job.
Scheduled Time	The date and time when the job was scheduled.
Status	The current status of the job. The following are the different status of a job: 1. PENDING EXECUTION: The job is in queue. 2. RUNNING: The job execution is in progress. 3. SUCCESSFUL: The job execution is completed. 4. INTERRUPTED: The job execution is cancelled. 5. PARTIAL FAILURE: The job execution has partially failed. 6. FAILED: The job execution has failed.
Job Name	A link to the Scheduler user interface. You can also cancel the job from the Scheduler user interface.

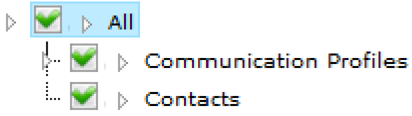
Table continues…

Name	Description
% Complete	The job completion status in percentage.
Records	The total number of global user settings records in the input file.
Error	The number of global user settings records in the input file that failed to import.

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

Export Users field descriptions

User Attribute Options

Name	Description
	User attribute options that an export administrator can choose to export for an export job. The options are: • **All**: The system exports all user attributes that includes all communications profiles and contacts. The default is **All**. • **Communications Profiles**: The export administrators can select communication profiles they want to export. For example : If the administrator selects all check boxes and clears the Session Manager profile check box, the system exports users with all data except the Session Manager communication profile attributes.

Name	Description
	- **Contacts**: The system exports all contacts. The system does not exports contacts if the check box is clear. **Note:** When you select the **Contacts** check box, the system exports the contacts of users only to an XML file. The system does not support exporting contacts to an Excel file. **Important:** If the exported file is used to import by using the replace option, the import operation replaces the existing user data from the system with user data in the exported file that might be incomplete because of the filter applied during the export.

Schedule

Name	Description
Schedule Job	The settings to configure the schedule of the job. The options are: - **Run immediately**: To run the export job immediately. - **Schedule later**: To run the job at the specified date and time.
Date	The date when you must run the export 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 **Schedule later** option for scheduling a job.
Time	The time of running the export 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 **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Button	Description
Export	Exports or schedules the export job based on the option that you selected.

Export List

Name	Description
Select check box	The option to select a job.
Start Time	The date and time when the job was scheduled.
Status	The status of the job. The options are: • PENDING EXECUTION: The job is in queue. • RUNNING: The job execution is in progress. • SUCCESSFUL: The job execution is completed. • INTERRUPTED: The job execution is cancelled. • FAILED: The job execution has failed.
Scheduled Job	A key to the Scheduler page. You can cancel the job from the Scheduler page.
% Complete	The job completion status in percentage.
User Records	The total number of user records that are marked for export.
Failed Records	The number of user records that failed to export.
Download File	The link to download the zip file that contains XML and Excel files.

Button	Description
View	Displays the details of the selected job.
Stop	Stops the export operation for the selected job.
Delete	Deletes the job that you selected.
Refresh	Refreshes the job details.
Select: All	Selects all the jobs from the list.
Select: None	Clears the check box selections.
Previous	Displays jobs in the previous page.
Next	Displays jobs in the next page.
Done	Returns to the User Management page.

Job Details field descriptions

The Job Details page displays the details of the selected Job.

Name	Description
Name	Specifies the name of the import job.
Scheduled by	Name of the user who initiated or scheduled the import job.
Scheduled at	Start time of the scheduled job.

Table continues…

Name	Description
End	End date and time of the job.
Status	Status of the job.
File	Name of the file that is used to import the global user settings records.
Count	Total number of global user settings records in the input file.
Success	Total number of global user settings records that are successfully imported.
Fail	Total number of global user settings records that failed to import.
Message	The message that indicates whether the import is successful or failure.
Completed	Displays the percentage completion of the import.

Name	Description
Record Number	Failed XML element in the input XML file.
Name	Name of the failed XML element.
Error Message	A brief description of the error.

Button	Description
Cancel	Takes you back to the Import Users page.

Quick start to importing users

Quick start to importing users

This section describes how to quickly create an XML file for importing users in bulk. This XML file includes user profiles with core attributes as well as with SIP phone (SIP communication profile).

XML for user with core attributes

The table lists the minimal elements for mapping the user import XML with user interface fields.

Table 3: Minimal elements

UI field	Description	XML tag	Possible value

Authentication Type	Specifies the type of authentication.	`<authenticationType>`
		...
		`</authenticationType>`
		>
			Basic or Enterprise

First Name	Specifies the first name of the user.	`<givenName>`	First name of the user.

Table continues…

UI field	Description	XML tag	Possible value
		... </givenName>	
Login Name	Specifies the primary handle of user.	<loginName> ... </loginName>	User log-in name.
Last Name	Specifies the last name of the user.	<surname> ... </surname>	Last name of the user.
Login Password	Specifies the password used to log in to System Manager.	<userPassword> ... </userPassword>	Login password of the user.

Sample XML with a single user profile

The following sample XML contains a user profile with basic fields. To create your own XML, replace the value of the tags explained in the Minimal elements table in *XML for user with core 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>
```

The highlighted XML tag in the user profile XML represents the data for a single user tag that starts and ends with `</tns:user>`. To create multiple users in the same XML, repeat the highlighted content multiple times with different user values.

For example, the following sample XML contains two users, John Miller and Roger Philip. Note that there are two instances of the `<tns:user>` tag, one for each user.

```
<?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>
    <authentication>TypeBasic</authenticationType>
    <givenName>John</givenName>
    <loginName>jmiller@avaya.com</loginName>
    <surname>Miller</surname>
    <userPassword>mypassword</userPassword>
  </tns:user>
```

```
<tns:user>
    <authenticationType>Basic</authenticationType>
    <givenName>Roger</givenName>
    <loginName>rphilip@avaya.com</loginName>
    <surname>Philip</surname>
    <userPassword>mypassword</userPassword>
  </tns:user>

</tns:users>
```

Note:

The XML is a text file. Therefore, you can edit this XML in any text editor.

Related links

XML for user with core attributes on page 514

Bulk import XML for users with SIP phone

To create a user XML, first perform the procedure for bulk importing users in the *Bulk importing users* section. If communication address is added to the user, then the **commPassword** field is mandatory.

To assign communication address, the mapping of Communication Profile for a new SIP user is as follows:

Table 4: Mapping of Communication Profile for a new SIP user

UI field	Description	XML tag	Possible value

Name	Specifies the name of the communication profile.	`<commProfileSetName>`
		...
		`</commProfileSetName>`
			The unique name of this communication profile.

Default	Indicates whether this is a default profile.	`<isPrimary>`
		...
		`</isPrimary>`
			True or False.

The attributes to set up the communication address for a user are as follows:

Table 5: User attributes to set up communication address

UI field	Description	XML tag	Possible value

Handle	Specifies the extension number of the user.	`<handleName>`
		...
		`</handleName>`
			Extension number.

Type	Specifies the communication type of the user profile.	`<handleType>`
		...
		`</handleType>`
			Communication type. For example, sip and smtp.

Table continues…

UI field	Description	XML tag	Possible value

SubType	Specifies the communication subtype of the user profile.	`<handleSubType>`
		…
		`</handleSubType>`
			Communication sub type. For example, username, e164, and msrtc.

Domain	Specifies the domain name of the user.	`<domainName>`
		…
		`</domainName>`
			Name of the configured SIP domain name.

The following is the mapping of Session Manager Communication profile elements with the corresponding user interface fields.

Table 6: Mapping of Session Manager Communication Profile elements

UI field	Description	XML tag	Possible value

Primary Session Manager	Specifies the name of the primary Session Manager instance that is used as the home server for a communication profile.	`<sm:primarySM>`
		…
		`</sm:primarySM>`
			Enter the name of Session Manager.

Origination Application Sequence	Specifies the Application Sequence that is invoked when calls are routed from this user.	`<sm:originationAppSequence>`
		…
		`</sm:originationAppSequence>`
			True or False.

Termination Application Sequence	Specifies the Application Sequence that is invoked when calls are routed to this user.	`<sm:terminationAppSequence>`
		…
		`</sm:terminationAppSequence>`	

Home Location	Specifies the routing home location.	`<sm:homeLocation>`
		…
		`</sm:homeLocation>`	

The following is the mapping of CM Endpoint Profile elements with the corresponding user interface fields.

Table 7: Mapping of CM Endpoint Profile elements

UI field	Description	XML tag	Possible value

System	Specifies the SIP Entity of the Communication Manager.	`<ipt:cmName>`
		…
		`</ipt:cmName>`
			Name of the configured Communication Manager.

Table continues…

UI field	Description	XML tag	Possible value

Use Existing	Indicates whether the station is already defined in the system.	`<ipt:useExistingExtension>`
		...
		`</ipt:useExistingExtension>`
			True or False.

Extension	Specifies the extension number for this profile.	`<ipt:extension>`
		...
		`</ipt:extension>`	

Template	Specifies the template name used for creating the station.	`<ipt:template>`
		...
		`</ipt:template>`	

Set Type	Specifies the set type of the station.	`<ipt:setType>`
		...
		`</ipt:setType>`	

Port	Specifies the port number from the list for the template you select.	`<ipt:port>`
		...
		`</ipt:port>`	

Related links

Bulk importing of users

Sample XML file for a user with SIP Communication Profile

Here is the sample XML of a user profile with basic fields. To create your own XML, replace the value of the tags explained in the Mapping of CM Endpoint Profile elements table in *Bulk import XML for users with SIP phone*.

```
<?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>
    <commPassword>12345</commPassword>
      <commProfileSet>
      <commProfileSetName>Primary</commProfileSetName>
      <isPrimary>true</isPrimary>
      <handleList>
        <handle>
          <handleName>sip:jmiller@avaya.com</handleName>
          <handleType>sip</handleType>
          <handleSubType>msrtc</handleSubType>
        </handle>
       </handleList>
      <!--The below is extended communication profile-->
      <commProfileList>
          <commProfile xsi:type="sm:SessionManagerCommProfXML" xmlns:sm="http://
xml.avaya.com/schema/import_sessionmanager">
            <commProfileType>SessionManager</commProfileType>
            <sm:primarySM>IBM1-Performance</sm:primarySM>
            <sm:terminationAppSequence>Perf_CM_Appl_Seq</sm:terminationAppSequence
            <sm:originationAppSequence>Perf_CM_Appl_Seq</sm:originationAppSequence
            <sm:homeLocation>SIT Lab</sm:homeLocation>
          </commProfile>

          <commProfile xsi:type="ipt:xmlStationProfile" xmlns:ipt="http://xml.avaya.com/
schema/import_csm_cm">
            <commProfileType>CM</commProfileType>
            <ipt:cmName>Performance_CM</ipt:cmName>
            <ipt:useExistingExtension>false</ipt:useExistingExtension>
            <ipt:extension>28000</ipt:extension>
            <ipt:template>DEFAULT_9620SIP_CM_5_2</ipt:template>
            <ipt:setType>9620SIP</ipt:setType>
            <ipt:port>S08012</ipt:port>
          </commProfile>
         </commProfileList>

      </commProfileSet>
    </tns:user>
</tns:users>
```

Related links

Bulk import XML for users with SIP phone on page 516

Managing public contacts

Manage public contact list

An administrator defines public contacts for the users in System Manager. You can share the public contacts with all the users in System Manager.

A user with administrator permission can 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

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.

3. On the Public Contacts page, click **New**.
4. On the New Public Contact page, in the **Contact Details** area, enter the appropriate information in the respective fields.

   Enter valid information in these fields to successfully create a new public contact.

   The 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.
5. In the **Postal Address** area, click **New** to add postal address of the contact.
6. In the **Contact Address** area, click **New** to add contact address.

   A contact address can be a phone number or any communication address that is supported by the application.
7. Click **Commit** to create a new public contact.

Related links

New Public Contact field descriptions on page 528

Modifying details of a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, click **Edit**.
4. On the Edit Public Contact page, modify the information of the contact.
5. Click **Commit**.

   ✱ **Note:**

   Before you click **Commit**, ensure that you entered valid information in the mandatory fields.

Related links

Edit Public Contact field descriptions on page 526

Deleting public contacts

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, select one or more contacts.

4. Click **Delete**.
5. On the Contact Delete Confirmation page, click **Delete**.

   The system deletes the contact from the default contact list of the user if the public contact is associated with the user.

Viewing the details of a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, select a public contact and click **View**.

   The View Public Contact page displays the details of a public contact.

Related links

View Public Contact field descriptions on page 524

Adding a postal address for a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, perform one of the following steps:
   - To add a postal address to a new public contact, click **New**.
   - To add a postal address to an existing public contact, select a public contact and click **Edit**.
4. Click **New** in the **Postal Address** area.
5. On the Add Address page, enter the appropriate information in the respective fields.

   Enter a valid information in these fields.
6. Click **Add** to create a new postal address for the public contact.
7. On the New Public Contact or Edit Public Contact page, click **Commit**.

Related links

Add Address field descriptions on page 202

Modifying postal address of a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, select a public contact and click **Edit**.
4. On the Edit Public Contact page, select an address from the Postal Address section.
5. Click **Edit**.
6. 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.
7. Click **Add** to save the modified address.

Related links

Add Address field descriptions on page 202

Deleting the postal addresses of a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, select a public contact and click **Edit**.

   If you are on the New Public Contact page, follow step 4.
4. Select an address from the table in the Postal Address section, and click **Delete**.
5. Click **Commit** to save the changes.

Choosing a shared address for a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. Click **Choose Shared Address**.
4. On the Choose Address page, select one or more shared addresses.
5. Click **Select** to add the selected addresses for the public contact.

6. Click **Commit**.

Adding a contact address of a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. Click **New** in the **Contact Address** area.
4. On the Add Address page, enter the appropriate information in the respective fields.

   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 links

Add Address field descriptions on page 239

Modifying the details of a public contact

About this task

You can use this feature to modify the contact details, postal address, and contact address of an existing public contact.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, select a public contact and click **Edit**.
4. On the Edit Public Contact page, modify the information in the Contact Details, Postal Address, and Contact Address sections.

   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.
5. Click **Commit**.

Related links

Edit Address field descriptions on page 240

Deleting the contact address of a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Public Contacts**.
3. On the Public Contacts page, select a public contact and click **Edit**.

   If you are on the New Public Contact page, follow Step 4.
4. In the **Contact Address** area, select one or more addresses from the list and click **Delete**.
5. Click **Commit** to save the changes.

View Public Contact field descriptions

Contact Details

Name	Description
Last Name	The last name of the contact.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the end points. For example, Miller. Typically, the name is the written or spoken language of the user. **Note:** When you create a user, if the **Last Name (Latin Translation)** and **First Name (Latin Translation)** fields are: • Blank, the system displays the last name and first name in the fields. The values change when the last name and first names change. • Filled, the values remain even after you change the values in the **Last Name** and **First Name** fields.
First Name	The first name of the contact.
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the contact.
Description	Displays a brief description of the contact.

Table continues…

Name	Description
Company	The name of contact's company.
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	The endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.

Postal Address

Name	Description
Name	The name of the contact.
Address Type	The mailing address type such as home or office address.
Street	The name of the street.
City	The name of the city or town.
Postal Code	The 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	The 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	The type of communication medium for interacting with the user.
Category	The categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This is similar to **Label**, but it is used to store label in an alternate language.

Related links

Viewing the details of a public contact on page 521

Edit Public Contact field descriptions

Contact Details

Name	Description
Last Name	The last name of the contact.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the end points. For example, Miller. Typically, the name is the written or spoken language of the user. ✱ **Note:** When you create a user, if the **Last Name (Latin Translation)** and **First Name (Latin Translation)** fields are: • Blank, the system displays the last name and first name in the fields. The values change when the last name and first names change. • Filled, the values remain even after you change the values in the **Last Name** and **First Name** fields.
First Name	The first name of the contact.
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the contact.
Description	Displays a brief description about the contact.
Company	The name of contact's company.
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	The endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.
Update Time	The time when the contact information was last updated.
Source	The source for provisioning the contact.

Postal Address

Name	Description
Name	The name of the contact.
Address Type	The mailing address type such as home or office address.
Street	The name of the street.
City	The name of the city or town.
Postal Code	The name of the contact's company.
Province	The full name of the contact's province.
Country	The name of the contact's country.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to add a new postal address of the public contact.
New	Opens the **Add Address** page. Use this page to modify an existing postal address of the public contact.
Delete	Deletes the selected public contacts.
Choose Shared Address	Opens the **Choose Address** page. Use this page to choose addresses of the public contact.

Contact Address

Name	Description
Address	The 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	The type of communication medium for interacting with the user.
Category	The categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays 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
Edit	Opens the **Edit Address** page. Use this page to edit a contact address of the public contact.
New	Opens the **Add Address** page. Use this page to add a contact address of the public contact.
Delete	Deletes the selected public contacts.

Button	Description
Commit	Saves the modified information to the database.

Related links

Modifying details of a public contact on page 520

New Public Contact field descriptions

Contact Details

Name	Description
Last Name	The last name of the contact.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the end points. For example, Miller. Typically, the name is the written or spoken language of the user. **Note:** When you create a user, if the **Last Name (Latin Translation)** and **First Name (Latin Translation)** fields are: • Blank, the system displays the last name and first name in the fields. The values change when the last name and first names change. • Filled, the values remain even after you change the values in the **Last Name** and **First Name** fields.
First Name	The first name of the contact.
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the contact.
Description	Displays a brief description of the contact.
Company	The name of company.
Localized Display Name	The localized display name of a user. It is typically the localized full name.
Endpoint Display Name	The endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.

Postal Address

Name	Description
Name	The name of the contact.
Address Type	The mailing address type such as home or office address.
Street	The name of the street.
City	The name of the city or town.
Postal Code	The name of the contact's company.
Province	The full name of the contact's province.
Country	The name of the contact's country.

Button	Description
Edit	Opens the **Edit Address** page. Use this page to add a new postal address of the public contact.
New	Opens the **Add Address** page. Use this page to modify an existing postal address of the public contact.
Delete	Deletes the selected public contacts.
Choose Shared Address	Opens the **Choose Address** page. Use this page to choose addresses of the public contact.

Contact Address

Name	Description
Address	The 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	The type of communication medium for interacting with the user.
Category	The categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays 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
Edit	Opens the **Edit Address** page. Use this page to edit a contact address of the public contact.
New	Opens the **Add Address** page. Use this page to add a contact address of the public contact.
Delete	Deletes the selected public contacts.

Button	Description
Commit	Creates a new contact. **Note:** Enter valid information in the mandatory fields to successfully create a new contact.

Related links

Adding a new public contact on page 519

Public Contacts field descriptions

Use this page to add new public contacts, and modify and delete the existing contacts.

Public Contacts

Name	Description
Last Name	The last name of the public contact.
First Name	The first name of the public contact.
Display Name	The display name of the public contact.
Contact Address	The address of the public contact.
Description	A brief description of the contact.

Button	Description
View	Displays the **View Public Contact** page. Use this page to view the details of the selected public contact.
Edit	Displays the **Edit Public Contact** page. Use this page to modify the information of the selected contact.
New	Display the **New public Contact** page. Use this page to add a new public contact.
Delete	Deletes the selected contacts.
Filter: Advanced Search	Displays fields that you can use to specify the search criteria for searching a public contact.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	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 upper-right corner of the public contact table.

Name	Description
Criteria	Displays the following three fields: • Field 1– The list of criteria that you can use to search public contacts. The options are: 1. Last Name: Searches public contacts by last name. 2. First Name: Searches public contacts by first name. 3. Display Name: Searches public contacts by display name. 4. Contact Address: Searches public contacts by contact address. • Field 2 – The operator for evaluating the expression. The list of operators displayed depends on the type of criterion that you selected in field 1. • Field 3 – The search value for the search criterion selected in field 1.

Managing shared addresses

Manage shared address

Shared address contains common addresses that you can specify for one or more users in the enterprise. The user with appropriate permissions can create a new shared address and modify and delete an existing shared address. For example, you can add the address of the company in the list of shared address and other users can use this address as their alternative address.

Assigning a shared address to the user

About this task

You can use the functionality to choose a shared address for a user from common addresses. You can assign and unassign a shared address.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following:
   - To assign shared addresses to a new user while creating the user, click **New**.
   - To assign shared addresses to an existing user, select the user, and click **Edit** or **View** > **Edit**.
4. On the New User Profile page or the User Profile Edit page, click **Identity** > **Address** > **Choose Shared Address**.
5. On the Choose Address page, select one or more shared addresses.

   For a new user, enter valid information in all mandatory fields on all tabs of the New User Profile page before you click **Commit**. If you enter invalid information, the system displays an error message.
6. Click **Select**.
7. Perform one of the following:
   - To save the changes, click **Commit**.
   - To save the changes and stay on the same page for making further modifications, click **Commit & Continue**.

Related links

Choose Address field descriptions on page 204

Adding a shared address

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Shared Addresses**.
3. On the Shared Address page, click **New**.
4. On the Add Address page, enter the appropriate information.
5. Click **Add**.

Result

The new address is available as shared address and you can specify this address when you create or modify a user account.

Modifying a shared address

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Shared Addresses**.
3. On the Shared Address page, select an address and click **Edit**.
4. On the Edit Address page, modify the information in the fields.
5. Click **Add**.

Deleting a shared address

About this task

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.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Shared Addresses**.
3. On the Shared Address page, select the address you want to delete and click **Delete**.

Add Address field descriptions

Name	Description
Address Name	The unique label that identifies the mailing address.
Address Type	The mailing address type such as home or office address.
Building	The name of the building.
Room	The number or name of the room.
Street	The name of the street.
City	The name of the city or town.
State or Province	The full name of the province.
Postal Code	The postal code or zip code used by postal services to route mail to a destination. For the United States, specify the Zip code.
Country	The name of the country.

Phone Details section

Name	Description
Business Phone	The business phone number of the user.
Other Business Phone	The secondary or alternate business phone number if applicable.
Home Phone	The residential phone number of the user.
Other Home Phone	The secondary or alternate residential phone number if applicable.
Mobile Phone	The mobile number of the user.
Other Mobile Phone	The secondary or alternate mobile number of the user if applicable.
Fax	The telephone number for direct reception of faxes.
Pager	The number used to make calls to the pager of the user.
Other Pager	The secondary or alternate number used to make calls to the pager of the user.

Button	Description
Add	Adds the mailing address of the user.
Cancel	Cancels the add address operation.

Related links

Modifying a shared address on page 533

Adding a shared address on page 532

Edit Address field descriptions

Use this page to edit the details of a contact's communication address.

Name	Description
Address	Displays the address that you can use to communicate with the contact. This can be a phone number, email address, SIP, or IM of the contact. The format of the address must conform to the type of address that you select in the **Type** field.
Type	Displays the type of address. The types of addresses are: • **Phone**: This address type supports phone numbers. • **SIP**: This address type supports SIP-based communication.

Table continues…

Name	Description
	• **MSRTC**: This address type supports communication with a Microsoft RTC server. • **IBM Sametime**: This address type supports communication with IBM Sametime. Specify the address in the DN=IBMHandle format. • **XMPP**: This address type supports xmpp-based communication. • **SMTP**: This address type supports communication with the SMTP server.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays 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
Add	Saves the modified information to the database.

Related links

Modifying the details of a public contact on page 523

Shared Address field descriptions

Use this page to create a new shared address and modify and delete an existing shared address.

Shared Address

Name	Description
Select check box	Provides the option to select an address.
Name	Displays the name of the person or entity associated with the address.
Address Type	Displays the type of address indicates whether the address is an Office or home address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the postal code used by postal services to route mail to a destination. In the United States, this is the Zip code.
Province	Displays the full name of the province.

Table continues…

Name	Description
Country	Displays the name of the country.
Refresh	Refreshes the address information in the table.
All	Selects all the addresses in the table.
None	Clears the check box selections.

Button	Description
New	Opens the Add Address page . Use this page to add an address.
Edit	Opens the Edit Address page. Use this page to modify the mailing address information.
Delete	Deletes a selected address.

Managing presence access control lists

Manage Presence Access Control Lists

Default Policy rules are global default rules that define access to presence information if none of the more specific rules apply. You must define atleast one System Default rule in the system.

Related links

Presence ACL field descriptions on page 536

Presence ACL field descriptions

Define Policy

You can use this section to define your personal rules for one or more watchers to access your presence information.

Field	Description
Select check box	The option to select a rule.
Access Level	The presence information for which access control rules are set.
Action	The access control permission for the presence information.

Button	Description
Edit	Changes the existing rule.
New	Adds a new rule for watchers.
Delete	Deletes the selected rule from the list of rules that are added for watchers.

The page displays the following fields when you click **New** or **Edit**:

Field	Description
Access Level	The presence information for which access control rules are set. The options are: • **Telephony**: The telephony-related presence information for which you can set an access permission. • **All**: All types of presence information for which you can set an access permission.
Action	The access control permission for the presence information. The options are: • **Allow**: Provides watcher the access to the presence information for the access level. • **Block**: Blocks the watcher from accessing the presence information for the access level. • **Confirm**: Watcher requires confirmation from the presentities to access the presence information of presentities. • **Undefined**: Access to the presence information for the access level is undefined for the watcher.

Button	Description
Save	Saves the rules information to the database when you add or change a rule for watchers.

Communication profile password policy enforcement

Communication profile password policy

The system administrator defines a password strength policy for the communication profile password. The policy has the following constraints:

- Passwords must contain 8 to 25 characters. The default is eight characters.
- Passwords must contain a combination of the following characters: a-zA-Z0-9{}|()<>,/.=[]^_@!$%&-+":?`;
- Passwords must contain at least one each of the following characters:
  - A lowercase letter
  - An uppercase letter
  - A digit
  - A special character

If a password does not meet the password strength policy, the system rejects the password. You can disable the password policy.

Related links

Editing the password policy for communication profile on page 538
Communication Profile Password Policy field descriptions on page 539

Editing the password policy for communication profile

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Communication Profile Password Policy**.
3. Complete the following steps as appropriate:
   a. In the **History** section, select the **Enforce policy against previously used passwords** check box, and modify the **Previous passwords disallowed** field.
   b. In the **Strength** section, select the **Enforce password content standards** check box, and modify the required fields.

   For more information, see Communication Profile Password Policy field descriptions.
4. Click **Commit**.

   The system saves the changes that you made to the password policy for the communication profile password.
5. **(Optional)** To undo the changes, click **Cancel**.

Related links

Communication Profile Password Policy field descriptions on page 539

Communication Profile Password Policy field descriptions

History

This page is applicable only for admin users.

Field	Description
Enforce policy against previously used passwords	Select the check box to enforce policies against earlier passwords.
Previous passwords disallowed	The number of latest passwords that the system maintains in history. You cannot reset your password to these values. The default is 6. The range is 1 to 99.

Strength

Field	Description
Enforce password content standards	Select the check box to enforce password content standards.
Minimum Required Length	The minimum number of characters that you must use in the password. The default is 8. The password can be of 6 to 25 characters.
Lower Case	The minimum number of lowercase characters that you must use in the password. The default is 1.
Upper Case	The minimum number of uppercase characters that you must use in the password. The default is 1.
Numeric Character	The minimum number of numeric characters that you must use in the password. The default is 1.
Special Character	The minimum number of special characters that you must use in the password. The default is 1.

Button	Description
Commit	Saves all your entries in the Communication Profile Password Policy page.
Cancel	Disregards the changes and goes you back to the earlier page.

Chapter 8: Managing user provisioning rules

User Provisioning Rule

System Manager 6.3.4 introduced a new set of workflows to streamline the user provisioning process. You can apply a user provisioning rule with other LDAP Synchronization Capabilities to achieve fully automated user provisioning. You can also assign a communication profile to every user.

A user provisioning rule includes a master communication profile template and a set of provisioning rules. A user provisioning rule enables predefined templates that consist of user attributes found in the communication profile of the user. In the user provisioning rule, the administrator specifies the following information to provision the user:

- Basic information that includes the communication profile password, time zone, and language preference
- The communication system that the user must use, for example, Communication Manager
- The method to assign or create a communication profile for the user, for example, by assigning the next available extension for Communication Manager

When the administrator creates the user using the user provisioning rule, the system populates the following data based on the user provisioning rule:

- The default values
- The communication addresses
- The communication profiles for the user

You can create and apply the user provisioning rule only if you have administrator credentials. The administrator can assign only one user provisioning rule to every user. The administrator can provision the user using the user provisioning rule from one of the following System Manager user interfaces:

- Web Console
- Web Services
- Folder name Synchronization
- Bulk import

Note:

To perform the user provisioning by using the user provisioning rule, map the user to the role with the following permissions:

Resource type	Permissions
All elements of type:elements	view

Capabilities and guidelines of user provisioning rules

Capabilities of user provisioning rules

User provisioning rule is a template that you can use to create a user. You can define and apply a user provisioning rule only if you have administrator credentials. You can use the user provisioning rule for the initial provisioning and during the creation of the user. User provisioning rules cannot be used after they are applied. After you create a user a user provisioning rule, System Manager populates the following data based on the rules defined in the user provisioning rule:

- The default values
- The communication addresses
- The user attributes from the communication profiles

General guidelines

- After you define a user provisioning rule and apply the user provisioning rule to create a user, you cannot edit the communication profile associated with the user provisioning rule. You cannot change, delete, or add the data in the communication profile. To edit the communication profile, you must reapply the user provisioning rule to the user. You can assign only one communication profile to a user provisioning rule.

  If user provisioning rule and communication profile data are available from System Manager user interface or bulk import, the communication profile data that you provide takes the precedence. System Manager does not use the communication profile data that is available in the user provisioning rule.

- You can edit the user attributes that are not the part of the communication profile. To edit such user attributes, you can use any of the following System Manager user provisioning interfaces:
  - System Manager native user interface
  - Web Services API
  - Bulk import and export
  - Global Endpoint Change Editor

Adding User Provisioning Rules

About this task

Add a service defined in a communications profile to an existing user that was created by using a user provisioning rule.

Procedure

1. Create a new user provisioning rule with the new service defined in the communication profile of the new rule.

   The system adds the new service defined in the communications profile to the existing user.

   You can add any of the following services:

   - Presence
   - Messaging
   - Engagement Development Platform
2. Apply the user provisioning rule to the user through LDAP synchronization.
3. Update the LDAP enterprise directory with the new user provisioning rule.
4. Synchronize users.

   The system creates a new communication profile for the user.

Creating the user provisioning rule

Procedure

1. Log on to System Manager as admin.
2. On the System Manager web console, click **Users** > **User Provisioning Rule**.
3. On the User Provisioning Rules page, click **New**.
4. On the New User Provisioning Rule page, perform the following:
   a. On the **Basic** tab, enter the appropriate information.
   b. On the **Communication Profile** tab, select the appropriate communication profile, and enter the information.

   For more information, see User Provisioning Rule field descriptions.
5. Click **Commit** to save the changes.

Related links

User Provisioning Rule field descriptions on page 545

Modifying the user provisioning rule

Before you begin

Create a user provisioning rule.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager web console, click **Users** > **User Provisioning Rule**.
3. On the User Provisioning Rules page, select the user provisioning rule.
4. To edit the user provisioning rule, perform one of the following:
   - Click **Edit**.
   - Click **View** > **Edit**.
5. On the Edit User Provisioning Rule page, perform the following:
   a. On the **Basic** tab, modify the appropriate information.

      Note:

      - System Manager does not automatically modify the user if the user provisioning rule changes.
      - You can select a different user provisioning rule when you modify the user information.

   b. On the **Communication Profile** tab, modify the communication profile information as appropriate.

   For information, see User Provisioning Rule field descriptions.
6. Click **Commit**.

Related links

User Provisioning Rule field descriptions on page 545

Viewing the user provisioning rule

Before you begin

Create a user provisioning rule.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager web console, click **Users** > **User Provisioning Rule**.
3. On the User Provisioning Rules page, select the user provisioning rule and click **View**.

Related links

User Provisioning Rule field descriptions on page 545

Creating a duplicate user provisioning rule

About this task

You can duplicate a user provisioning rule to create a new user provisioning rule by copying the information from the existing user provisioning rule.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager web console, click **Users** > **User Provisioning Rule**.
3. On the User Provisioning Rules page, select the user provisioning rule.
4. Click **Duplicate**.
5. On the Duplicate User Provisioning Rule page, perform the following:
    a. On the **Basic** tab, change the appropriate information.
    b. On the **Communication Profile** tab, change the communication profile information as appropriate.

    For more information, see User Provisioning Rule field descriptions.
6. Click **Commit**.

Related links

User Provisioning Rule field descriptions on page 545

Deleting the user provisioning rule

Procedure

1. Log on to System Manager as admin.
2. On the System Manager web console, click **Users** > **User Provisioning Rule**.
3. On the User Provisioning Rules page, select one or more user provisioning rules.
4. Click **Delete**.
5. On the Delete User Provisioning Rule page, click **Delete**.

    The system removes the user provisioning rule from System Manager.

    System Manager disassociates the user provisioning rule from the user if you have already provided the user provisioning rule for the user.

Related links

User Provisioning Rule field descriptions on page 545

User Provisioning Rules Management field descriptions

Field	Description
Name	The name of the user provisioning rule.
SIP Domain	The name of the configured SIP domain name.
Description	A brief description of the user provisioning rule.

Button/Icon	Description
View	Displays the View User Provisioning Rule page with details of the user provisioning rule that you selected.
Edit	Displays the Edit User Provisioning Rule page where you can modify the selected rule.
New	Displays the New User Provisioning Rule page where you can create a new rule.
Delete	Deletes the user provisioning rule that you selected.
Duplicate	Copies the user provisioning rule that you selected.
🔄	Refreshes the user provisioning rule information in the table.
Select	• All: Selects all user provisioning rules in the table. • None: Clears the check box selections.

User Provisioning Rule field descriptions

Basic

Field	Description
User Provisioning Rule Name	The name of the user provisioning rule.
Description	A description of the user provisioning rule.
SIP Domain	The name of the configured SIP domain name. If **SIP Domain** is nonblank, create an Avaya SIP communication address for this user.
Presence/IM Domain	The name of the configured Presence domain name.

Table continues…

Field	Description
	If **Presence/IM Domain** is nonblank, create an Avaya Presence/IM communication address for this user.
Communication Profile Password	The communication profile password.
Confirm Password	The communication profile password that you must re-enter.
Use Phone Number last ..... digits for Extension	The number of last digits of the phone number that the system uses from the LDAP attribute. E.164 numbers can contain maximum 15 digits. Usually, the numbers are written with a plus (+) as the prefix. The system populates the phone number that is mapped to the LDAP attribute with the value in the **Prefix for Avaya E164 Handle** field. The LDAP attribute is mapped to the `Phone Number` attribute of System Manager on the User Synchronization Datasource page.
Prefix for Avaya E164 Handle	The digits that the system must prefix to Avaya E. 164 Handle.
Language Preference	The preferred written or spoken language of the user. For example, English.
Time Zone	The preferred time zone of the user.

Button	Description
Commit	Creates the user provisioning rule and displays the User Provisioning Rule page.
Cancel	Cancels the create, edit, or delete operation of the user provisioning rule.
Done	Saves the changes that you make to the user provisioning rule. The system displays this button only during the view operation.
Edit	Displays the fields in the edit mode. The system displays this button only during the view operation.

Communication Profile tab: Session Manager Profile

Note:

The system displays the following fields only if a communication profile of the user exists for the product.

Field	Description
Primary Session Manager	The instance that you want to use as the home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura® network. You must select the primary Session Manager server.
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. A selection is optional.
Survivability Server	For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile when the local connectivity to Session Manager instances in Avaya is lost. If you select a Branch Session Manager , and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional. ✱ **Note:** If a termination or origination application sequence contains a Communication Manager application, the Communication Manager instance associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.
Block New Registration When Maximum Registrations Active	If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint.

Table continues…

Field	Description
Origination Application Sequence	The application sequence that the system will invoke when routing the calls from this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Termination Application Sequence	The application sequence that will be invoked when the system routes the calls to this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Home Location	The home location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any of the location. You must specify a value.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.

Communication Profile tab: Engagement Development Platform Profile

Name	Description
Service Profile	The profile that you assign to the user. The user can gain access to the service contained in the profile.

Communication Profile tab: CM Endpoint Profile

Note:

The system displays these fields only if a CM Endpoint profile exists for the user.

Field	Description
Use Next Available Extension	Select the check box to instruct the system to create a new extension for the user. **Note:** For LDAP synchronization, the value in the **Use Phone Number last ..... digits for Extension** field takes priority.
Template	The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add. You must select the template.
Security Code	The security code for authorized access to the endpoint.
Preferred Handle	Avaya SIP or Avaya E.164 handle that is administered for the user. The field is optional. By default, the field is blank.
Password	The password to gain access to the endpoint. The system displays the field if you select Agent in the **Profile Type** field.
Allow H.323 and SIP Endpoint Dual Registration	The option to register both an H.323 endpoint and a SIP endpoint together at the same time to the same extension.

Communication Profile tab: CS 1000 Endpoint Profile

Field	Description
System	The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.
Target	The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template.
Template	The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template.
Include in Corporate Directory	The option to add this profile to the CS 1000 Corporate Directory feature.
Delete Endpoint on Unassign of Endpoint from User	An option to specify whether to delete the endpoint from the CS 1000 system when you unassign the endpoint from the user.

Communication Profile tab: MessagingProfile

Note:

The system displays the following fields only if you can configure a messaging profile for the user.

Name	Description
System	The messaging system on which you add the subscriber. You must select the system.
Mailbox Number	The mailbox number of the subscriber. The options are: • Use CM Extension: Use this option only if the Communication Manager profile and Session Manager profile are specified. • Use Next Available Subscriber: Use this option if the system must use the next mailbox number to associate with this profile.
Template	The system-defined or user-defined template that you associate with the subscriber.
Password	The password for logging in to the mailbox. You must provide the password.
Delete Subscriber on Unassign of Subscriber from User or on Delete User	The option to specify whether 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.

Communication Profile tab: CallPilot Messaging Profile

You cannot assign the mailbox number in the CallPilot communication profile by using the user provisioning rule. You must add the mailbox number for the CallPilot communication profile.

Field	Description
System	The CallPilot system of the messaging profile. The selection is mandatory required.
Target	The field that maps to the CallPilot **Location** field. CallPilot Manager provides the **Target** field. You must select the target.
Template	The mailbox template that you use. Select a template from the drop down list. The element manager maintains all the mailbox templates. You must select the template.

Communication Profile tab: IP Office Endpoint Profile

Field	Description
System	The list of IP Office device names from which you can select the IP Office device that you associate with the user. You must select the template.
Extension	The extension of the endpoint to which you associate the profile. The options are: • Use CM Extension: Use this option only if Communication Manager profile is specified. • Use Next Available Extension: Use this option if the system must use the next extension to associate with this profile.
Template	A list of user templates from which you can select a template to set the user configurations.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the system automatically populates the set type value.

Communication Profile tab: Presence Profile

Name	Description
System	The Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile: • Aggregate presence • Archive instant messages if the Instant Messages option is enabled
SIP Entity	The option to route the SIP-based messages through the Presence Services This system selects the SIP entity only if you select a Presence Services instance in the **System** field. **SIP Entity** is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.
IM Gateway	The IP address of the IM gateway.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with the AES Collector. The options are: • **System Default** • **Off**

Table continues…

Name	Description
	• **On** The default is **System Default**. You can change the default value. You do not require to configure AES Collector in the Presence Services server.

Communication Profile tab: Conferencing Profile

Name/Button	Description
Template	The template that you use to set the user configurations.
Location	The location that Conferencing uses when the IP address of the calling phone does not match any IP address pattern of any location. Specify this field to support the mobility of the user.
Select Auto-generated Code Length	The number of digits in the security code that the system generates.
Auto Generate Participant and Moderator Security Codes	The check box that you select to instruct the system to generate the security codes for the participant and moderator.

Button	Description
Commit	Saves the changes and displays the User Provisioning Rules page.
Cancel	Cancels the operation and displays the User Provisioning Rules page.

Chapter 9: Managing elements

Registering CS 1000 or CallPilot with System Manager

Adding CallPilot to the element registry

Procedure

1. On the System Manager console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Elements**.
3. On the Elements page, click **Add**.
4. On the Add New Element page, specify the following:
    - **Name**: Element name of CallPilot.
    - **Description**: Element description of CallPilot.
    - **Type**: Element type from the drop-down list.
5. On the Add New Element page, click **Next** and then specify the following:
    - **CallPilot Manager address**: The IP address or FQDN of CallPilot Manager.
    - **CallPilot server address**: The IP address or FQDN of the CallPilot server.
    - **Administrator mailbox number**: The administrator mailbox number.
    - **Administrator password**: The administrator password.
6. Click **Save**.

Adding CallPilot certificate to System Manager

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. In the **Elements** section, select a managed element instance.
4. On the Manage Elements page, click **More Actions** > **Configure Trusted Certificates**.

The system displays the certificates that are currently installed on the managed element you selected.

5. To add a CallPilot certificate, click **Add**.
6. On the Add Trusted Certificate page, in the **Select Store Type to add trusted certificate** field, click **All**.
7. To add the certificate, perform one of the following:
   - To import the certificate as PEM, click **Import as PEM Certificate**.
   - Copy the certificate from the `.CER` file to the window on the Add Trusted Certificate page.
8. Click **Commit**.

Importing users from Subscriber Manager to User Management

User data import to System Manager

The User Profile Management (UPM) service in System Manager is a single point of administration for user profile data associated with multiple Avaya products. Similarly, the Subscriber Manager service in CS 1000 UCM is a single point of administration for user profile data for Heritage Nortel products. In System Manager 6.1, the UPM and Subscriber Manager applications coexist and are part of System Manager. Element Managers use:

- UPM to manage users for Heritage Avaya products
- Subscriber Manager to manage users for Heritage Nortel products

In System Manager 6.2, Subscriber Manager is merged into UPM and is called User Management (UM). UM includes several Subscriber Manager features. With the removal of Subscriber Manager, perform the steps listed in this section on System Manager 6.1 and 6.2 or later to ensure that the subscriber data is successfully migrated to UM of System Manager 6.2 and later.

Prerequisites

Register CS 1000 with the preupgraded System Manager Release 6.1 primary security domain.

Moving users and accounts from Subscriber Manager to User Management involves the following key procedures:

- On System Manager Release 6.1: Preparing the Subscriber Manager user data for import to User Management. This preimport procedure copies the Subscriber Manager Universally Unique ID (UUID) of the user to another field which can be preserved during the import to User Management. After the import, you must use the UUID to reassociate phones and mailboxes.
- On System Manager Release 6.1: Importing the Subscriber Manager user data to User Management. This procedure transfers the user data from the Subscriber Manager directory to the User Management database using LDAP synchronization.

- On System Manager Release 6. 2 and later: Performing postimport tasks that involve:
    - Exporting the users to an XML file to assign communication profile passwords in User Management and reimporting the users.
    - Creating the communication profile for each user and performing profile synchronization in User Management for CS 1000 and CallPilot elements that you import.

Related links

Adding CallPilot to the element registry on page 553

Preparing the Subscriber Manager user data for import to User Management

You must perform this procedure on System Manager Release 6.1.

Before you begin

- Ensure that you install the latest CS 1000 Service Pack on all the CS 1000 network elements.
- Ensure that you update all Subscriber Manager user profiles for completeness that includes First Name, Last Name, and Preferred Name / CPND Name.
- Ensure that you synchronize Subscriber Manager and the CS 1000 network elements and that you upload Corporate Directory and Numbering Groups to the CS 1000 network elements.
- Ensure that the firewall is stopped on System Manager Release 6.1. Perform the following to verify that the firewall is stopped:
    1. Using the command line interface, log in to System Manager Release 6.1 as `root`.
    2. Enter `service iptables status`.

       The system must indicate that the firewall service has stopped.
    3. If firewall is enabled, enter `service iptables stop`.

       The system stops the firewall service.

Procedure

1. Log on to the Web console of System Manager Release 6.1.
2. On the Avaya Unified Communications Management page, click **Network** > **Subscriber Manager**.
3. In the left navigation pane, click **CSV Export**.
4. Click **Generate** on the upper-right of the page to create a new `CSV` file with the latest subscriber data.
5. Click **Download** on the upper-right of the page to download the subscriber data to your computer.

   Note the location of the `subscribers.csv` file.

6. Open the `subscribers.csv` file using Microsoft Excel and perform the following steps:

    a. Copy the data from the **UUID** column to the **postOfficeBox** column, without the column header information. This is to ensure that the Subsciber Manager datastore UUID is mapped to a column that the UPM LDAP datastore synchronization supports. For example:

entryUUID	postOfficeBox
c0bbc2d2-3096-4ce8-8fca-2670ea681be3	c0bbc2d2-3096-4ce8-8fca-2670ea681be3
86d11715-3b36-4238-be37-5284ca7a7a68	86d11715-3b36-4238-be37-5284ca7a7a68

    b. Copy the data from the **ucDomain** to the **User ID (uid)** column. For example:

ucDomain	uid
ca.avaya.com	user1@ca.avaya.com
ca.avaya.com	user2@ca.avaya.com

    c. Save the modified `subscribers.csv` file in a csv format.

7. To synchronize the Subscriber Manager data with the modified `subscribers.csv` file, import the modified Subscriber Manager data in the `subscribers.csv` file back to Subscriber Manager and perform the following steps:

    a. In the left navigation panel, on the **Subscriber Manager**, click **CSV Synchronization**.

    b. Browse to the location where you saved the modified `subscribers.csv` file.

    c. Click **Synchronize**.

    d. Click **View Results** to verify that the synchronization is successful.

    If error occurs, the page displays the location of the error logs on the System Manager server. For example, `/opt/nortel/cnd/log/LDAP_Sync`.

    e. Click **Subscribers**, and perform the following:

        a. Leave the **Name** field blank.

        b. Click **Search**.

    f. Select one of the user and verify that the system updated the **Unified Communication Username** field correctly.

    The system does not display the **postOfficeBox** field.

8. If Numbering Groups are used, perform the following:

    a. Click **UCM Services** > **Numbering Groups**.

    b. Click **Generate**.

    c. Click **Export** to export the data to a location on your computer to ensure that the data is captured.

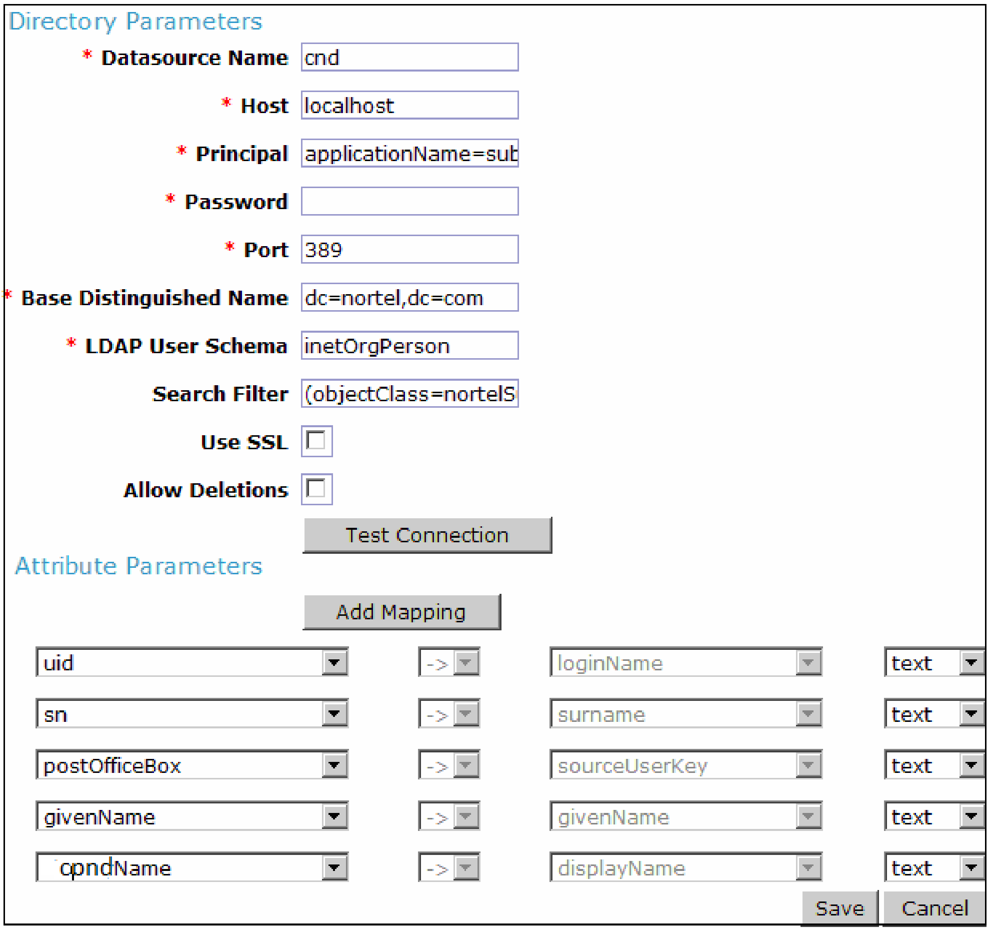
Importing the Subscriber Manager user data to User Management

Before you begin

- Log on to the web console of System Manager Release 6.1.
- Prepare the Subscriber Manager user data for import to User Management.

Procedure

1. On the System Manager web console, click **Users** > **Synchronize and Import**.
2. In the left navigation pane, click **Sync Users**.
3. To create a new LDAP synchronization source, on the **Synchronization Datasources** tab, click **New** and enter the directory parameters as listed in the Subscriber Manager datasource parameters and attributes table.



Directory Parameters

* **Datasource Name**	cnd
* **Host**	localhost
* **Principal**	applicationName=sub
* **Password**	
* **Port**	389
* **Base Distinguished Name**	dc=nortel,dc=com
* **LDAP User Schema**	inetOrgPerson
Search Filter	(objectClass=nortelS
Use SSL	□
Allow Deletions	□

Attribute Parameters

uid	->	loginName	text
sn	->	surname	text
postOfficeBox	->	sourceUserKey	text
givenName	->	givenName	text
cpndName	->	displayName	text

Note:

If a subscriber does not have an account or the cpndName field is blank, you can map Last name, First Name to the displayName attribute of System Manager.

4. Click **Test Connection** to verify that the system can establish connection to the cnd database.
5. Perform the following steps to run the LDAP synchronization job:
    a. On the Sync Users page, on the **Active Synchronization Jobs** tab, click **Create New Job**.
    b. On the New User Synchronization Job page, in the **Datasource Name** field , select the name of the datasource and click **Run Job**.

       The system starts the synchronization of the Subscriber Manager datastore with the User Management datastore.
6. On the Sync Users page, on the **Synchronization Job History** tab, click **View Job Summary** for the cnd job, and verify that the system successfully imported the users in the **Added** and **Modified** fields.

   Note:

   The **Failed** field might contain some errors due to the import of unsupported fields.
7. To verify that the users are available in User Management, do the following:
    a. Navigate to **Users** > **User Management** > **Manage Users**.
    b. On the User Management page, select a user and click **View** or **Edit** and verify that the System Manager Release 6.1 is configured correctly.

       System Manager Release 6.1 now contains User Management configured with the Subscriber Manager data. The system is now ready for upgrading to System Manager Release 6.2 and later.

Related links

Creating the user synchronization job on page 60
Adding the synchronization datasource on page 51
Subscriber Manager datasource parameters and attributes on page 558

Subscriber Manager datasource parameters and attributes

Use the values from the following tables to update the fields on the Edit User Synchronization Datasource page.

Directory Parameters

Parameter	Value
Datasource Name	cnd
Host	For UPM: localhost For CS 1000: <**CS 1000 UCM R7.X Server IP**>

Table continues…

Parameter	Value
Principal	applicationName=subMgr,ou=Applications,dc=Nortel, dc=com
Password	submgrpass
Port	389
Base Distinguished Name	dc=nortel,dc=com
LDAP User Schema	inetOrgPerson
Search Filter	(objectClass=nortelSubscriber)
Use SSL	Clear the check box.
Allow Deletions	Clear the check box.

Attribute Parameters

Map the following attributes of the Subscriber Manager datasource to the attributes of the User Management datastore.

Subscriber Manager attribute	User Management attribute	Import Type	Description
uid	loginName	text	Modified Subscriber Manager uid: user1@domain.
sn	surname	text	
postOfficeBox	sourceUserKey	text	Saved Subscriber Manager UUID.
givenName	givenName	text	
displayName	displayName	text	

Exporting the user data and creating the user profile

To complete the import job of the user data from Subscriber Manager, you must perform the following procedure after you complete the server upgrade from System Manager Release 6.1 to Release 6.2 and later.

Before you begin

Start an SSH session.

About this task

The system does not support the export of users and user profiles in bulk from the web console of System Manager Release 6.2 and release earlier than 6.3.8. Therefore, use the command line interface of System Manager to perform bulk export activities.

Procedure

1. Log on to the system on which you want to export the user data as root.

2. Export the users and the user profiles using the following steps:
    a. Perform one of the following:
        - For System Manager 6.3.8 and later, use the web console to export the user data.

          For more information, see Exporting users in bulk.
        - For System Manager 6.3, type `cd $MGMT_HOME/bulkadministration/exportutility/`.
        - For System Manager 6.2, type `$MGMT_HOME/upm/bulkexport/exportutility/`.

    b. For System Manager release earlier than 6.3.8, type `sh exportUpmUsers.sh`.

       The system creates an XML file `exportfile_<time stamp in milliseconds>.zip` in the `$MGMT_HOME/upm/bulkexport/` location.

       The system also creates a `readme.txt` file that outlines the use and various options for the export utility in the `$MGMT_HOME/upm/bulkexport/exportutility/` directory. For information, see Bulk exporting of users.
3. Copy the zip file on the desktop of your local computer and extract the XML file.

   Note the location where you saved the file.
4. Make the following edits to the XML file:
    a. Add the <commPassword>password_value</commPassword> tag after the <userName> tag to assign the communication profile password in User Management.

       Note:

       The password must have at least seven characters and the first character must not be a digit or a special character such as <, >, ^, %, $, @, # and *.
    b. Delete the <userPassword>userpassword_value</userPassword> tag.

   For example:

```
<tns:user>
        <authenticationType>enterprise</authenticationType>
        <displayName>user1</displayName>
        <displayNameAscii>user1</displayNameAscii>
        <dn>cn=f225860c-2f2c-4290-
a660-660e51fe0d4f,ou=Subscribers,dc=nortel,dc=com</dn>
        <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>first1</givenName>
        <loginName>user1@ca.avaya.com</loginName>
        <preferredLanguage>en-US</preferredLanguage>
        <source>cnd</source>
        <sourceUserKey>c0bbc2d2-3096-4ce8-8fca-2670ea681be3</sourceUserKey>
        <status>provisioned</status>
        <surname>last1</surname>
        <userName>user1</userName>

        <commPassword>123456</commPassword>
        <roles>
            <role>End-User</role>
        </roles>
        <ownedContactLists>
            <contactList>
                <name>list-user1_ca.avaya.com</name>
                <isPublic>false</isPublic>
                <contactListType>general</contactListType>
            </contactList>
        </ownedContactLists>
        <commProfileSet>
            <commProfileSetName>Primary</commProfileSetName>
            <isPrimary>true</isPrimary>
        </commProfileSet>
    </tns:user>
```

5. Reimport the user data from the modified XML files to the Import users page on the web console.

   You can navigate to the Import users page from **Services** > **Bulk Import and Export** > **Import** > **User Management** > **Users** on the web console. For more information, see Bulk importing of users.

   Note:

   The system might display an error message when you reimport the modified user data for admin user because the XML file includes the admin user when you export the user data. Ignore the message because you cannot edit the data for the admin user.

6. To create a user profile, synchronize profile in User Management for CS 1000 or CallPilot elements that are being imported. For information on profile synchronization, see Synchronizing CS 1000 and CallPilot profiles.

   Note:

   For synchronizing the CallPilot profile, you might have to reimport the `ca.cer` file to the **Services** > **Inventory** > **Manage Elements** page of System Manager 6.2 instead of the **UCM** > **Security** > **Certificates** page of System Manager 6.1.

Related links

Bulk importing of users
Exporting users in bulk from web console on page 328

Importing users from CS 1000 Subscriber Manager to User Management

CS 1000 Subscriber Manager data import options

If CS 1000 Release 7.x is available while installing System Manager 6.2 or later, you can import the CS 1000 Release 7.x Subscriber Manager user data into System Manager User Management.

Use one of the following options to import the CS 1000 Subscriber Manager data:

- Using the active primary CS 1000 Subscriber Manager server to LDAP syncnchronize the Subscriber Manager data.
- Using the CND or LDAP Data Interchange Format (LDIF) output to capture the CS 1000 Subscriber Manager data.

Preparing the CS 1000 Subscriber Manager user data for import to System Manager

This option uses the active primary CS 1000 Subscriber Manager server for System Manager User Management to perform an LDAP synchronization of the user data.

Procedure

1. Log in to the primary CS 1000 UCM server command line using one of the following user names:
   - For CS 1000 Release 7.5 systems, admin2
   - For CS 1000 Release 7.0 and later systems, nortel
2. On the CS 1000 Release 7.x UCM server, perform the steps outlined in Preparing the Subscriber Manager user data for import to User Management.

Related links

Preparing the Subscriber Manager user data for import to User Management on page 555

Importing the CS 1000 Subscriber Manager user data to System Manager

Before you begin

- Prepare the CS 1000 Subscriber Manager user data for import to System Manager.
- Ensure that the firewall is stopped on the CS 1000 Release 7.x server to gain access to System Manager UPM LDAP.

Procedure

1. Log on to the Web console of System Manager Release 6.2 or later.
2. Perform the LDAP synchronization as outlined in Importing the Subscriber Manager user data to User Management.

   For the directory parameters that you must use, see Subscriber Manager datasource parameters and attributes.

Related links

Importing the Subscriber Manager user data to User Management on page 557
Subscriber Manager datasource parameters and attributes on page 558

Exporting the CS 1000 user data and creating the user profile

To complete the import job of user data from CS 1000 Subscriber Manager:

Procedure

Perform the same procedure as System Manager Release 6.1 Exporting the user data and creating the user profile.

Related links

Exporting the user data and creating the user profile on page 559

Preparing the CS 1000 Subscriber Manager user data for import to System Manager

This method uses the CND or LDIF output to capture the CS 1000 Subscriber Manager user data that you later import to User Management in System Manager.

Perform this procedure on System Manager Release 6.2 or later.

Procedure

1. Log in to the primary CS 1000 UCM server command line using one of the following user names:
   - For CS 1000 Release 7.5 systems, admin2
   - For CS 1000 Release 7.0 and later systems, nortel
2. On the CS 1000 Release 7.x UCM server, perform the steps outlined in Preparing the Subscriber Manager user data for import to User Management in System Manager.
3. Change to super user su - root.
4. Type `cd /opt/nortel/cnd`.
5. Type `./cnd.sh stop_service`.

6. Type `./slapcat -f slapd.conf -s ou=subscribers,dc=nortel,dc=com -a objectclass=nortelsubscriber -l subscriberData.ldif`.
7. Type `./cnd.sh start_service`.
8. Using a secure ftp client, connect to the CS 1000 UCM Linux system using the same credentials you used in Step 1.
9. Copy the `/opt/nortel/cnd/subscriberData.ldif` file to your computer.

Related links

Preparing the Subscriber Manager user data for import to User Management on page 555

Importing the CS 1000 UCM Subscriber Manager user data to System Manager

Before you begin

Prepare the CS 1000 Release 7.x Subscriber Manager user data for import to System Manager User Management.

Procedure

1. Using a secure ftp client, connect to the System Manager server using admin.
2. Copy the `subscriberData.ldif` file to the `/home/admin` directory on System Manager.
3. Log on to System Manager server using the command line interface.
4. Change to the super user su - root.
5. Type `cd /opt/nortel/cnd`.
6. Type `mv /home/admin/subscriberData.ldif`.
7. Type `./cnd.sh stop_service`.
8. Type `./slapadd -f slapd.conf -l subscriberData.ldif -c`.
9. Type `./cnd.sh start_service`.
10. Perform the LDAP synchronization procedure as outlined in Importing the Subscriber Manager user data to System Manager.

    Note:

    Ensure that the **Host** field in the **Directory Parameter** area displays localhost.

Related links

Importing the Subscriber Manager user data to User Management on page 557
Subscriber Manager datasource parameters and attributes on page 558

Exporting the CS 1000 user data and creating the user profile

To complete the import job of user data from CS 1000 Subscriber Manager:

Procedure

Perform the same procedure as System Manager Release 6.1 Exporting the user data and creating the user profile.

Related links

Exporting the user data and creating the user profile on page 559

Managing messaging

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

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. Click **Class Of Service** in the left navigation pane.
3. Choose one or more messaging systems from the Messaging Systems list.
4. Click **Show List**.
5. Click the respective column heading to sort the Class Of Service by **Name** in alphabetical order or by **Class No.** in numeric order.

   This is a read-only list.

Class of Service List field descriptions

Name	Description
Class No	The number of each class of service.
Name	The name of the class of service.
Last Modified	The time and date when the class of service was last modified.
Messaging System	The type of messaging system.

Messaging

Subscriber Management

With System Manager, you can perform messaging system administration activities, such as add, view, edit, and delete subscribers. You can also administer mailboxes, and modify mailbox settings for a messaging system.

System Manager supports:

- Communication Manager 5.0 and later
- Avaya Aura® Messaging 6.0 and later
- Avaya Modular Messaging 5.0 and later
- Communication Manager Messaging 5.2 and later with patch and LDAP support

Adding a subscriber

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select one or more messaging systems from the list of Messaging Systems.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Basic Information**, **Subscriber Directory**, **Mailbox Features**, **Secondary Extensions**, and **Miscellaneous** sections.
7. Complete the **Add Subscriber** page and click **Commit** to add the subscriber.

   Note:

   If you select more than one Messaging, 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 Messaging, Modular Messaging, or Communication Manager Messaging in context.

Related links

Subscribers (Avaya Aura Messaging) field descriptions on page 569
Subscribers (MM) field descriptions on page 577
Subscribers (Communication Manager Messaging) field descriptions on page 574

Editing a subscriber

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. From the Subscriber List, choose the subscriber you want to edit.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields in the **Edit Subscriber** page.
8. Click **Commit** to save the changes.

Related links

Subscribers (Avaya Aura Messaging) field descriptions on page 569
Subscribers (MM) field descriptions on page 577
Subscribers (Communication Manager Messaging) field descriptions on page 574

Viewing a subscriber

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. Select the subscriber you want to view from the Subscriber List.
6. Click **View**.

   Note:

   You cannot edit any field on the View Subscriber page.

Related links

Subscribers (Avaya Aura Messaging) field descriptions on page 569
Subscribers (MM) field descriptions on page 577

Subscribers (Communication Manager Messaging) field descriptions on page 574

Deleting a subscriber

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. Select the subscriber you want to delete from the Subscriber List.
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

The subscriber list displays all subscribers in a messaging version, such as Messaging, Communication Manager Messaging, or Modular Messaging. You can apply filter to each column in the subscriber list. You can also sort subscribers according to each of the column in the subscriber list. You must refresh the page to view the information that is updated after the last synchronization.

Name	Description
Name	The name of the subscriber.
Mailbox Number	The mailbox number of the subscriber.
Email Handle	The email handle of the subscriber.
Telephone Number	The telephone number of the mailbox.
Last Modified	The time and date when the subscriber details were last modified.
User	The name of the user to which the subscriber is associated.
System	The messaging system of the subscriber.

Filtering subscribers

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.

4. Click **Show List**.
5. Click the **Filter: Enable** option in the Subscriber List.
6. Filter the subscribers 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 subscribers that match the filter criteria.

Subscribers (Avaya Aura® Messaging) field descriptions

Name	Description
System	The name of the messaging system.
Template	The messaging template of a subscriber template.
Last Name	The last name of the subscriber.
First Name	The first name of the subscriber.
Mailbox Number	The full mailbox number of a subscriber, including the site group and site identifiers, and the short mailbox number. Subscribers use mailbox numbers to log on to their respective mailbox. For a PBX subscriber, the mailbox number ranges from 3 to 10 digits in length. Other local subscribers use this field to address messages to the PBX subscriber. For a Multisite system subscriber, the mailbox number is up to 50 digits in length. Ensure that the mailbox number is: • Within the range of mailbox numbers assigned to your system. • Unassigned to another local subscriber. • A valid length on the local computer. This is a mandatory field on the Add Subscriber pages for all types of messaging systems.
Password	The default password the subscriber must use to log in to the mailbox. The password can be from 3 to 15 digits and adhere to system policies set on the Avaya Aura® Messaging server
Save as Template	Saves your current settings as a template.

Basic Information

Name	Description
Class Of Service Name	The name of the class of service (CoS) for this subscriber. CoS controls subscriber access to many features and provides general settings, such as mailbox size. The value that you select must be available in the messaging system.
Community ID	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.
Numeric Address	The unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
Time zone	The time zone for Avaya Aura® Messaging time subscribers. The value must be in the standardized name format, America/Phoenix. Otherwise, the system sets the Avaya Aura® Messaging subscriber time zone to the System Manager server time zone.
PBX Extension	The primary telephone extension of the subscriber. For a Multisite system subscriber, this number is up to 50 digits in length.
Site	The name of the site. Avaya Aura® Messaging includes a site named **Default**. Change the default name when you set site properties for the first time.

Subscriber Directory

Field	Description
Email Handle	The name that the system displays before the computer name and domain in the subscriber's email address.
Telephone Number	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 (]).
Common Name	The display name of the subscriber in address book listings, such as those for email client applications. The name can be 1 to 64 characters in length. This

Table continues…

Field	Description
	field is automatically populated when you add a new subscriber.
ASCII version of name	If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.
Pronounceable Name	The pronounceable name of the user. The name of a user, info mailbox, or distribution list might not follow the pronunciation rules of the primary language for your system. To increase the likelihood of the Speech Recognition feature recognizing the name, spell the name as you would pronounce the name. For example, if the primary language of your system is English, spell Dan DuBois as Dan Doobwah. You can enter an alternative name for the user. For example, William Bell might also be known as Bill Bell. If you enter William in the First name field, Bell in the Last name field, and Bill Bell in the Pronounceable name field, the speech engine recognizes both William Bell and Bill Bell.
Include in Auto Attendant directory	The option to add the messaging system to the auto attendant directory.

Subscriber Security

Name	Description
Expire Password	An option to set the password expiry. The options are: • **yes**: for password to expire • **no**: if you do not want your password to expire
Is Mailbox Locked?	The option to lock your mailbox. A subscriber mailbox can get locked after two unsuccessful login attempts. The options are: • **no**: To unlock your mailbox • **yes**: To lock your mailbox and prevent access to it

Mailbox Features

Name	Description
Personal Operator Mailbox	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

Table continues…

Name	Description
	subscriber presses 0 while listening to the subscriber greeting.
Personal Operator Schedule	The option to specify when to route calls to the backup operator mailbox. The default value is **Always Active**.
TUI Message Order	The order in which the subscriber hears the voice messages. The options are: • **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.
Intercom Paging	The intercom paging settings for a subscriber. The options are: • **paging is off**: Disables intercom paging for this subscriber. • **paging is manual**: Callers can page the subscriber with Subscriber Options or TUI if the subscriber can modify. • **paging is automatic**: Callers automatically page the subscriber with TUI.
VoiceMail Enabled	The option to specify if a subscriber can receive messages, email messages, and call-answer messages from other subscribers. The options are: • **yes**: 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 TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.

Table continues…

Name	Description
MWI enabled	The option to enable the message waiting indicator (MWI) light feature. The options are: • **No**: The user has a voice mailbox only. • **ByCOS**: CoS controls how the system enables MWI. The **MWI enabled** field overrides the MWI setting defined by the CoS to which the user is associated.

Secondary Extensions

Field	Description
Secondary Extension	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. For Avaya Aura® Messaging 6.3, you can add a maximum eight secondary extensions.

Miscellaneous

Field	Description
Miscellaneous 1	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous 2	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous 3	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous 4	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Saves all the changes.
Edit	Allows you to edit the fields.

Table continues…

Button	Description
Reset or **Clear**	Clears all changes.
Cancel	Returns to the previous page.

Subscribers (Communication Manager Messaging) field descriptions

Name	Description
System	The messaging system of the subscriber that you want to add.
Template	The template for this subscriber.
Last Name	The last name of the subscriber.
First Name	The first name of the subscriber.
Mailbox Number	The full mailbox number of a subscriber, including the site group and site identifiers and the short mailbox number. Subscribers use mailbox numbers to log on to their respective mailbox. For a PBX subscriber, the mailbox number ranges from 3 to 10 digits in length. Other local subscribers use this field to address messages to the PBX subscriber. For a Multisite system subscriber, the mailbox number is up to 50 digits in length. Ensure the mailbox number is: • Within the range of mailbox numbers assigned to your system. • Unassigned to another local subscriber. • A valid length on the local computer. A mandatory field on the Add Subscriber pages for all types of messaging systems.
Password	The default password to log in to the mailbox. The password can be from 1 to 15 digits in length.

Basic Information

Name	Description
Extension	The extension number between 3 to 10 digits that the subscriber uses to log in to the mailbox. Other local subscribers can use the mailbox number to address messages to this subscriber. Ensure that the mailbox number is: • Within the range of mailbox numbers assigned to your system. • Unassigned to another local subscriber.

Table continues…

Name	Description
	• A valid length on the local computer.
Class Of Service ID	The class of service (CoS) ID for this subscriber. CoS controls subscriber access to many features and provides general settings, such as mailbox size. The value that you select must be available in the messaging system.
Community ID	The default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default is 1.
MWI Enabled	The option to set the message waiting indicator (MWI) for the subscriber. The options are: • **No**: If the system must not send MWI to the subscriber or if the subscriber does not have a phone or switch on the network. • **Yes**: If the system must send MWI to the subscriber.
Account Code	The subscriber account code. The account code is used to create Call Detail Records on the switch for calls placed by the voice ports. The account code can contain a combination of digits from 0 to 9. If an account code is not specified, the system uses the mailbox extension of the subscriber as the account code.

Subscriber Directory

Name	Description
Email Handle	The name that the system displays before the computer name and domain in the subscriber email address.
Common Name	The display name of the subscriber.

Subscriber Security

Name	Description
Expire Password	An option to set the password expiry. The options are: • **yes**: for password to expire • **no**: if you do not want your password to expire

Table continues…

Name	Description
Is Mailbox Locked?	The option to lock your mailbox. A subscriber mailbox can get locked after two unsuccessful login attempts. The options are: • **no**: To unlock your mailbox • **yes**: To lock your mailbox and prevent access to it

Mailbox Features

Name	Description
Covering Extension	The default destination for the Transfer Out of Messaging feature. You can enter from 3 to 10 digits depending on the length of the system extension. You can leave this field blank.

Secondary Extensions

Name	Description
Secondary extension	The number assigned to a subscriber for receiving fax messages. You can enter from 3-10 digits, depending on the length of the extension of the system or leave the field blank.

Miscellaneous

Name	Description
Misc 1	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber to the messaging system.

Table continues…

Button	Description
Schedule	Adds the subscriber at the specified time.
Save as Template	Saves the settings as a template.
Reset	Clears all the changes.
Edit	Allows you to edit the fields.
Done	Completes your action and takes you to the previous page.
Cancel	Returns to the previous page.

Subscribers (MM) field descriptions

Field	Description
System	The messaging system of the subscriber you want to add. You can choose this option from the drop-down box.
Template	The messaging template of a subscriber. You can choose an option from the drop-down box.
Last Name	The last name of the subscriber.
First Name	The first name of the subscriber.
Mailbox Number	The full mailbox number of a subscriber, including the site group and site identifiers and the short mailbox number. Subscribers use mailbox numbers to log on to their respective mailbox. For a PBX subscriber, the mailbox number ranges from 3 to 10 digits. Other local subscribers use this field to address messages to the PBX subscriber. For a Multisite system subscriber, the mailbox number is up to 50 digits in length. Ensure the mailbox number is: • Within the range of mailbox numbers assigned to your system. • Unassigned to another local subscriber. • A valid length on the local computer. This is a mandatory field on the Add Subscriber pages for all types of messaging systems.
Password	The default password to log in to the mailbox. The password can contain 1 to 15 digits.
Save as Template	Saves your current settings as a template.

Basic Information

Name	Description
Class Of Service	The class of service for this subscriber. COS controls subscriber access to many features and provides general settings, such as mailbox size.
Community ID	The default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default is 1.
Numeric Address	A unique address in the voice mail network. The address can contain 1 to 50 digits and can contain the mailbox number.
PBX Extension	The primary telephone extension of the subscriber. For a Multisite system subscriber, the number is up to 50 digits in length.

Subscriber Directory

Field	Description
Email Handle	The name that the system displays before the computer name and domain in the subscriber's email address. The system adds the computer name and domain to the handle that you enter when the subscriber sends or receives an email.
Telephone Number	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 (]).
Common Name	The display name of the subscriber in address book listings, such as the names for email client applications. The name you enter can be 1 to 64 characters in length. The system automatically populates the name when you add a new subscriber.
ASCII Version of Name	The ASCII translation of the subscriber name if the subscriber name is entered in a multi-byte character format.

Subscriber Security

Name	Description
Expire Password	An option to set the password expiry. The options are: • **yes**: for password to expire • **no**: if you do not want your password to expire
Is Mailbox Locked?	The option to lock your mailbox. A subscriber mailbox can get locked after two unsuccessful login attempts. The options are: • **no**: To unlock your mailbox • **yes**: To lock your mailbox and prevent access to it

Mailbox Features

Name	Description
Personal Operator Mailbox	The mailbox number or transfer dial string of the subscriber's personal operator or assistant. The field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting.
Personal Operator Schedule	The option to specify when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
Voicemail Enabled	The option to specify whether a subscriber can receive messages, email messages, and call-answer messages from other subscribers. The options are: • **yes**: use this 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 TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.
Intercom Paging	The intercom paging settings for a subscriber. The options are: • **paging is off**: Disables intercom paging for this subscriber. • **paging is manual**: Callers can page the subscriber with Subscriber Options or TUI if the subscriber can modify. • **paging is automatic**: Callers automatically page the subscriber with TUI.

TUI Message Order

Field	Description
TUI New Message Order	The order in which the subscriber hears the new voice messages. The options are: • **urgent first then newest**: 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 play messages in the order they were received. • **urgent first then oldest**: 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 play messages in the reverse order of how they were received.
TUI Saved Message Order	The order in which the subscriber hears the saved voice messages. The options are: • **urgent first then newest**: 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 play messages in the order they were received. • **urgent first then oldest**: 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 play messages in the reverse order of how they were received.
TUI Deleted Message Order	The order in which the subscriber hears the deleted voice messages. The options are: • **urgent first then newest**: 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 play messages in the order they were received.

Table continues…

Field	Description
	• **urgent first then oldest**: 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 play messages in the reverse order of how they were received.
TUI Admin Message Order	The order in which the administrator hears the voice messages. The options are: • **urgent first then newest**: 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 play messages in the order they were received. • **urgent first then oldest**: 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 play messages in the reverse order of how they were received.

Secondary Extensions

Name	Description
Secondary extension	One or more alternate numbers 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

Name	Description
Misc 1	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.
Misc 2	Useful information about a subscriber template. The messaging system does not use this information.

Table continues…

Name	Description
	Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system.

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

Chapter 10: Managing Communication Manager

System Manager Communication Manager capabilities

System Manager provides a common, central administration of some IP Telephony products. This helps you to consolidate the 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, Modular Messaging, Avaya Aura® Messaging. Some features of System Manager include:

- Endpoint management
- Template management
- Mailbox management
- Inventory management
- Element cut through to native administration screens

Managing Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Communication Manager**. From System Manager, you can add, edit, view, or delete the objects through **Communication Manager**.

Endpoint management

Using endpoint management, you can create and manage endpoint objects, and add, change, remove, and view the endpoint data.

Templates

Using Templates, you can specify specific parameters of an endpoint or a subscriber once and then reuse the template for subsequent add endpoint or subscriber tasks. You can use default templates or 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 at any time.

Subscriber management

Using Subscriber Management, you can manage, add, change, remove, and view subscriber data. Subscriber management supports Avaya Aura® Messaging, Communication Manager Messaging, and Messaging objects.

With 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 user profiles with the required endpoints and subscribers.

Configuring Communication Manager user profile settings

Some Communication Manager capabilities depend on the license file available with the customers. For a successful functioning of Communication Manager capabilities, ensure that the following settings are in place:

Procedure

1. Log in to Communication Manager SAT as a customer super-user.
2. Execute the `display system-parameters customer-options` command.
3. On Page 5, ensure that **Station and Trunk MSP?** is set to **y**.
4. Execute the `duplicate user-profile`*18* command.
5. On Page 1, perform the following:
   a. Enter a new profile number. The profile number can range from `20` to `69`.
   b. Set **Shell Access** to `y`.
6. On Page 31, set **station M** to **wm**.
7. Save the user profile settings.
8. Exit Communication Manager SAT.
9. Open Communication Manager shell and perform the following to create a new user and assign password to the new user:
   a. To create a new user, use the `cmuseradd` <*type*> [`-C` *profile*] <*login name*> command

      where,

      - <*type*> is the super-user.
      - *profile* is the profile number created in Step 5.
      - <*login name*> is the user login name.

      For example, `cmuseradd super-user -C 20 iptuser`.

   b. To assign password to the new user, use the command `cmpasswd` <*login name*>

      where, <*login name*> is the login name in step 9a. For example, `cmpasswd iptuser`.

Note:

You can also execute Step 9 from the **Administrator Accounts** Web page in Communication Manager SMI. The navigation path for **Administrator Accounts** Web page in Communication Manager SMI is **Administration** > **Server Maintenance** > **Security** > **Administrator Accounts**.

Editing the Select All attribute in a table

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. Click **Settings** > **Communication System Management** > **Configuration**.
3. On the View Profile: Configuration page, edit the value of the **Select All** attribute.

   This setting affects all the tables in the user interface.

   The default value for the **Select All** attribute is 1000. You can increase this value up to 5000.

Search component for Communication Manager objects

System Manager supports data and link search for certain Communication Manager objects. Use the search bar on the Communication Manager objects list page for the following Communication Manager objects:

- Endpoints
- Agents
- Vector Directory Number (VDN)
- Vector
- Vector Routing Table (VRT)
- Announcement
- Audio Group
- Hunt Group
- Off PBX Endpoint Mapping
- Data Module
- Communication System
- Trunk Group
- Signaling Groups

Link based search: When you hover your mouse on the search bar, the system lists the Communication Manager objects that support search. Click a Communication Manager object to go to the relevant page directly. For example, if you click Hunt Group from the search bar, you can directly view the Hunt Group page.

Data search: Free text search and specific search are both supported in the search feature. If you type `Endpoints 100`, the system displays the endpoint with the extension 100. When you hover your mouse on this extension, a prop up window appears by the side. From this window, you can view certain details of the endpoint and directly go to the view, edit, and delete pages for the endpoint.

If you type the name of a Communication Manager object followed by space, the system lists all the searchable fields for the particular CM object. You can click a particular field and use the search option for that field.

The following table lists the fields that are searchable for the supported Communication Manager objects:

Communication Manager object	Searchable fields	Supported Actions
Endpoint	Name, Extension, Port, Set Type, TN, Location, IP soft phone, COS, COR, User, Communication Manager name, Emergency Location Extension, Message Lamp Extension	View, Edit, Delete
Agent	Extension, Name, AAS, Call Handling Preference, COR, User, Coverage Path, CM NamCommunication Manager name	View, Edit, Delete
VDN	Extension, Name, Destination, Allow VDN Override, Attendant, Vectoring, Meet-me Conferencing, COR, TN, Communication Manager name	View, Edit, Delete
Vector	Number, Name, Multimedia Attendant, Vectoring, Meet-me Conf, Communication Manager name	View, Edit
VRT	Number, Name, Sort, Communication Manager name	View, Edit, Delete
Announcement	Name, Extension, Group/Board, Type, Protected, Rate, COR, TN, Queue Size, Communication Manager name	View, Edit, Delete
Audio Group	Group Number, Group Name, Communication Manager name	View, Edit, Delete
Hunt Group	Group Number, Group Name, Group Extension, Group Type, Communication Manager name	View, Edit, Delete

Note:

You must have at least View permission for a Communication Manager object to use the search component for that Communication Manager object.

When you search a Communication Manager object, the system also displays the search results for other Communication Manager objects which support the search feature.

Managing Communication Manager objects

Communication Manager objects

Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Communication Manager**. Through **Communication Manager** you can directly add, edit, view, or delete the Communication Manager objects.

Note:

To manage the Communication Manager objects not identified here, access the Communication Manager Element Cut-Through which provides an enhanced System Access Terminal (SAT) interface. To launch Element Cut-Through, click **Inventory** > **Synhronization** > **Communication System**.

The Communication Manager objects you can administer through System Manager are:

Group	Communication Manager objects
Call Center	Agents Announcements Audio Group Best Service Routing Holiday Tables Variables Vector Vector Directory Number Vector Routing Table Service Hours Tables
Coverage	Coverage Answer Group Coverage Path Coverage Remote Coverage Time of Day

Table continues…

Endpoints	Alias Endpoint Intra Switch CDR Manage Endpoints Off PBX Endpoint Mapping Site Data Xmobile Configuration
Groups	Group Page Hunt Group Intercom Group Pickup Group Terminating Extension Group
Network	Automatic Alternate Routing Analysis Automatic Alternate Routing Digit Conversion Automatic Route Selection Analysis Automatic Route Selection Digit Conversion Automatic Route Selection Toll Data Modules IP Interfaces IP Network Regions IP Network Maps Node Names Route Pattern Signaling Groups Trunk Group
Parameters	System Parameters - CDR Options System Parameters - Customer Options System Parameters - Features System Parameters - Security System Parameters - Special Applications
System	Abbreviated Dialing Enhanced Abbreviated Dialing Group Abbreviated Dialing Personal Authorization Code Class of Restriction

Table continues…

	Class of Service Class of Service Group Dialplan Analysis Dialplan Parameters Feature Access Codes Locations Uniform Dial Plan Uniform Dial Plan Group Tenant

Note:

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

Related links

Adding Communication Manager objects on page 589
Editing Communication Manager objects on page 590
Viewing Communication Manager objects on page 590
Deleting Communication Manager objects on page 590
Filtering Communication Manager objects on page 591

Adding Communication Manager objects

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object.
3. Select a Communication Manager instance from the Communication Manager list.
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

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object.
3. Select a Communication Manager instance 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

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object.
3. Select a Communication Manager instance from the Communication Manager list.
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

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the objects you want to delete from this group.
6. Click **Delete**.
7. Confirm to delete the Communication Manager objects.

Filtering Communication Manager objects

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object.
3. Select a Communication Manager instance 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.

Changing to classic view

The System Manager Web interface of Communication Manager objects support two types of views: classic and enhanced. Enhanced view is the default setting, where you can execute tasks on the Web interface. In the classic view, the system directs you to Element Cut Through screen for executing the tasks.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object you want to manage.
3. By default, the system displays the Web page for the Communication Manager object in enhanced view. To change to classic view, click the **Switch to Classic View** link on the upper-right of the interface.
4. To return to the default view, click the **Switch to Enhanced View** link.

Agents

Agents

Use the Agents capability to manage agent login IDs and skill assignments in an Expert Agent Selection (EAS) environment. If skills are added or changed, agents must log out and then log in again before the changes are effective.

Agents List

Agents List displays all the agents under the Communication Manager you select. You can perform an advanced search on this list using the search criteria. You can also apply filters and sort each column in the Agents List.

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

Name	Description
LoginID	The identifier for the Logical Agent as entered in the command line.
Agent Name	The 27-character string name of the agent. Any alphanumeric character is valid. Default is blank.
Direct Agent Skill	The number of the skill used to handle Direct Agent calls.
Call Handling Preference	The call that an agent receives the next when calls are in queue.
COR	The Class of Restriction associated with the agent.
System	The name of the Communication Manager associated with the agents.

Adding an agent

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the New Agent page and click **Commit**.

Related links

Agents field descriptions on page 595

Viewing agent data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Agents List, select the agent whose data you want to view.

6. Click **View**.

Related links

[Agents field descriptions](#) on page 595

Editing agent data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Agents List, select the agent whose properties you want to edit.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields on the **Edit Agent** page.
8. Click **Commit** to save the changes.

Related links

[Agents field descriptions](#) on page 595

Deleting agents

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Agents List, select the agents you want to delete.
6. Click **Delete**.
7. Confirm to delete the agents.

Related links

[Agents field descriptions](#) on page 595

Adding agents in bulk

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.

5. Click **More Actions** > **Bulk Add Agents**.
6. Complete the **Bulk Add Agents** page and click **Now**.

   The **Agent Name Prefix** field displays the common prefix which appears for all the agents you bulk add. You can enter any prefix name of your choice in this field.

   Note:

   With Multi Tenancy, when you add the agents, the **Tenant Number** field is auto populated according to the Site you select.

   Fields like **COR** are validated with the tenant permissions when you add the agents.

Related links

Agents field descriptions on page 595

Editing agent data in bulk

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Bulk Edit Agents**.
6. Complete the **Bulk Edit Agents** page and click **Now**.

   The **Agent Name Prefix** field displays the common prefix which appears for all the agents you bulk add. You can enter any prefix name of your choice in this field.

Related links

Agents field descriptions on page 595

Deleting agents in bulk

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Agents**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Bulk Delete Agents**.
6. Perform one of the following actions:
   - Select the agents you want to delete in bulk from the **Current Agent Extensions** field.
   - Type the agent extensions you want to bulk delete in the **Enter Extensions** field.
7. Click **Continue**.

8. On the Bulk Delete Agents Confirmation page, click **Now**.

   Click **Schedule** to schedule the bulk delete job at a later time.

   Note:

   You cannot delete agent associated extensions.

Agents field descriptions

Field	Description
System	The Communication Manager system in which you have added the agent.
Login ID	The identifier for the Logical Agent as entered in the command line. This is a display-only field.
Template	The agent template.
Agent Name	The 27-character string name of the agent. Any alphanumeric character is valid. By default, this field is blank.
Attribute	The agent attribute.
AAS	The option to use this extension as a port for an Auto Available Split/Skill. By default, this check box is clear. This option is intended for communication server adjunct equipment ports only, not human agents. **Important:** When you enter `y` in the AAS field, it clears the password and requires execution of the **`remove agent-loginid`** command. To set AAS to `n`, remove this logical agent, and add it again.
ACW Agent Considered Idle	The option to count After Call Work (ACW) as idle time. The valid entries are **System**, **Yes**, and **No**. Select **Yes** to include ACW agents in the Most-Idle Agent queue. Select **No** to exclude ACW agents from the queue.
AUDIX	The option to use this extension as a port for AUDIX. By default, this check box is clear. **Note:** Both AAS and AUDIX fields cannot be `y`.
AUDIX Name for Messaging	The name of the AUDIX Messaging System. The options are: • The messaging system used for LWC Reception.

Table continues…

Field	Description
	• The messaging system that provides coverage for this Agent LoginID. • Blank, the default value.
Auto Answer	When using EAS, the auto answer setting of the agent applies to the endpoint where the agent logs in. If the auto answer setting for that endpoint is different, the agent setting overrides the endpoint setting. One of the following is a valid entry: • **All**. Immediately sends all ACD and non-ACD calls to the agent. The endpoint is also given a single ring while a non-ACD call is connected. You can use the ringer-off button to prevent the ring when the feature-related system parameter, **Allow Ringer-off with Auto-Answer**, is set to `y`. • **acd**. Only ACD split /skill calls and direct agent calls go to auto answer. If this field is set to **acd**, non-ACD calls terminated to the agent ring audibly. • **none**. All calls terminated to this agent receive an audible ringing. This is the default setting. • **station**. Auto answer for the agent is controlled by the auto answer field on the Endpoint screen.
Aux Work Reason Code Type	Determines how agents enter reason codes when entering AUX work. One of the following is a valid entry: • **system**. Settings assigned on the Feature Related System Parameters screen apply. This is the default setting. • **none**. You do not want an agent to enter a reason code when entering AUX work. • **requested**. You want an agent to enter a reason code when entering AUX mode but do not want to force the agent to do so. To enter this value, the reason codes and EAS on the System-Parameters Customer-Options screen must be set to `y`. • **forced**. You want to force an agent to enter a reason code when entering AUX mode. To enter this value, the Reason Codes and EAS on the System-Parameters Customer-Options screen must be set to `y`.
Call Handling Preference	Determines which call an agent receives next when calls are in queue. When calls are in queue and an

Table continues…

Field	Description
	agent becomes available, any of the following entries is valid: • **skill-level**. Delivers the oldest, highest priority calls waiting for the highest-level agent skill. • **greatest-need**. Delivers the oldest, highest priority calls waiting for any agent skill. • **percent-allocation**. Delivers a call from the skill that will otherwise deviate most from its administered allocation. Percent-allocation is available only with Avaya Business Advocate software. For more information, see *Avaya Business Advocate User Guide*.
COR	The Class Of Restriction (COR) for the agent. Valid entries range from **0** to **995**. The default entry is **1**.
Coverage Path	The coverage path number used by calls to the LoginID. A valid entry is a path number from **1** to **999**, time of day table **t1** to **t999**, or blank by default. Coverage path is used when the agent is logged out, busy, or does not answer calls.
Direct Agent Calls First (not shown)	The option to direct agent calls to override the percent-allocation call selection method and be delivered before other ACD calls. Clear the check box if you want to treat direct agent calls as other ACD calls. This field replaces the Service Objective field when percent-allocation is entered in the Call Handling Preference field. For more information, see *Avaya Business Advocate User Guide*.
Direct Agent Skill	The number of the skill used to handle Direct Agent calls. A valid entry can range from **1** to **2000**, or blank. The default setting is blank.
Forced Agent Logout Time	Enables the Forced Agent Logout by Clock Time feature by administering a time of day to automatically log out agents using an hour and minute field. A valid entry for the hour field ranges from **01** to **23**. A valid entry for the minute field is **00**, **15**, **30**, or **45**. The default is blank (not administered). Examples are: 15:00, 18:15, 20:30, 23:45.
Local Call Preference	The option to administer Local Preference Distribution to handle agent-surplus conditions, call-surplus conditions, or both. Use this field to administer call-surplus conditions. To set up an algorithm for agent-surplus conditions, set the Local Agent Preference field on the Hunt Group screen.

Table continues…

Field	Description
	You can select this check box only if the Call Center Release field is set to 3.0 or later and the Multiple Locations customer option is active.
LoginID for ISDN/SIP Display	Use to include the **Agent LoginID CPN and Name** field in ISDN and SIP messaging over network facilities. By default, the check box is clear, indicating that the physical endpoint extension CPN and Name is sent. If you set the **Send Name** to n or r (restricted) on the ISDN Trunk Group screen, the calling party name and number is sent.
Logout Reason Code Type	Determines how agents enter reason codes. One of the following is a valid entry: • **System**. Settings assigned on the Feature Related System Parameters screen apply. This is the default entry. • **Requested**. You want an agent to enter a reason code when logging out but do not want to force the agent to do this. To enter this value, the reason codes and EAS on the System-Parameters Customer-Options screen must be set to `y`. • **Forced**. You want to force an agent to enter a reason code when logging out. To enter this value, the Reason Codes and EAS on the System-Parameters Customer-Options screen must be set to `y`. • **None**. You do not want an agent to enter a reason code when logging out.
LWC Reception	Indicates whether the terminal can receive Leave Word Calling (LWC) messages. One of the following is a valid entry: • **audix** • **msa-spe**. This is the default entry. • **none**
Maximum time agent in ACW before logout (Sec)	Sets the maximum time the agent can be in ACW on a per agent basis. One of the following is a valid entry: • **system**. This is the default entry. Settings assigned on the Feature Related System Parameters screen apply. • **none**. ACW timeout does not apply to this agent.

Table continues…

Field	Description
	• **30-9999 sec**. Indicates a specific timeout period. This setting will take precedence over the system setting for maximum time in ACW.
Percent Allocation	The percentage for each of the agent skills if the call handling preference is percent-allocation. a valid entry is a number from **1** to **100** for each skill. Entries for all the agent skills together must add up to 100%. Do not use target allocations for reserve skills. Percent Allocation is available as part of the Avaya Business Advocate software.
Password	The password the agent must enter upon login. Displayed only if both the AAS and AUDIX check boxes are clear. A valid entry is a digit ranging from **0** through **9**. Enter the minimum number of digits in this field specified by the Minimum Agent-LoginID Password Length field on the Feature-Related System Parameters screen. By default, this field is blank.
Confirm Password	Confirms the password the agent entered in the Password field during login. Displayed only if both the AAS and the AUDIX check boxes are clear. By default, this field is blank. **Note:** Values entered in this field are not populated to the screen.
Port Extension	The assigned extension for the AAS or AUDIX port. The values are displayed only if either the AAS or AUDIX check box is selected. This extension cannot be a VDN or an Agent LoginID. By default, this field is blank.
Reserve Level	The reserve level to be assigned to the agent for the skill with the Business Advocate Service Level Supervisor feature or the type of interruption with the Interruptible AUX Work feature. You can assign a reserve level of `1` or `2` or an interruptible level of `a`, `m`, `n`, or blank for no reserve or interruptible level, where, • `a` is auto-in-interrupt • `m` is manual-in-interrupt • `n` is notify-interrupt Changes to this field take effect the next time the agent logs in. Values of 1 and 2 are allowed only if Business Advocate is enabled. A skill level cannot be

Table continues…

Field	Description
	assigned with a reserve level setting. Reserve level set to `1` or `2` defines the EWT threshold level for the agent to be added to the assigned skill as a reserve agent. When the EWT for this skill reaches the corresponding threshold set on the Hunt Group screen, this skill gets this skill gets automatically added to the logged in skills of the agents. Agents are delivered calls from this skill until the skill EWT drops below the assigned overload threshold. Use the Interruptible Aux functionality to help meet service level targets by requesting agents who are on break to become available when the service level target is not being met. For more information on Service Level Supervisor, see *Avaya Business Advocate User Guide*.
Service Objective	The option to administer Service Objective. Service Objective is administered on the Hunt Group screen and the agent LoginID screen. This field is displayed only when Call Handling Preference is set to greatest-need or skill-level. The communication 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 part of the Avaya Business Advocate software.
Skill Number	The Skill Hunt Groups that an agent handles. The same skill cannot be entered twice. You have the following options: • If EAS-PHD is not optioned, enter up to four skills. • If EAS-PHD is optioned, enter up to 20 or 60 skills depending on the platform. **Important:** Assigning a large number of skills to agents can potentially impact system performance. Review system designs with the ATAC when a significant number of agents have more than 20 skills per agent.
Skill Level	A skill level for each of an agent assigned skills. If you specify the EAS-PHD option, 16 priority levels are available. If you do not specify this option, two priority levels are available.
Tenant Number	The tenant partition number. A valid entry ranges from **1** to **100**. The default is **1**.

Table continues…

Field	Description
	Note: Values entered in this field are not echoed to the screen.
Multibyte Language	When you configure agent information, if the localized display name contains multiscript language characters, you must set the then multibyte language or locale. You can set the locale using the **Multibyte Language** field.
Check skill TNs to match agent TN	The skill tenant number to match the tenant number.
Include Tenant Calling Permissions	The tenant calling permissions. **Note:** To enable this feature you must first select **Check skill TNs to match agent TN** checkbox.

Button	Description
Commit	Completes the action you initiate.
Schedule	Performs the action at the chosen time.
Reset	Clears the action and resets the field.
Clear	Clears all entries.
Edit	Allows you to edit the fields in the page.
Commit with Auto Logout/Login (applicable only for Edit Agent page)	Enabling automatic logout and login after you commit a change. After automatic logout and login, the change you made takes immediate effect.
Schedule with Auto Logout/Login (applicable only for Edit Agent page)	Scheduling automatic logout and login every time you edit an agent property.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Announcements

What is an announcement?

An announcement is a recorded message that a caller hears while the call is in a queue. An announcement is often used in 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.

From Release 7.0, with Avaya Aura® Media Server, you can upload up to 10 MB size of `.wav` files.

Announcement List

Announcement List displays the property of an announcement. To view the announcement list, on the **Elements** menu, navigate to **Communication Manager** > **Call Center** > **Announcements**.

Name	Description
Name	The file name of the audio file. The alphanumeric file name can contain up to 27 characters.
Extension	The valid extension number for the announcement. Extension numbers might not include punctuation.
Group/Board	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).
Type	The type of the announcement. Possible values include: • **Integ-mus**. Integrated music type • **Integ-rep**. Integrated repeating type • **Integrated**. Stored internally on a special integrated announcement circuit pack. Use this for general announcements and VDN of Origin Announcements.
Protected	Use this field to set the protection mode for an integrated announcement.

Table continues…

Name	Description
	When you set this field to **y**, the recording is protected and cannot be deleted or changed through a telephone session or FTP. When you set this field to **n**, you can change or delete the recording if you have the corresponding console permissions.
Rate	If the VAL board is administered on the circuit packs form, then the system automatically displays 64 (64Kbps) in the **Rate** field.
COR	The Class of Restriction associated with this announcement.
TN	The tenant partition number of the announcement. A valid entry ranges from 1 to 100.
Queue	The announcement queuing or barge-in. Possible values include: • **no**. This is the default value. Indicates that the announcement does not play if a port is not available. • **yes**. 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 used in most call center applications. • **bargain**. 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.
Size	The size of the audio files in kilobytes.
Timestamp	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.
System	The name of the Communication Manager associated with the announcement.

Adding an announcement

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select **New**.

6. Complete the **Add Announcement** page and click **Commit**.

Related links

Announcements field descriptions on page 609

Editing an announcement

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the announcement you want to edit from the Announcement List.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields on the **Edit Announcement** page.
8. Click **Commit** to save the changes.

Related links

Announcements field descriptions on page 609

Viewing an announcement

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the announcement you want to view.
6. Click **View**.

   You can view the properties of the announcement in the **View Announcements** page.

Related links

Announcements field descriptions on page 609

Deleting an announcement

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.

5. Select the announcement you want to delete from the Announcement List.
6. Click **Delete**.
7. Confirm to delete the announcements.

Saving an announcement

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the announcement you want to save from the Announcement List.
6. Click **More Actions** > **Save**.

   This action internally edits and updates the announcements in the Communication Manager.

Related links

Announcements field descriptions on page 609

Backing up announcements

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the announcements you want to backup.
6. Click **More Actions** > **Backup** to back up your announcements.

Related links

Announcements field descriptions on page 609

Backing up all announcements

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Backup All** to back up all the announcements.

Downloading announcements

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Download**.
6. Select the files you want to download from the Backedup Announcements list.
7. Click **Download** to download the backed up announcements.

Related links

Announcements field descriptions on page 609

Restoring announcements

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Restore**.
6. Select a Communication Manager instance from the Communication Manager list.
7. Select the options from the Restore Options section.
8. If you want to restore from client, select the **Restore from Client** check box.
9. Select the announcements you want to restore from the Backedup Announcement List.
10. Click **Restore** to restore your announcement and announcement property files from your application to a VAL/Virtual VAL board you select.

Related links

Announcements field descriptions on page 609

Restoring all announcements

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.

5. Click **More Actions** > **Restore All**.

Moving an announcement

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Move**.
6. Select the destination where you want to move the announcement.
7. Click **Now** to move the announcement from one VAL board to another within the same voice system.

Related links

Announcements field descriptions on page 609

Broadcasting announcements

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the announcements you want to broadcast from the Announcement list.
6. Click **More Actions** > **Broadcast**.
7. Select the destination VAL source.
8. Click **Now** to broadcast the announcement files to various VAL boards on a voice system.

Related links

Announcements field descriptions on page 609

Using File Transfer Settings

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select an announcement from the Announcement List.

6. Click **More Actions** > **File Transfer Settings**.
7. Select a VAL board from the VAL Board and Media Gateway list.
8. Click **Done**.

Related links

Announcements field descriptions on page 609

Using List Usage Extension

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select an announcement from the Announcement List.
6. Click **More Actions** > **List Usage Extension**.

   You can view the details of the announcement through the List Usage for Extension list.
7. Click **Done**.

Related links

Announcements field descriptions on page 609

Filtering the Announcements list

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.
3. Click **Filter: Enable** in the Announcement list.
4. Filter the list according to one or multiple columns.
5. 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

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Announcements**.

3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Advanced Search** in Announcement List.
6. 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 the plus sign (**+**) and repeat the substeps listed in Step 5.

    If you want to delete a search condition, click the minus sign (**-**) . This button is available if there is more than one search condition.
7. Click **Search**.

Announcements field descriptions

Name	Description
System	The name of the Communication Manager associated with the announcement.
Name	The filename of the audio file. The filename can be up to 27 characters and must be alphanumeric.
Extension	Valid extension number for the announcement. Extension numbers might not include punctuation.
Type	The type of the announcement. Possible values include: • **Integ-mus**. Integrated music type • **Integ-rep**. Integrated repeating type • **Integrated**. Stored internally on a special integrated announcement circuit pack. Use this for general announcements and VDN of Origin Announcements.
Source	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). • Type the identifier for the Media Server device.
Protected	Use this field to set the protection mode for an integrated announcement.

Table continues…

Name	Description
	When you set this field to **y**, the recording is protected and cannot be deleted or changed through a telephone session or FTP. When you set this field to **n**, you can change or delete the recording if you have the corresponding console permissions.
Rate	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. **Note:** The system disables the **Rate** field when you select a Media Server as a source.
COR	The Class of Restriction associated with this announcement.
TN	The tenant partition number of the announcement. Valid entries include 1 to 100.
Queue	The announcement queuing or barge-in. Possible values include: • **no** (default)- indicates that the announcement does not play if a port is not available. • **yes** 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 used in most call center applications. • **bargain** 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.
Size	The size of the audio file in kilobytes.
Timestamp	The date and time the audio file was created or modified. This changes each time the audio file is uploaded.

Audio File Information

Name	Description
Use Unused Wave File	Select the check box to use an audio file that has not been used yet.
Upload Audio File	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
File Name	The filename of the audio file. The filename can be up to 27 characters and must be alphanumeric.
File Size	The size of the audio file in kilobytes.
Backup Announcement Properties	Backs up the announcement property
Backup Wave Files	Backs up the WAVE files only
Backup Both (Announcement Properties with associated wave file)	Backs up both the announcement property and the WAVE file for the announcement.
Restore Announcement Properties	Restores only your announcement properties
Restore Wave Files	Restores only the wave files present for the announcement.
Restore Both (Announcement Properties with associated wave file)	Restores both the announcement property and the wave file for the announcement.
Source	This field indicates the source location from where the announcement plays back. • The the location of the TN2501 board in the format of cabinet(1-64), carrier(A-E) and slot(1-20). For Example, 03A10 • The location of the Media Gateway vVAL in the format of `gggV9`, where ggg is the gateway number of the media gateway (up to 250). • The Group number (G1-G50) or the Media Server number (M1-M250)
Type	The whether the Announcement is a VAL Announcement or a Media Gateway (MG) Announcement.
Transfer Mode	Type of transfer used to backup or restore or upload audio files. Possible values are FTP, SFTP, and, SCP.
Used By	The object in which the extension is used. For example Endpoint, Announcement etc.
Object info	The details of the object.
Used as	The manner in which the extension is used in the object.

Button	Description
Commit	Completes the action you initiate.
Schedule	Performs the action at the chosen time.
Reset	Clears the action and resets the field.

Table continues…

Button	Description
Clear	Clears all the entries.
Edit	Allows you to edit the fields in the page.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Download	Downloads the audio files or announcement files.
Now	Performs the action you initiate real time.
Restore	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

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Audio Group**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Add Audio Groups** page and click **Commit**.

Related links

Audio Groups field descriptions on page 614

Editing an audio group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Audio Group**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the audio group you want to edit.

6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields and click **Commit** to save the changes.

Related links

Audio Groups field descriptions on page 614

Viewing an audio group

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Call Center** > **Audio Group** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the audio group you want to view.
6. Click **View** to view the properties of the audio group.

Related links

Audio Groups field descriptions on page 614

Deleting an audio group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Audio Group**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the audio groups you want to delete from the Audio Groups List.
6. Click **Delete**.
7. Confirm to delete the audio groups.

Using More Actions

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Audio Group**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select an audio group from the Audio Groups List.
6. Click **More Actions**.

7. 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 links

Audio Groups field descriptions on page 614

Audio Groups field descriptions

Name	Description
System	The device type. In this case, the Communication Manager you choose.
Group Number	The audio group number.
Group Name	The name of the audio group.

Members List

Name	Description
Source	Specifies whether the VAL board, Media Gateway or Media Server shown is a member in the audio group. 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). • The location of the TN2501 board in the format of cabinet(1-64), carrier(A-E) and slot(1-20). For Example, 03A10 • The location of the Media Gateway vVAL in the format of gggV9, where ggg is the gateway number of the media gateway (up to 250). • The Media Server number (M1-M250)
Is Member	Specifies whether the VAL board, the Media Gateway or the Media Server 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
CM	The Communication Manager you have chosen.
Backup Announcement Properties	Backs up the announcement property.

Table continues…

Name	Description
Backup Wave Files	Backs up the waves files only.
Backup Both (Announcement Properties with associated wave file)	Backs up both the announcement property and the wave file for the announcement.
File Name	Name of the audio group.
File Size	The size of the audio file in kilobytes.
Restore Announcement Properties	Restores only your announcement properties.
Restore Wave Files	Restores only the wave files present for the announcement.
Restore Both (Announcement properties with Associated wave file)	Restores both the announcement property and the wave file for the announcement.
Restore from client	Select this checkbox if you want to restore from the client machine.

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

Vector Directory Number

Vector Directory Number

The Vector Directory Number capability defines the 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.

Vector Directory Number List

Vector Directory Number List displays all the Vector Directory Number (VDN) details under the Communication Manager you select. You can view the usage list of the extension you select in this list. You can also apply filters and sort each of the columns in the Vector Directory Number List.

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

Name	Description
Extension	The extension number of the Vector Directory Number.
Name	The name associated with the Vector Directory Number.
Destination	Indicates whether the calls are routed using a Vector Number or Policy Routing Table.
Allow VDN Override	Indicates whether the routed-to Vector Directory Number is changed to active VDN for the call.
COR	The Class Of Restriction (COR) of the Vector Directory Number consisting of a one or two-digit number.
TN	The tenant partition number.
System	The name of the Communication Manager associated with the vector directory number.

Adding Vector Directory Number

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Add Vector Directory Number (VDN)** page and click **Commit**.

Viewing Vector Directory Number

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Directory Number List, select the vector directory number you want to view.

6. Click **View**.

Editing Vector Directory Number

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Directory Number List, select the vector directory number you want to edit.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Directory Number (VDN)** page.
8. Click **Commit** to save the changes.

Deleting Vector Directory Number

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Directory Number List, select the vector directory number you want to delete.
6. Click **Delete**.
7. Confirm to delete the vector directory number.

List Usage Extension in Vector Directory Number

Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Call Center** > **Vector Directory Number** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Directory Number List, select a vector directory number.
6. Click **More Actions** > **List Usage Extension**.
7. Click **Done**.

   You can view the details of the vector directory number in the List Usage for Extension list.

Vector Routing Table

Vector Routing Table

Use Vector Routing Table to store ANI or digits that you refer to in the **goto** vector steps. This capability is available only if the **Vectoring (G3V4 Enhanced)** field on the System-Parameters Customer-Options screen is set to **y**.

Vector Routing Table List

Vector Routing Table List displays all the Vector Routing Tables under the Communication Manager you select. You can also apply filters and sort each of the columns in the Vector Routing Table List.

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

Name	Description
Number	The table number you entered on the command line.
Name	The 1 to 15-character alphanumeric table name. By default, this field is blank.
Sort	Enables you to sort the digit fields.
Number Of Entries	The number of entries in the dialing list.
System	The name of the Communication Manager associated with the Vector Routing Table.

Adding Vector Routing Table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Routing Table**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Add Vector Routing Table** page and click **Commit**.

Related links

Vector Routing Table field descriptions on page 619

Viewing Vector Routing Table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Routing Table**.

3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Routing Table List, select the vector routing table you want to view.
6. Click **View**.

Related links

Vector Routing Table field descriptions on page 619

Editing Vector Routing Table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Routing Table**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Routing Table List, select the vector routing table you want to edit.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields on the **Edit Vector Routing Table** page.
8. Click **Commit** to save the changes.

Related links

Vector Routing Table field descriptions on page 619

Deleting Vector Routing Table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Call Center** > **Vector Routing Table**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Routing Table List, select the vector routing tables you want to delete.
6. Click **Delete**.
7. Confirm to delete the selected vector routing tables.

Related links

Vector Routing Table field descriptions on page 619

Vector Routing Table field descriptions

Field	Description
Name	The 1 to 15-character alphanumeric table name or blank. By default, this field is blank.
Number	The table number you entered on the command line. This is a display-only field.
Digit String	Entries in this field can include the plus sign (+) and question mark (?) wildcard. The plus sign (+) represents a group of digits. The question mark (?) represents a single digit. By default, this field is blank. The field is limited to 16 characters and these characters are restricted as follows: • You can enter only a plus sign (+), a question mark (?), or the numbers 0 through 9. No other entries are valid. • You can enter a plus sign (+) as either the first or last character in the number field. However, you cannot use this character as the sixteenth character of the number field. • You can use unlimited question marks (?) anywhere in the number field. • You should not embed blanks in the number field. • You can leave the field entirely blank. If you do, the communication server will store the entry as a null value.
Sort	Provides the option to sort the digit fields. By default, this check box is clear. If you do not to sort the numbers, they will remain in the order that you entered them. If you sort the number fields, they will be sorted as described below. Remember that leading zeros are significant. That means that 02 will sort ahead of a 2 followed by a space. • Any plus signs (+) will sort first. • Any question marks (?) will sort second. • All numbers (0-9) will sort last.
Route Number	The static route numbers that are available in the selected vector routing table.

Button	Description
Commit	Completes the action you initiate.
Schedule	Performs the action at the chosen time.
Reset	Clears the action and resets the field.

Table continues…

Button	Description
Clear	Clears all entries.
Edit	Allows you to edit the fields in the page.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate in real time.

Coverage Path

Coverage Path

Use Coverage Path to implement 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 telephone rings before the call redirects to coverage.

Coverage Path List

Coverage Path List displays all the coverage path details under the Communication Manager you select. You can also apply filters and sort each column in the Coverage Path List.

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

Name	Description
Coverage Path Number	The coverage path that is being administered.
Next Path Number	The number of the next coverage path in a coverage path chain.
Hunt after Coverage	Indicates whether the coverage treatment is continued or terminated.
Number of Rings	The number of times a telephone rings before the system redirects the call to the first point in the coverage path.
System	The name of the Communication Manager associated with the coverage path.

Adding Coverage Path

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Path**.
3. Select a Communication Manager instance from the Communication Manager list.

4. Click **Show List**.
5. Click **New**.
6. Complete the **Coverage Path** page and click **Commit**.

Related links

Coverage Path on page 623

Viewing a Coverage Path

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Path**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Path List, select the coverage path you want to view.
6. Click **View**.

Related links

Coverage Path on page 623

Editing a Coverage Path

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Path**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Path List, select the coverage path you want to edit.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Coverage Path** page.
8. Click **Commit** to save the changes.

Related links

Coverage Path on page 623

Deleting a Coverage Path

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Path**.
3. Select a Communication Manager instance from the Communication Manager list.

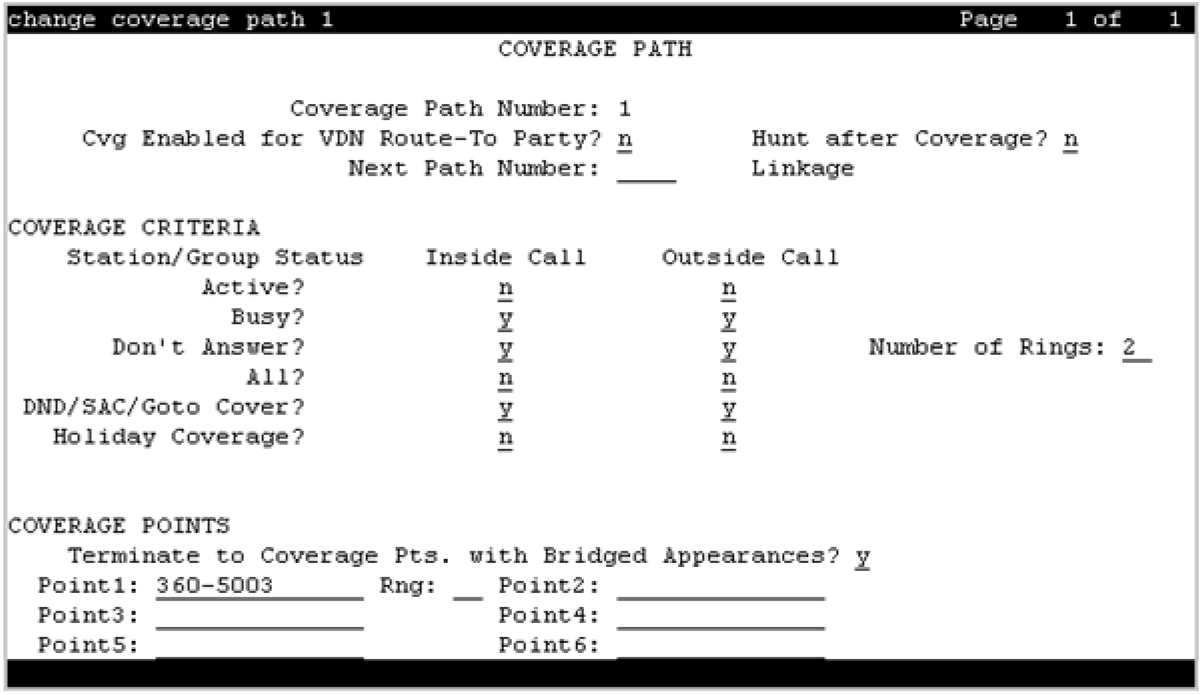
4. Click **Show List**.
5. From the Coverage Path List, select the coverage path you want to delete.
6. Click **Delete**.
7. Confirm to delete the coverage path.

Related links

Coverage Path on page 623

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.



```
change coverage path 1                                          Page   1 of   1
                                 COVERAGE PATH

                  Coverage Path Number: 1
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                      Next Path Number: ____      Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?             n               n
               Busy?             y               y
        Don't Answer?            y               y         Number of Rings: 2_
                All?             n               n
 DND/SAC/Goto Cover?             y               y
   Holiday Coverage?             n               n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? y
  Point1: 360-5003______    Rng: __ Point2: ______________
  Point3: ______________            Point4: ______________
  Point5: ______________            Point6: ______________
```

Coverage Path Number

The coverage path being administered.

Cvg Enabled for VDN Route-To Party

Enables or disables the route-to party coverage path after a covered call hits a VDN vector route-to step. By default, the value is n.

Holiday Coverage

Use the **Holiday Coverage** field to redirect all calls during a holiday to a coverage path. For **Holiday Coverage** to function, set the **Don't Answer** field to y.

You must set the **Holiday Coverage** field separately for internal and external calls.

Valid Entry	Usage
y	Communication Manager checks the Holiday Table screen for a specific holiday entry. If an entry on the Holiday Table screen matches with the current date and time, Communication Manager forwards the call to the first point that is defined in the coverage path. If there is no entry that matches with the current date and time, Communication Manager forwards the call to the subsequent point that is defined in the coverage path.
n	Communication Manager forwards the call to the subsequent point in the coverage path.

Holiday Table

Available only when **Holiday Coverage** is set to `y` for inside or outside calls.

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, the 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 dissatisfied, the system checks in 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 stays out of coverage.
blank	The only path for the principal.

COVERAGE CRITERIA

Active

Use this field to assign a coverage criteria. When the coverage criteria is met, the system redirects the call to coverage.

Valid Entry	Usage
y	The system redirects the call if at least one call appearance is busy.
n	The system does not redirect the call.

Busy

Use this field to assign a coverage criteria. When the coverage criteria is met, the system redirects the call to coverage.

Valid Entry	Usage
y	The system redirects the call if all call appearances that accept incoming calls are busy.
n	The system does not redirect the call.

Don’t Answer

Use this field to assign a coverage criteria. When the coverage criteria is met, the system redirects the call to coverage.

Valid Entry	Usage
y	The system redirects the call when the specified number of rings have been exceeded.
n	The system does not redirect the call.

All

Use this field to assign a coverage criteria. When the coverage criteria is met, the system redirects the call to coverage.

Valid Entry	Usage
y	The system redirects all calls to coverage. This option overrides any other criteria. Calls redirect immediately to coverage. Overrides any other criteria administered for this field.
n	The system does not redirect the call.

DND/SAC/Go to Cover

Use this field to assign a coverage criteria. When the coverage criteria is met, the system redirects the call to coverage.

Valid entry	Usage
y	With this option, a calling user, when calling to another internal extension, can redirect a call immediately to coverage by pressing the **Go to Cover** button. A principal user can temporarily direct all incoming calls to coverage, regardless of the other assigned coverage criteria by pressing the **Send All Calls** or **Do Not Disturb** button. With the **Send All Calls** button, covering users can temporarily remove their telephones from the coverage path. **Note:** You must assign this criteria before a user can activate **Do Not Disturb (Hospitality Services)**, **Send All Calls (SAC)**, or **Go to Cover** features.
n	The system does not redirect the call.

Logged off/PSA/TTI

Use this field to assign a coverage criteria. When the coverage criteria is met, the system redirects the call to coverage.

The system displays this field only when you set the **Criteria for Logged Off/PSA/TTI Stations** field to y.

Valid Entry	Usage
y	The system redirects the call after the number of rings exceeds the value specified in the **Number of Rings** field. The system displays the associated **Number of Rings** field only when the **Logged off/PSA/TTI** field is set to y.
n	The system does not redirect the call.

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 be unlisted 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 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 is nonexistent.

If the Coverage of Calls Redirected Off-Net feature is not supported, a remote coverage point functions as the last point in the coverage path because the system can no longer control calls once they redirect off-net. However, if the Coverage of Calls Redirected Off-Net feature is enabled, calls redirected off-net can be monitored by the system and brought back for call coverage processing.

Valid Entry	Usage
extension	Redirects the call to an internal extension or announcement. **Note:** If you enter a shortened extension of the multilocation dial plan, the system does not perform certain administration and validation tasks. Therefore, the system might not display the resultant warnings or submittal denials.

Table continues…

Valid Entry	Usage
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 h8000	Redirects the call to the corresponding hunt-group, for example, `h32` routes to hunt group 32.
c1 to c1500	Redirects the call to the corresponding coverage answer group, for example, `c20` routes to call coverage answer group 20.
r1 to r10000	Redirects the call to the corresponding remote coverage point number, for example, `r27` routes to remote coverage point 27.
v + extension	Redirects the call to the corresponding Vector Directory Number (VDN) extension, for example, `v12345` routes to the VDN associated with extension 12345. **Note:** A VDN can be used only as the last administered point in a coverage plan.
y + extension	Redirects the call to an internal extension, announcement, or the corresponding Vector Directory Number (VDN) extension as per the current date and time set in Holiday Table.

Rng

Valid Entry	Usage
1 to 99 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	If activated, a call can 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.

Coverage Time-of-day

Coverage Time-of-day

Use Coverage Time-of-day to administer 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 a given time.

Coverage Time-of-day List

Coverage Time-of-day List displays all the coverage time-of-day details under the Communication Manager you select. You can also apply filters and sort each column in the Coverage Time-of-day List.

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

Name	Description
Number	The Coverage Time-of-day table number.
System	The name of the Communication Manager associated with the vector directory number.

Adding Coverage Time-of-day

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Time-of-day**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Add Coverage Time-of-day Data** page and click **Commit**.

Related links

Time of Day Coverage Table on page 629

Viewing Coverage Time-of-day

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Time-of-day**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Time-of-day List, select the coverage time-of-day you want to view.
6. Click **View**.

Related links

Time of Day Coverage Table on page 629

Editing Coverage Time-of-day

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Time-of-day**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Time-of-day List, select the coverage time-of-day you want to edit.

6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Coverage Time-of-day Data** page.
8. Click **Commit** to save the changes.

Related links

Time of Day Coverage Table on page 629

Deleting Coverage Time-of-day

Procedure

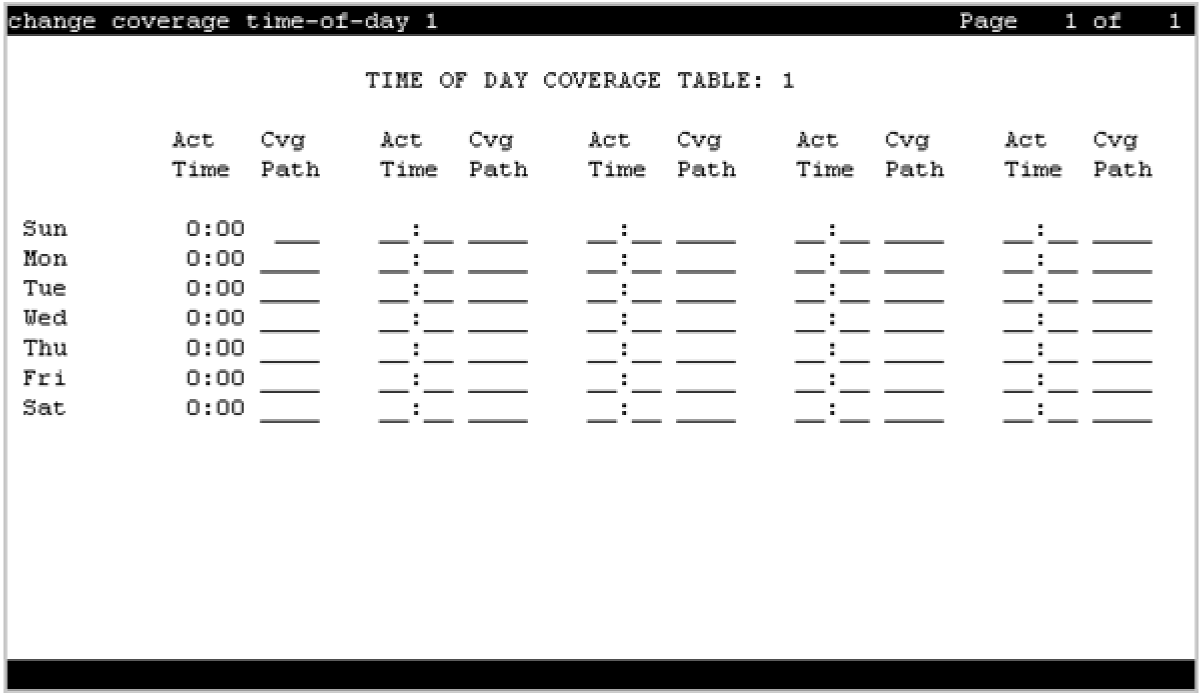
1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Coverage** > **Coverage Time-of-day**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Time-of-day List, select the coverage time-of-day you want to delete.
6. Click **Delete**.
7. Confirm to delete the coverage time-of-day.

Related links

Time of Day Coverage Table on page 629

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.



```
change coverage time-of-day 1                                    Page   1 of   1

                          TIME OF DAY COVERAGE TABLE: 1

            Act   Cvg       Act   Cvg       Act   Cvg       Act   Cvg       Act   Cvg
            Time  Path      Time  Path      Time  Path      Time  Path      Time  Path

 Sun         0:00 ____    __:__ ____     __:__ ____     __:__ ____     __:__ ____
 Mon         0:00 ____    __:__ ____     __:__ ____     __:__ ____     __:__ ____
 Tue         0:00 ____    __:__ ____     __:__ ____     __:__ ____     __:__ ____
 Wed         0:00 ____    __:__ ____     __:__ ____     __:__ ____     __:__ ____
 Thu         0:00 ____    __:__ ____     __:__ ____     __:__ ____     __:__ ____
 Fri         0:00 ____    __:__ ____     __:__ ____     __:__ ____     __:__ ____
 Sat         0:00 ____    __:__ ____     __:__ ____     __:__ ____     __:__ ____
```

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. 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 blank	The coverage path number.

Time of Day Coverage Table

Displays the Time of Day Coverage Table number.

Element Cut-Through

Element Cut-Through

The Element Cut-Through link allows you to access the Communication Manager cut through the Element Cut-Through page. As an administrator you can have various permissions to access the Communication Manager cut through.

- If you have only Communication Manager level access to Communication Manager1 and not Communication Manager2 nor Communication Manager3, then you will see only Communication Manager1 in the list. The other Communication Managers are not shown in the list at all.
- If you have no access to Element Cut-Through on any Communication Manager, then the Cut-Through navigation item will be grayed out or hidden.
- If you have access Element Cut-Through level permissions to some Communication Managers and not others, then the table displays only those Communication Managers that you have permissions.
- If you do not have Element Cut-Through permissions for a given Communication Manager, then the system displays an error message stating that you do not have permission for this operation.

Accessing Element Cut-Through

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Element Cut-Through**.
3. On the Element Cut-Through page, click on a Communication Manager.

   The system displays the Element Cut-Through page.

Element Cut-Through field descriptions

Name	Description
Element Name	The name of Communication Manager.
FQDN/IP Address	The fully qualified domain name or the IP address of Communication Manager.
Last Sync Time	The time when this Communication Manager was last synchronized with the Communication Manager database.
Last Translation Time	The time when the last translation of Communication Manager has been saved.

Table continues…

Name	Description
Sync Type	The type of synchronization. The options are initial and incremental.
Sync Status	The status of synchronization. The options are complete and in progress.
Location	The daylight saving time displayed to set the area code for each location.
Software Version	The software version of the Communication Manager.
CM Notification	The **CM Notification** is enabled or not while adding a Communication Manager system in System Manager.

Button	Description
Done	Saves your action and returns to the previous page.

Endpoints

Endpoint management

In System Manager, you can create and manage endpoints using the **Manage Endpoints** option. You can also manage other endpoint related objects such as, Alias Endpoints, Intra Switch CDR, Off PBX Endpoint Mappings, Site Data, and Xmobile Configuration. Additionally, using the **Manage Endpoints** option you can also view, edit, and delete endpoints and other endpoint related objects. System Manager provides support for the following set types:

Category	Set Type
IP/SIP Set types	9610SIP/9620SIP/9630SIP/9640SIP/9650SIP 9608SIP/9621SIP/9641SIP/9611SIP 9610/9620/9630/9640/9650 9608/9611/9621/9641 1603/1608/1616CC 9600SIP 4620SIP 9608SIPCC/9611SIPCC/9621SIPCC/9641SIPCC 4610/4620/4621/4622/4625/4630 4602+ 4612CL H.323

Table continues…

DCP Set types	2402/2410/2420 9404/9408 6402/6402D/6408/6408+/6408D/6408D+/6416D+/6424D+ 8403B/8405B/8405B+/8405D/8405D+/8410B/8410D/8411B/8411D/8434D 1408 1416
Analog Set types	2500
BRI Set types	WCBRI
X-Mobile endpoints	XMOBILE. Configured as ISDN DECT, IP DECT, PHS, or EC500 type endpoints. **Note:** Endpoints that are configured as XMOBILE cannot access important enhancements to EC500, such as support for SIP trunk groups.

Note:

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

Adding an endpoint

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Select the template based on the set type you want to add.
7. To add the endpoint, complete the New Endpoint page, and click **Commit**.

   Before adding an endpoint, complete the mandatory fields that are marked with a red asterisk (*). in the **General options**, **Feature Options**, **Site Data**, **Data Module/Analog Adjunct**, **Abbreviated Call Dialing**, **Enhanced Call Fwd**, and **Button Assignment** sections.

   Note:

   To add an endpoint with a non-supported set type, use Element Cut Through. For alias endpoints, 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 system displays the Alias endpoint type template in the drop-down menu, you must create an alias set type on the managed Communication Manager. You can then use the template to add an endpoint.

Related links

Endpoint / Template field descriptions on page 644

Using Native Name

Before you begin

To enter the native name:

- You need the Input Method Editor (IME) application.
- You must enable IME.

  Note:

  If IME is disabled, the keyboard input remains in the default language.

About this task

Using the IME application, you can enter characters in multiple languages such as Japanese, Korean, Russian, Arabic, and Chinese without requiring a special keyboard.

The IME icon appears in the Windows system tray and indicates the language that you currently use. 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**.

Procedure

1. In the Windows system tray, click the IME icon.

   The system displays a list of languages installed on your computer.
2. Select the language that you want to use.
3. On the System Manager web console, click **Users** > **User Management** and select the native name.

Editing an endpoint

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to edit from the Endpoint List.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields in the **Edit Endpoint** page.
8. Click **Commit** to save the changes.

Related links

Endpoint / Template field descriptions on page 644

Duplicating an endpoint

About this task

The Duplicate Endpoint functionality is to support the “duplicate station” command on Communication Manager. Use this functionality to copy information from an existing endpoint and modify it for each new endpoint. For example, you can configure one endpoint as desired for an entire work group. Then, you merely duplicate this endpoint to all the other extensions in the group. Note that only endpoints of the same type can be duplicated. This functionality copies all the feature settings from the selected endpoint to the new endpoints. You can duplicate up to 16 endpoints at one time.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to duplicate from the Endpoint List and click **Duplicate**.
6. On the Duplicate Endpoint page, complete the required fields.
7. Click **Commit** to duplicate the endpoint or do one of the following:
    - Click **Schedule** to duplicate the endpoint at a specified time.
    - Click **Cancel** to cancel the operation.

Related links

Endpoint / Template field descriptions on page 644

Viewing an endpoint

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to view from the Endpoint List.
6. 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 links

Endpoint / Template field descriptions on page 644

Deleting an endpoint

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to delete from the Endpoint List.
6. Click **Delete**.

   The system displays a confirmation message alerting you to a user associated with the endpoint. The system highlights 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.

Related links

Endpoint / Template field descriptions on page 644

Saving an endpoint as a template

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Select the template based on the set type you want to add, and complete the New Endpoint page.
7. To save the current settings as a template, click **Save As Template**.
8. Enter the name of the template in the **Template Name** field.
9. Click **Save**.
10. Click **Commit**.

Editing endpoint extensions

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.

2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint from the Endpoint List for which you want to edit the extension.
6. Click **More Actions** > **Edit Endpoint Extension**.
7. 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 links

Edit Endpoint Extension field descriptions on page 669

Bulk adding endpoints

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Bulk Add Endpoints**.
6. 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.

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

   Note:

   With Multi Tenancy, when you add endpoints in bulk, the Communication Manager devices and the extension range are available according to the Site you selected in the Communication Manager List page. **Tenant Number** and **Location** fields are auto populated for all the endpoints according to the Site you selected.

   COR and **COS** fields are validated as per the tenant permissions when you add the endpoints in bulk.

Related links

Bulk Add Endpoint field descriptions on page 670

Deleting endpoints in bulk

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select **More Actions** > **Bulk Delete Endpoints**.
6. On the Bulk Delete Endpoints page, select the Communication Manager from the **System** field.
7. Do one of the following:
   - Select the extension range you want to delete from the **Existing Extensions** field.
   - Type the extensions you want to bulk delete in the **Enter Extensions** field.
8. Click **Continue**.
9. On the Bulk Delete Endpoint Confirmation page, click **Now**.

   Click **Schedule** to schedule the bulk delete at a later time.

   Note:

   You cannot delete user associated stations.

Filtering endpoints

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Filter: Enable** in the Endpoint List.
6. Filter the endpoints 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 endpoints that match the filter criteria.

Related links

Endpoint / Template field descriptions on page 644

Using Advanced Search

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Advanced Search** in the Endpoint list.
6. 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 the plus sign (**+**) and repeat the sub steps listed in Step 5.

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

Related links

Endpoint / Template field descriptions on page 644

Changing endpoint parameters globally

About this task

Use the Global Endpoint Change capability to edit endpoint properties in bulk across one or more Communication Manager systems.

You can change the endpoint properties manually or change the endpoint properties based on a default template. You can select your preferred default template from the **Template Name** list on the **General Options** tab. When you select your preferred default template, the system overwrites the field values in different property tabs, such as General Options, Feature Options, and Button Assignment, with values in the default template. You can modify the endpoint properties of the default template to meet your requirement. The customization does not impact the default template because the system applies the changes only to the listed extensions.

For example, you can find all buttons or features with a specific assign and change the parameters for all those buttons or features respectively, locate new buttons without overwrite, and change the set type of many endpoints simultaneously as you move from digital to IP or SIP.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. On the Endpoints page, select the endpoints from the list for which you want to change the parameters.

4. Select a Communication Manager instance from the Communication Manager list.
5. Click **Show List**.
6. Select one or more endpoints, click **More Actions** > **Global Endpoint Change**.

   The system displays the Endpoint Changes page.
7. Click the General Options tab, and select **Set Type** to update the template.

   Note:

   If you also change the **Set Type** while updating the station, the default value overwrites the value in the **Port** field. The options for the default values are X and IP. Therefore, you must manually change the **Port** value for each station.
8. On the Endpoint Changes page, set the error configuration option in **Select Error Configuration**. The options are:
   - **Continue processing other records**: When you select this option, the system skips the erroneous record and continues to process the other records. This is the default setting.
   - **Abort on first error**: When you select this option, the system aborts the importing process on encountering the first error.
9. Do one of the following:
   - Modify the fields in each of the tabs as required.
   - In the General Options tab, select your preferred default template from the **Template Name** field, and update the property fields as required.

     The system overwrites all the field values with the values in the template. This update does not affect the default template because the system applies the changes only to the listed extensions.
10. Do one of the following:
    - To change the endpoint parameters immediately, click **Commit**.
    - To change the endpoint parameters at a specified time, click **Schedule**.

    The system updates the selected endpoints or schedules the edit job to the specified time.

Related links

Endpoint / Template field descriptions on page 644

Viewing endpoint status

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. From the Endpoint List, select the endpoints whose status you want to view.
4. Click **Maintenance** > **Status**.

Result

The system displays the status of the selected endpoint on the Element Cut Through screen.

Related links

Endpoint / Template field descriptions on page 644
Error codes on page 671

Busy out endpoints

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select the endpoints you want to busy out from the Endpoint List.

   ❗ **Important:**

   This maintenance operation is service affecting.
4. Click **Maintenance** > **Busyout Endpoint**.
5. On the Busyout Endpoint Confirmation page, click **Now** to busy out the endpoints or do one of the following:
   - Click **Schedule** to perform the busy out at a specified time.
   - Click **Cancel** to cancel the busy out.

Result

The system displays the result of the busy out operation on the **Busyout Endpoint Report** page.

Related links

Endpoint / Template field descriptions on page 644
Error codes on page 671

Releasing endpoints

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select the endpoints you want to release from the Endpoint List.

   ❗ **Important:**

   This maintenance operation is service affecting.
4. Click **Maintenance** > **Release Endpoint**.
5. On the **Release Endpoint Confirmation** page, click **Now** to release the endpoints or do one of the following:
   - Click **Schedule** to perform the release at a specified time.

- Click **Cancel** to cancel the release.

Result

The system displays the result of the release operation on the **Release Endpoint Report** page.

Related links

Endpoint / Template field descriptions on page 644
Error codes on page 671

Testing endpoints

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select the endpoints you want to test from the Endpoint List.

   ❗ **Important:**

   This maintenance operation is service affecting.
4. Click **Maintenance** > **Test Endpoint**.
5. On the Test Endpoint Confirmation page, click **Now** to test the endpoints or do one of the following:
   - Click **Schedule** to test the endpoints at a specified time.
   - Click **Cancel** to cancel the test operation.

Result

The system displays the **Test Endpoint Report** page, where you can view the test result and error code of the endpoint. Click the **Error Code Description** link to view the error details.

Related links

Endpoint / Template field descriptions on page 644
Error codes on page 671

Using Clear AMW All

Clear AMW All is one of maintenance operations listed under the **Maintenance** drop-down on the Manage Endpoints page. You can perform this operation on a single or multiple endpoints from the Endpoint List. In this maintenance operation, for each endpoint, the system runs the following SAT command

```
clear amw all <endpoint>
```

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select the endpoints from the Endpoint List for which you want to use this functionality.

4. Click **Maintenance** > **Clear AMW All**.
5. On the **Clear AMW All Confirmation** page, click **Now** to perform this task immediately, or do one of the following:
   - Click **Schedule** to perform this task at a specified time.
   - Click **Cancel** to cancel this task.

   The system displays a confirmation that the command has been completed and returns you to the Manage Endpoint landing page.

Using Swap Endpoints

About this task

Use this functionality to swap location site data between two endpoints of the same type and the same Communication Manager system. For Analog and DCP endpoint types, this functionality also swaps the physical port information. While swapping the endpoint data, you also have the option to assign new location site data to the endpoints.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Swap Endpoints**.
6. On the Swap Endpoints page, enter endpoint extension values in the fields **Endpoint 1** and **Endpoint 2**.
7. Click **Show Details**. The system displays the location site data for each endpoint under the respective endpoint tabs.
8. Click **Commit** to swap data between the two endpoints.
9. To assign new values to the endpoints, perform the following:
   a. Click the endpoint tab whose data you want to change.
   b. Select the **Assign data for Endpoint**<*n*> check box.
   c. Enter the required values for the endpoint under **Descriptions**.
   d. Click **Commit**.

Related links

Swap Endpoints field descriptions on page 670

Endpoint / Template field descriptions on page 644

Endpoint list

The endpoint list displays all endpoints associated with Communication Manager that you select. You can perform an advanced search on the endpoint list by using the search criteria. You can apply filters and sort each of the columns in the endpoint list.

Name	Description
Name	The endpoint name.
Extension	The extension of the endpoint.
Port	The port of the endpoint.
Set Type	The set type of the endpoint.
COS	Class Of Service for the endpoint.
COR	Class Of Restriction for the endpoint.
User	The user to which the endpoint is associated.
System	Communication Manager of the endpoint.

Button	Description
Refresh	Displays the updated information that is available after the last synchronization.

Add Endpoint Template

Endpoint / Template field descriptions

Use the fields to perform endpoint or template tasks. The page displays 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 descriptions for Endpoints

Name	Description
System	The Communication Manager that the endpoint is assigned to.
Template	Templates that correspond to the set type of the endpoint.
Set Type	The set type or the model number of the endpoint.
Name	The name of the endpoint. The system displays the name on called telephones with display capabilities. In some messaging applications, such as Communication Manager Messaging, you enter the user name (last name first) and the extension to identify the telephone. The name is also used in the integrated directory. When you enter the first name and the last name of the user associated with an endpoint on User Management, the system populates Latin translation of the first name and the last name in the **Name** field.

Field descriptions for Templates

Name	Description
Set Type	The set type or the model of the endpoint template.
Template Name	The name of the endpoint template. You can enter the name of your choice in this field.

Button	Description
Commit	Saves the values that you enter and starts the add or edit operation.
Schedule	Displays the Job Scheduler where you can schedule the edit operation.
Reset	Clears the values that you enter on the page.
Cancel	Cancels the current operation and returns to the previous page.

Extension

The extension for this station.

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

Port

The Auxiliary and Analog ports assigned to the station are as follows.

Valid Entry	Usage
01 to 64	The first and second numbers are the cabinet numbers.
A to E	The third character is the carrier.
01 to 20	The fourth and fifth characters are the slot numbers. G650 has 14 slots.
01 to 32	The sixth and seventh characters are the port numbers.
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 has 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 Branch Gateway. • xxx is the Branch Gateway number, which is in the range 001 to 250.

Table continues…

Valid Entry	Usage
	• m is the module number, which is in the range 1 to 9. • pp is the port number, which is in the range 01 to 32.
Analog Trunk port	Analog trunk port is available with: • MM711 and MM714 media modules • TN747 and TN797 circuit packs

General Options

Use this section to set the general fields for a station.

COR

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

COS

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

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 thirteen 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.

Message Lamp Ext

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

TN

Use this field to specify a tenant number. You can enter a value from 1 to 250.

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.

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.

Multibyte Language

When you configure endpoints, if the localized display name contains multiscript language characters, then you must set the locale or multibyte language. You can set the locale using the **Multibyte Language** field. The possible values for the **Multibyte Language** field are:

- Japanese
- Simplified Chinese
- Traditional Chinese
- Not Applicable

In **User Management** > **Manage Users** > **Identity**, if you choose the Simplified Chinese, Traditional Chinese, or Japanese from the **Language Preference** field for a user, the appropriate language is auto populated in the **Multibyte Language** field for the same user. If you choose any other language from the **Language Preference** field, the system displays **Not Applicable** in the **Multibyte Language** field.

Continue on Error

When an error occurs, the system provides an option to continue or abort the implementation of parameter changes.

Security Code

The security code required by users for specific system features and functions are as follows:

- Extended User Administration of Redirected Calls
- Personal Station Access
- Redirection of Calls Coverage Off-Net
- Leave Word Calling
- Extended Call Forwarding
- Station Lock
- Voice Message Retrieval
- Terminal Self-Administration
- Enterprise Mobility User
- Extension to Cellular
- Call Forwarding
- Posted Messages

- Security Violation Notification
- Demand Printing

The required security code length is administered system wide.

Feature Options

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

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. If disabled and **Per Button Ring Control** is also disabled, audible ringing is suppressed for incoming calls on bridged appearances of another telephone's primary extension.

Location

The system displays this field only when you set the **Multiple Locations** field on the system parameters customer options screen to y, and set the **Type** field to H.323 or SIP station types.

Valid entry	Usage
1 to 2000	(Depending on your server configuration, see *Avaya Aura® Communication Manager System Capacities Table*, 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 *Avaya Aura® Communication Manager Feature Description and Implementation*, 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 an Expert Agent Environment (EAS) environment, the auto answer setting for an Agent LoginID overrides the endpoint settings when the agent logs in.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 to an idle station cut through immediately. The agent cannot use automatic hands-free answer for intercom calls. With non-ACD calls, the station rings while the call is cut through. To prevent the station from ringing, activate the **ringer-off** feature button, provided the Allow Ringer-off with Auto-Answer feature is enabled for the system.
acd	Only ACD split, ACD skill, and direct agent calls cut through. Non-ACD calls to the station ring audibly. For analog stations: • Only the ACD split or skill calls and direct agent calls cut through. • 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 to the station receive an audible ringing.
icom	The user can answer an intercom call from the same intercom group without pressing the intercom button.

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(ystem)	Administered system-wide coverage parameters determine treatment.

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 french italian spanish user-defined	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. **Note:** Unicode display is only available for Unicode-supported telephones. Currently, 4610SW, 4620SW, 4621SW, 4622SW, 16xx, 96xx, 96x1, 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 must hunt to for this telephone when the telephone is busy. You can create a station hunting chain 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. You cannot use an Avaya IP endpoint to dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. Avoid using 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. If you have questions about emergency calls from IP telephones, go to the Avaya Support website at http://support.avaya.com.

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). If the administrator populates the IP address mapping with emergency numbers, the value as-on-local functions as follows: • If the station emergency location extension is the same as the IP address mapping emergency location extension, the value as-on-local sends the station's own extension to the Public Safety Answering Point (PSAP). • 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).
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. Use this entry for IP Softphones with road warrior service that are near enough to the server that an emergency call reaches the PSAP that covers the softphone's physical location. If the server uses ISDN trunks for emergency calls, the digit string is the

Table continues…

Valid Entry	Usage
	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. The user chooses between block and cesid on the softphone. A DCP or IP telephone in the office automatically selects the extension.

Service Link Mode

Use this field to specify the duration of a service link connection. The service link is the combined hardware and software multimedia connection between an H.320 Desktop Video Conferencing (DVC) system and Communication Manager.

The service link is established when a user receives or makes a call during a multimedia, IP softphone, or IP telephone session.

Valid entry	Usage
as-needed	For multimedia, IP softphone, and IP telephone users. The service link remains connected for 10 seconds after the user disconnects a call so that the user can immediately make or receive another call. After 10 seconds, the link is disconnected, and a new link must be established to make or receive a call.
permanent	For call center agents who are constantly making or receiving calls during the multimedia, IP softphone, or IP telephone session. The service link remains connected for the entire duration of the session.

Loss Group

Valid Entry	Usage
1 to 17	Determines which administered two-party row in the loss plan applies to each station. Is not displayed for stations that do not use loss, such as x-mobile stations.

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	With Group Listen, a telephone user can 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

Table continues…

Valid Entry	Usage
	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. Available only with 6400-series and 2420/2410 telephones.
none	Not administered for a speakerphone.

LWC Reception

Use this field to specify the location where the system must store the LWC messages.

Valid entry	Usage
spe	Use this option to store the LWC messages on Switch Processor Element (SPE).
none	Use this option if you do not want to store the LWC messages.
audix	Use this option to store the LWC messages on the voice messaging system.

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 has 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 Branch 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.

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 Branch 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. With this, the IP station can 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 46*xx* or 96*xx* models.

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.

Call Appearance Display Format

Specifies the display format for the station. Bridged call appearances are not affected by this field. This field is 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.

IP Phone Group ID

Available only for H.323 station types.

Valid Entry	Usage
0 to 999 blank	The Group ID number for this station.

Always Use

Use this field to enable the following emergency call handling settings:

- A softphone can register irrespective of the emergency call handling settings the user has entered into the softphone. If a softphone dials 911, the value administered in the **Emergency Location Extension** field is used as the calling party number. The user-entered emergency call handling settings of the softphone are ignored.
- If an IP telephone dials 911, the value administered in the **Emergency Location Extension** field is used as the calling party number.
- If an agent dials 911, the physical station extension is used as the calling party number, overriding the value administered in the **LoginID for ISDN Display** field.

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

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.

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 Idle Line Preference

Use this field to specify that the line that the system selects when you go off hook is always an idle call appearance for incoming bridged calls.

Valid entry	Usage
y	The user connects to an idle call appearance instead of the ringing call.
n	The user connects to the ringing bridged appearance.

CDR Privacy

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

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**.

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

Use this field to specify whether the extension has IP video capability. The system displays this field for H.323 and SIP station types.

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.

Direct IP-IP Audio Connections

Use this field to enable direct audio connections between IP endpoints. Direct audio connections save bandwidth resources and improve the 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.

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 Branch 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 Branch Gateways.

Available for all analog and IP station types.

Valid Entry	Usage
y	Allows this station to be an incoming trunk destination while the Branch 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

Use this field to enable the conversion of H.320-compliant calls to voice-only calls for the attendant console.

Note:

The system can handle only a limited number of conversion calls. Therefore, the number of attendant consoles with H.320 conversion must 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 trunk groups. H.323 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.

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. With LWC, internal telephone users on this extension can leave short pre-programmed messages for other internal users.

You must use LWC if:

- The system has hospitality and the guest-room telephones require LWC messages indicating that wakeup calls failed

- The 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.

You must enable the station for the Multimedia Early Answer 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

Using this option you can enable or disable ring control for every button, provided you have the station user credentials.

Valid Entries	Usage
y	To enable Automatic Abbreviated and Delayed ring transition for each call-appr on the station, select ring behavior individually for each call-appr or brdg-appr option. To prevent the system from automatically moving the line selection to a silently alerting call, unless the call was audibly ringing earlier. **Note:** The abrdg-appr option is unavailable for SIP station.
n	To enable the calls on **call-appr** buttons always to ring the station To enable the calls on **brdg-appr** buttons always ring or not ring based on the **Bridged Call Alerting** value To move line selection to a silently alerting call, if the call is not audibly ringing the station **Note:** The abrdg-appr option is unavailable for SIP station.

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.

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 ion the bridged appearance is allowed. This is normal behavior, and is the default.

Voice Mail Number

Displays the complete voice mail dial up number. Accepts a value of up to 24 characters consisting of digits from 0 to 9, asterisk (*), pound sign (#), ~p (pause), ~w/~W (wait), ~m (mark), and ~s (suppress). This field is supported in the following set types: 9620SIP, 9630SIP, 9640SIP, 9650SIP, 9608SIP, 9611SIP, 9621SIP, 9641SIP, 9608SIPCC, 9611SIPCC, 9621SIPCC, and 9641SIPCC.

Music Source

Field	Description
Music Source	Valid values are 1 to 100 or blank. The value can extend to 250 when you select the Multi Tenancy feature from the system parameter customer option on the Communication Manager. **Music Source** field is applicable for all endpoint set types. **Note:** Select the **System Parameter Special Application**, and select **SA8888 Per Station Music On Hold**, Only then you can select the **Music source** field.

Site Data

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

Room

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

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.

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).

You can change the list of allowed set colors by using the Valid Set Color fields on the site-data screen.

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	Telephone user can access the enhanced system abbreviated dialing list.
group	Telephone user can access the specified group abbreviated dialing list. Requires administration of a group number.
personal	Telephone user can access and program their personal abbreviated dialing list. Requires administration of a personal list number.
system	Telephone user can access the system abbreviated dialing list.

Personal List

Use this list to establish a personal dialing list for telephone or data module users.

Enhanced List

Use this list to establish system-wide or personal lists for speed dialing.

Users access this list to:

- place local, long-distance, and international calls
- activate or deactivate features
- access remote computer equipment.

Note:

You must activate dialing in the license file before the system programs the Abbreviated Dialing Enhanced List.

Group List

You can provide up to 100 numbers for every group list.

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

With **SAC/CF Override**, the user of the calling station can override the redirection set by the called station.

Valid entry	Usage
ask	The system prompts the user of the calling station whether the call must follow the redirection path or override the redirection path. The user can type y or n.

Table continues…

Valid entry	Usage
no	The user of the calling station cannot override the redirection path of the call. The call follows the redirection path.
yes	The user of the calling station can override the redirection path of the call, provided the called station has at least one idle call appearance.

Button assignment

You can assign features to the buttons on a phone. You can assign the main buttons for your endpoint by choosing an option from the list for each button.

Endpoint Configurations:

The endpoint configuration is available on the 9608, 9611, 9621, 9641 SIP, and SIPCC endpoints for Communication Manager 6.2 and later.

The Favorite Button and Button Label features function when the endpoint is associated to a user with the Session Manager profile.

Name	Description
Favorite	The favorite button. **Note:** You can mark maximum nine buttons as favorites on an endpoint, which includes the configured contacts on the phone. The **Favorite** button is disabled for the **call-appr**, and the **bridge-appr** button features. Therefore, you cannot select these button features as a favorite. To set the **Auto Dial** button as a favorite, or to set the **Button Label** for auto dial, you must specify the **Dial Number**.
Button Label	The personalized button label that is displayed on the phone. **Note:** The button label is not localized on the phone.

Button Configurations:

Name	Description
Button Feature	The button feature that is available on the phone.
Argument	The argument for the button feature that is available on the phone.

Profile settings field descriptions

Note:

Profile Settings is available for 9608, 9611, 9621, 9641 SIP, and SIPCC set types of endpoints for Communication Manager Release 6.2 and later.

Profile Settings work when the endpoint is associated to a user with a Session Manager profile.

Call Settings options

Name	Description
Phone Screen on Calling	The option to specify whether the phone must automatically display the phone screen when the user goes off-hook or starts dialing. The options are: • **Yes**. • **No**.
Redial	The field to select from the following redial options: • **List**: To display a list of recently dialed numbers. • **One Number**: To automatically dial the last dialed number.
Dialling Option	The field to specify the dialing options: • **Editable**: To enable off-hook dialing that mimics dialing a call on a cell phone. When the user starts dialing, the edit dialing interface displays the dialed digits. The user can enter all or part of the number or backspace to correct a number if needed. When ready, the user must press the **Call** soft key to connect. • **On-hook**: To enable on-hook dialing so that when the user starts dialing , the phone automatically goes on-hook on the first available line and dials the digits.
Headset Signalling	The field that defines a headset signaling profile. The options are: • **Disabled**: To disable headset signaling profile. • **Switchhook and Alerts**: To set the switch hook and alert headset signaling profile. • **Switchhook only**: To set the switch hook headset signaling profile.

Table continues…

Name	Description
Audio Path	The field to set the phone to go off-hook when you make an on-hook call. The options are: • **Speaker**: To go off-hook on the Speaker when you make an on-hook call. • **Headset**: To go off-hook on the Headset when you make an on-hook call. **Note:** If your system administrator has set up auto-answer, incoming calls are also answered on the default audio path you designate here.

Screen & Sound Options

Name	Description
Button Clicks	The field to activate or deactivate the standard button click sound. The options are: • **On**. • **Off**.
Phone Screen	The field to configure the phone screen width. The options are: • **Half**: To split the phone screen width to half so that each call appearance or feature occupies half the width of a line. • **Full**: To set the phone screen width to full so that each call appearance or feature occupies the entire width of a line.
Background Logo	The option to set a customized background logo. The **Default** value sets the built-in Avaya logo.
Personalized Ringing	The option to set a personalized ring tone for an incoming call. The options are: • Classic Tone, with 8 options • Cheerful • Chimes • Telephone Bell • Xylophone • Drum Beat • Shimmer

Table continues…

Name	Description
	✱ **Note:** The Personalized Ringing parameter is available on the Communication Manager Release 6.2 and 6.3 templates. However, the parameter does not apply to Release 6.2 and earlier Avaya Advanced SIP Telephony (AST) endpoints. In some cases, the Avaya EST endpoints might overwrite the newly configured value of the parameter. For example, an endpoint where the related ringing parameter called Ringer Cadence is set to a value other than 1. In this case, the endpoint sets the Personalized Ringing parameter to the value of Ringer Cadence within a few minutes of the change. The reset can also happen during the next login of the endpoint. Session Manager was modified to reduce the instances of this occurrence. The default value of Ringer Cadence is set to 1 for any new Device Settings Groups added to Release 6.3.8. You can set the parameter on the **Device and Location Configuration** > **Device Settings Groups** page from the **Elements** > **Sessions Manager** link.
Call Pickup Indication	The option to set ring tones to alert you about an incoming call. The options are: • **None**: No pickup indication for an incoming call. • **Audible**: Audible ringing indicates an incoming call. • **Visual**: LED flashes indicate an incoming call. • **Both**: Both audible ringing and LED flashes indicate an incoming call.
Show Quick Touch Panel	The options to display **Quick Touch Pane**l on the phone. The options are: • **0**: Not to display **Quick Touch Panel**. • **1**: To display a one-line **Quick Touch Panel**. • **2**: To display a two—line **Quick Touch Panel**. ✱ **Note:** Displaying the **Quick Touch Panel** field can limit your call appearances display to three lines at a time.

Table continues…

Name	Description
	This field is available for 9621 and 9641 SIP, and SIPCC set type of endpoints.

Language & Region

Field	Description
Language	The option to configure the language. The options are: • English • Hebrew • Brazilian Portuguese • Canadian French • German • Parisian French • Latin American Spanish • Castilian Spanish • Italian • Dutch • Russian • Simplified Chinese • Japanese • Korean • Arabic **Note:** The Arabic language is not available for 9608 SIP and SIPCC set type of endpoints.
User Preferred Language	The option to configure the user preferred language. The options are: • English • Hebrew • Brazilian Portuguese • Canadian French • German • Parisian French • Latin American Spanish • Castilian Spanish

Table continues…

Field	Description
	- Italian - Dutch - Russian - Simplified Chinese - Japanese - Korean - Arabic **Note:** The Arabic language is not available for 9608 SIP and SIPCC set type of endpoints.
Language File in Use	The option to configure the file name to use for the configured language. The options are: - Mlf_English.xml - Mlf_Hebrew.xml - Mlf_BrazilianPortuguese.xml - Mlf_CanadianFrench.xml - Mlf_German.xml - Mlf_ParisianFrench.xml - - Mlf_LatinAmericanSpanish.xml - Mlf_CastilianSpanish.xml - Mlf_Italian.xml - Mlf_Dutch.xml - Mlf_Russian.xml - Mlf_Chinese.xml - Mlf_Japanese.xml - Mlf_Korean.xml - Mlf_Arabic.xml **Note:** The Mlf_Arabic.xml language file is not available for 9608 SIP and SIPCC set type of endpoints.
Time Format	The option to configure the time format to be displayed on the phone screen. The options are: - **12 Hour**.

Table continues…

Field	Description
	• **24 Hour**.

Advance Options Presence integration

Field	Description
Away Timer	The option to enable the automatic away timer for presence indication. The options are: • **On**. • **Off**.
Timer Value	The option to specify a value for the automatic **Away Timer**. The **Timer Value field** accepts a value from 5 to 480.

Group Membership

This section describes the different groups that an extension can be a member of. Select the station you want to group, and then choose the group from the drop-down box, before you click **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 might include other types of groups such as trunk groups. For more information on groups, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Your voice system can 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 100 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 *Administering Avaya Aura® Communication Manager, 03-300509*.
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

Table continues…

Type	Description
	than one person to be able to answer calls to the same number. For more information on hunt groups, see “Managing Hunt Groups” in the *Administering Avaya Aura® Communication Manager, 03-300509*.
intercom group	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. For more information on intercom groups, see “Using Phones as Intercoms” in the *Administering Avaya Aura® Communication Manager, 03-300509*.
pickup group	A pickup group is a group of extensions in which one person can pick up calls of another person. For more information on pickup groups, see “Adding Call Pickup” in the *Administering Avaya Aura® Communication Manager, 03-300509*.
terminating extension group	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. For more information on terminating extension groups, see “Assigning a Terminating Extension Group” in the *Administering Avaya Aura® Communication Manager, 03-300509*.

Edit Endpoint Extension field descriptions

Name	Description
System	The list of Communication Manager systems from where you can select.
Extension	The extension of the device that you want to change.
New Extension	The new extension for the device.
Emergency location extension	The existing extension for the emergency location of your device.
New emergency location extension	The new extension for the existing emergency location of your device.
Message lamp extension	The existing extension for the message lamp of your device.
New message lamp extension	The new extension for the message lamp of your device.

Button	Description
Commit	Saves the new extension.
Schedule	Saves the extension at the scheduled time.
Reset	Clears all entries.
Cancel	Return to the previous page.

Bulk Add Endpoint field descriptions

Name	Description
Template	The template for the endpoints.
Station name prefix	The prefix name that the system displays for each endpoint that you add.
System	The list of Communication Manager systems.
Available extensions	The list of extensions that are available.
Enter extensions	The extensions that you want to use.

Button	Description
Commit	Adds the endpoints in bulk.
Schedule	Adds the station in bulk at the scheduled time.
Clear	Undoes all entries.
Cancel	Returns to the previous page.

Swap Endpoints field descriptions

Name	Description
Assign data for Endpoint <*n*>	An option to assign new values of location site data to an endpoint. When you select this check box for an endpoint, the system copies the location site data values of this endpoint to the second endpoint where this check box is clear. If you select the check boxes for both endpoints, the system copies new location site data to respective endpoints. The system does not swap values.
System	Communication Manager to which the endpoint is assigned. The system is listed in the Communication Manager List page.
Endpoint 1 **Endpoint 2**	The existing endpoint extension number on the selected Communication Manager.

Button	Description
Commit	Performs the action that you initiate.
Schedule	Performs the action at the specified time.
Cancel	Cancels your current action and returns to the previous page.

Error codes

Following table gives the common error codes for Busyout, Release, Test, and Reset Commands lists. This table also has the common error codes associated with abort and fail results for busyout, release, test, and reset commands. In addition to these, many maintenance objects have other unique error codes.

Error Code	Command Result	Description/Recommendation
	ABORT	System resources are unavailable to run command. Try the command again at 1-minute intervals up to 5 times.
0	ABORT	Internal system error. Retry the command at 1-minute intervals up to 5 times.
1005	ABORT	A DS1 interface circuit pack could not be reset because it is currently supplying the on-line synchronization reference. Use set sync to designate a new DS1 interface circuit pack as the on-line reference, then try the reset again.
1010	ABORT	Attempt was made to busyout an object that was already busied out.
1011	ABORT	Attempt was made to release an object that was not first busied out.
1015	ABORT	A reset of this circuit pack requires that every maintenance object on it be in the out-of-service state. Use busyout board to place every object on the circuit pack in the out-of-service state, and try the reset again.
1026	ABORT	The specified TDM bus cannot be busied out because the control channel or system tones are being carried on it. Use set tdm PC to switch the control channel and system tones to the other TDM bus.
2012 2500	ABORT	Internal system error.
2100	ABORT	System resources to run this command were unavailable. Try the command again at 1-minute intervals up to 5 times.
62524 62525 62526	ABORT	Maintenance is currently active on the maximum number of maintenance objects that the system can support. A common cause is that the system contains a large number of administered stations or trunks with installed circuit packs that are not physically connected. Resolve as many alarms as possible on the station and trunk MOs, or busyout these MOs to prevent maintenance activity on them. Then try the command again.
	NO BOARD	The circuit pack is not physically installed.
2100	EXTRA BD	This result can appear for: S8700 Maintenance/Test, Announcement circuit packs S8700 MC Call Classifier, Tone Detector, Speech Synthesis circuit packs Each of these circuit packs has restrictions on

Table continues…

		how many can be installed in the system or in a port network, depending on system configuration. Remove any extra circuit packs.
1	FAIL	For reset commands, the circuit pack was not successfully halted.
2	FAIL	For reset commands, the circuit pack was not successfully restarted after being halted. For both results replace the circuit pack.
	FAIL	See the applicable maintenance object (from the Maintenance Name field) in Maintenance Alarms Reference, 03-300190.
	PASS	The requested action successfully completed. If the command was a reset, the circuit pack is now running and should be tested.

Auto answer

When you administer **Auto Answer**, the **Communication Manager Endpoint Manager** field displays the following behavior with regards to the **Mute Speakerphone Interaction**, the **Auto Answer** field and the **int aut-an** button:

1. The system does not display the **Turn On Mute for Remote Off-hook Attempt** field for the following configurations:
   - When **Auto Answer** has a value other than **none**.
   - When you enable the **int-aut-an** button for an endpoint.
2. If you enable the **Turn On Mute for Remote Off-hook Attempt** field in the endpoints page, **Communication Manager Endpoint Manager** field does not permit the following administration:
   - **Auto Answer** values other than **none**.
   - **int-aut-an** button administration.

Auto answer field descriptions

In **Expert Agent Environment (EAS)** environment, the auto answer setting for an **Agent LoginID** overrides the endpoint settings when the agent logs in.

Valid entry	Usage
all	All ACD and non-ACD calls to an idle station cut through immediately. The agent cannot use automatic hands-free answer for intercom calls. With non-ACD calls, the station rings while the call is cut through. To prevent the station from ringing, activate the ringer-off feature button, provided the **Allow Ringer-off with Auto-Answer** feature is enabled for the system.
acd	Only ACD split, ACD skill, and direct agent calls cut through. Non-ACD calls to the station ring tone.

Table continues…

Valid entry	Usage
	For analog stations: • Only ACD can perform: 1. Split calls and Skill calls 2. Direct agent calls cut through • Non-ACD calls receive busy tone. If the station is active on an ACD call and a non-ACD call arrives, the agent hears call-waiting tone.
none	All calls to the station receive a ringing tone.
icom	The user can answer an intercom call from the same intercom group without pressing the **intercom** button.

Turn On Mute for Remote Off-hook Attempt

Using the **Telecommuter** mode of a soft phone or an ASAI, users can control the desk phone remotely. However, users can remotely hear the conversations, which might be considered a privacy breach.

The **Turn On Mute for Remote Off-hook Attempt** field prevents the potential privacy breach in the following manner.

- When users enable the **Turn On Mute for Remote Off-hook Attempt** field on the station screen, any off-hook event on the desk phone turns on the **Mute** button.
- When the **Mute** button is active, the user cannot remotely hear conversations

This feature applies to Calls received or originated remotely from soft phones in a shared control mode and Calls received or originated remotely by using ASAI in H.323 configuration. The Communication Manager controls the signaling by activating the mute button for the off-hook event.

Use case scenario for endpoints set type

Change Set type of an Endpoint

To change **Set Type** of an **Endpoint** , for example to change from 9630SIP to 9641SIP, do one of the following:

- To change the **Set Type** of an **Endpoint**, default template or custom template of the **Set Type** to be updated can be applied from Endpoint editor, Global Endpoint change or User Management Communication profile section. This operation applies the values of templates in the end point fields and overwrites the values that you entered.
- To change the **Set Type** of an **Endpoint** and keep current data of endpoint such as **COR**, **COS**, **loss group**, do one of the following:
  - **Global Endpoint Change** For more information see Changing endpoint parameters globally.
  - **Element Cut Through** For more information see Element Cut Through.

Related links

Use Element Cut Through on page 680

Changing endpoint parameters globally on page 639

Configuring the Feature buttons

Adding a Feature button to the SIP endpoint

About this task

Use this procedure to add a Feature button to the SIP endpoint.

Before you begin

1. Select a set type of the SIP endpoint that supports the Feature button that you want to add.
2. For the SIP set type that you selected, configure the required endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide*.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. On the Endpoints page, click **New** to add a new endpoint.

   The system displays the New Endpoint page.
4. In the **Template** field, click the Communication Manager template that you configured for the set type of your SIP endpoint.
5. In the **Feature Options** tab:
   a. Enter the required configuration parameters.
   b. In the **Features** list, select the features for the SIP endpoint.
6. In the **Button Assignment** tab:
   a. Click **Feature Buttons**.
   b. In **Endpoint Configurations**, in the **Button Label** field, type a name for the button. For example, call pick up.
   c. In **Button Configurations**, in the **Button Feature** field, click the feature button that you want to add. For example, click **call— pkup**.
7. Click **Commit**.

   The SIP endpoint displays the **Feature** button that you added.

Adding the Call Pickup button on an endpoint

About this task

Use this procedure to specify the number of times that an endpoint must ring for call pick up. For example, System Manager7.0 supports a Triple Ringer.

Before you begin

1. Select a set type for your endpoint from the following:
   - 9620

- 9630
- 9640
- 9650
- 9608
- 9611
- 9621
- 9641

2. For the endpoint set type that you selected, configure the required endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide*.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. On the Endpoints page, click **New** to add a new endpoint.

   The system displays the New Endpoint page.
4. In the **Template** field, click the Communication Manager template that you configured for the set type of your SIP endpoint.
5. In the **Feature Options** tab:
   a. Enter the required configuration parameters.
   b. In the **Features** list, select the features for the SIP endpoint.
6. In the **Button Assignment** tab:
   a. Click **Feature Buttons**.
   b. In **Endpoint Configurations**, in the **Button Label** field, type `Call Pickup`.
   c. In **Button Configurations**, in the **Button Feature** field, click **call-pkup**.
   d. In the **Rg** field, type the number of times that the endpoint must ring for the call pickup: The options are: `continuous`, `if-busy-silent`, `if-busy-single`, `no-ring`, `single`,`triple`.
7. Click **Commit**.

   The endpoint displays the **Call Pickup** button that rings three successive times for call pick up.

Adding the Service Observe button on a SIP endpoint

About this task

Use this procedure to add the **Service Observe** button, which is useful in the Contact Center environment for managing and monitoring agent calls. You can add the **Service Observe** button on SIP endpoints in the following modes:

- **listen—only** : To monitor agent calls without interrupting the call
- **so-coach** : To coach an agent during the call

Before you begin

- Select a set type for your SIP endpoint from the following:
  - 9608SIPCC
  - 9611SIPCC
  - 9621SIPCC
  - 9641SIPCC
- You must configure the endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide* .

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. On the Endpoints page, click **New** to add a new endpoint.

   The system displays the New Endpoint page.
4. In the **Template** field, click the Communication Manager template that you configured for the set type of your SIP endpoint.
5. In the **Feature Options** tab:
   a. Enter the required configuration parameters.
   b. In the **Features** list, select the features for the SIP endpoint.
6. In the **Button Assignment** tab:
   a. Click **Feature Buttons**.
   b. In **Endpoint Configurations**, in the **Button Label** field, type `Service Observe`.
   c. In **Button Configurations**, in the **Button Feature** field, click **sip-sobsv** mode. The options are:
      - **listen-only**
      - **so-coach**
7. Click **Commit**.

   The endpoint displays the **Service Observe** button that you added.

Adding the VOA Repeat button on a SIP endpoint

Before you begin

- Select a set type for your SIP endpoint from the following:
  - 9608SIPCC
  - 9611SIPCC
  - 9621SIPCC
  - 9641SIPCC
- Configure the required endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide* .

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. On the Endpoints page, click **New** to add a new endpoint.

   The system displays the New Endpoint page.
4. In the **Template** field, click the Communication Manager template that you configured for the set type of your SIP endpoint.
5. In the **Feature Options** tab:
   a. Enter the required configuration parameters.
   b. In the **Features** list, select the features for the SIP endpoint.
6. In the **Button Assignment** tab:
   a. Click **Feature Buttons**.
   b. In **Endpoint Configurations**, in the **Button Label** field, type `VOA Repeat`.
   c. In **Button Configurations**, in the **Button Feature** field, click **VOA Repeat**.
7. Click **Commit**.

   The endpoint displays the **VOA Repeat** button that you added.

Adding an Agent skill on a SIP endpoint

Before you begin

1. Select a set type for your SIP endpoint from the following:
   - 9608SIPCC
   - 9611SIPCC
   - 9621SIPCC
   - 9641SIPCC
2. Configure the required endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide* .

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. On the Endpoints page, click **New** to add a new endpoint.

   The system displays the New Endpoint page.
4. In the **Template** field, click the Communication Manager template that you configured for the set type of your SIP endpoint.
5. In the **Feature Options** tab:
   a. Enter the required configuration parameters.
   b. In the **Features** list, select the features for the SIP endpoint.
6. In the **Button Assignment** tab:
   a. Click **Feature Buttons**.
   b. In **Endpoint Configurations**, in the **Button Label** field, type a name for the agent skill.
   c. In **Button Configurations**, in the **Button Feature** field, click **add-rem-sk**.
7. Click **Commit**.

   The SIP endpoint displays the agent skill that you added.

Creating a Single Administration Dual Registration endpoint

Before you begin

1. Select a set type for your endpoint from the following:
   - 9608
   - 9610
   - 9611
   - 9620
   - 9621
   - 9630
   - 9641
   - 9650

   Note:

   The system enables the **Allow H.323 and SIP Endpoint Dual Registration** field only for the set types mentioned in the list.
2. For the endpoint set type that you selected, configure the required endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide*.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **New**.
4. On the New User Profile page, do the following:
    a. Click **Communication Profile** > **CM Endpoint Profile**.
    b. In the **Set Type** field, click the endpoint set type that you want to add.

       For example, click **9608**.
    c. Select **Allow H.323 and SIP Endpoint Dual Registration** .

    For more information, see *CM Endpoint Profile field descriptions*.
5. Click **Commit**.

Enabling Reachability on a SIP endpoint

Before you begin

1. Select a set type for your SIP endpoint from the following:
    - 9608SIP
    - 9611SIP
    - 9621SIP
    - 9641SIP
    - 9608SIPCC
    - 9611SIPCC
    - 9621SIPCC
    - 9641SIPCC
2. Configure the required endpoint template on Communication Manager. For more information, see *Administering Communication ManagerGuide*.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. On the Endpoints page, click **New** to add a new endpoint.

    The system displays the New Endpoint page.
4. In the **Template** field, click the Communication Manager template that you configured for the set type of your SIP endpoint.
5. In the General Options tab, perform the following:
    a. In the **Reachability** field, click **System**.

   b. Select the **Enable Reachability for Domain Control SIP Stations** check box.

6. Click **Commit**.

Use Element Cut Through

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Select the Communication Manager endpoint, click **Switch to Classic View** > **Edit**.
5. On the Element Cut Through page, select **Set Type** to update the template.
6. Click **Enter** to commit the endpoint update.

   The updated endpoint is in sync with the System Manager.

Managing Off PBX Configuration Set

Viewing Off PBX Configuration Set

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Off PBX Telephone** > **Off PBX Configuration Set**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Off PBX Configuration Set list, select the Off PBX Configuration Set you want to view.
6. Click **View**.

   You can view the details of the Off PBX Configuration Set through the classic view.

Editing Off PBX Configuration Set

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Off PBX Telephone** > **Off PBX Configuration Set**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.

5. From the Off PBX Configuration Set list, select the Off PBX Configuration Set you want to edit.
6. Click **Edit**.

   You can edit the Off PBX Configuration Set details through the classic view.
7. To save the changes, click **Enter**.

Off PBX Configuration Set field descriptions

Name	Description
Number	The Off PBX endpoint configuration set number.
Description	Description of the Off PBX endpoint configuration set. The description field can also specify the name of the Off PBX Configuration Set.
Calling Number Style	Determines the format of the caller ID for calls from a local Communication Manager extension to an extension to a cellular telephone. The possible values are: • **Network**: Provides a display of only 10-digit numbers. For internal calls, the ISDN numbering tables are used to create the calling number. DCS calls use the ISDN calling number, if provided. Externally provided calling numbers are used for externally originated calls. • **Port**: Provides a display of less than 10-digits. Extensions are sent as the calling number for all internal and DCS network-originated calls.
CDR Origination	Determines the Call Detail Record (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 excludes dialed Feature Name Extensions (FNEs). The possible values are: • **phone-number**: The calling party on the CDR report is the 10-digit cell phone number. This is the default value. • **extension**: The calling party on the CDR report is the internal office telephone extension associated with the Extension to Cellular cell phone. • **none**: The system does not generate an originating CDR report.
CDR EC500	Determines whether a CDR is generated for any call to the cellular telephone. Available only if CDR

Table continues…

Name	Description
	reports are enabled for the trunk group. The possible values are: • **true**: Treats calls to the XMOBILE station as trunk calls and generates a CDR. • **false**: Treats calls to the XMOBILE station as internal calls, without generating a CDR.
Fast Conn	Determines whether additional processing occurs on the server running Communication Manager prior to connecting a call. Fast Conn is reserved for future that the cell telephone provider might provide.
Post Conn	Determines whether additional capabilities, beyond standard ISDN dialing, are available for those incoming ISDN trunk calls that are mapped to XMOBILE endpoints. Post Conn options come into effect after the call has entered the active state. The possible values are: • **dtmf**: Expect digits from either in-band or out-of-band, but not simultaneously. The server allocates a DTMF receiver whenever the server needs to collect digits. This option is normally used for Extension to Cellular XMOBILE endpoint calls. • **out-of-band**: Expect all digits delivered by out-of-band signaling only. The server running Communication Manager collects digits from the out-of-band channel or no touch-tone receiver. In addition, any digits received when the server is not collecting digits are converted to DTMF and is broadcast to all the parties on the call. This option is implemented for DECT XMOBILE endpoint 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 in-band signaling consists of DTMF in the voice path. The server running Communication Manager collects all the digits from the out-of-band channel. To prevent double digit collection, touch tone receive is not allocated. End-to-end signaling occurs transparently to the server through in-band transmission of DTMF. This option is implemented for PHS XMOBILE endpoint calls.
Voice Mail Dest	Voice Mail Dest prevents cellular voice mail from answering an Extension to Cellular call. When the call server detects that the cell phone is not the entity

Table continues…

Name	Description
	answering the call, the call server brings the call back to the server. The possible values are: • **none**: No restrictions on cellular voice mail. This is the default value. • **timed**: When you enter timed, the system displays the seconds field, which accepts values from 1 to 9. The default value is 4 seconds. In the Extension to Cellular-enabled environment, if you answer the call at the cell within the configured time, Communication Manager treats the call as a call that the cellular voice mail answers, and disconnects the cellular leg of the call. The call continues to ring at the desk phone. You can use this configuration for any type of network, including GSM, CDMA, and ISDN. • **message**: The message option works with carriers who use non-ISDN voice mail systems. You must not use this option with ISDN-based voice mail systems.
System	The name of the Communication Manager system.

Button	Description
View	Click to view the details of the Off PBX Configuration Set.
Edit	Click to edit the Off PBX Configuration Set.

Managing Off PBX Endpoint Mapping

Adding Off PBX Endpoint Mapping to an endpoint

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Off PBX Telephone** > **Off PBX Endpoint Mapping**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Add Off PBX Endpoint Mapping through the SAT screen.
7. Click **Enter**.

Viewing the Off PBX Endpoint Mapping

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Off PBX Telephone** > **Off PBX Endpoint Mapping**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the Off PBX Endpoint Mapping that you want to view.
6. Click **View**.

   The system displays the details of the Off PBX Endpoint Mapping from the classic view.

Editing the Off PBX Endpoint Mapping of an endpoint

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Off PBX Telephone** > **Off PBX Endpoint Mapping**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the Off PBX Endpoint Mapping you want to edit.
6. Click **Edit**.
7. Edit the required fields through the SAT screen.
8. To save the changes, click **Enter**.

Off PBX Endpoint Mapping field descriptions

Name	Description
Endpoint Extension	The SIP and non-SIP extensions that have Off PBX Endpoint Mapping. When you add a SIP endpoint, an entry for this endpoint is automatically available in Off PBX Endpoint Mapping. To add an endpoint mapping to a non-SIP endpoint, you must manually add an Off PBX Endpoint Mapping for that endpoint.
System	The Communication Manager system in which the endpoint extension is available.

Button	Description
New	Adds an Off PBX Endpoint mapping.
View	Displays an Off PBX mapping for an endpoint.
Edit	Edits an Off PBX Endpoint mapping.

Xmobile Configuration

Xmobile Configuration

Xmobile Configuration defines the 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.

Xmobile Configuration List

Xmobile Configuration List displays the Xmobile Configuration details under the Communication Manager you select. You can apply filters and sort each column in this list.

Click **Refresh** to view the updated information after the last synchronization.

Name	Description
Configuration Set	The configuration set value.
Calling No.	The format of the caller ID for calls from a local switch extension to an EC500 cell phone.
CDR Orig	The CDR report format when CDR records are generated for a call that originates from an Extension to Cellular cell phone.
CDR EC 500	Displays whether a call detail record is generated for any call to the cell phone.
Fast Conn	Displays whether some additional processing occurs on the switch prior to connecting a call.
Post-Connect Dialing	Displays whether additional capabilities, beyond standard ISDN dialing, are available for those incoming ISDN trunk calls that are mapped into XMOBILE stations.
System	The name of the Communication Manager associated with the Xmobile Configuration set.

Viewing Xmobile Configuration data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Xmobile Configuration**.
3. Select a Communication Manager instance from the Communication Manager list.

4. Click **Show List**.
5. From the Xmobile Configuration List, select the configuration set you want to view.
6. Click **View**.

Related links

Xmobile Configuration field descriptions on page 686

Editing Xmobile Configuration

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Endpoints** > **Xmobile Configuration**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Xmobile Configuration List, select the configuration set you want to view.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required details on the **Edit Xmobile Configuration Data** page.
8. Click **Commit** to save the changes.

Related links

Xmobile Configuration field descriptions on page 686

Xmobile Configuration field descriptions

Field	Description
Barge-in Tone	Enables 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.
Calling Number Style	Determines the format of the caller ID for calls from a local switch extension to an EC500 cell phone. • **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.

Table continues…

Field	Description
CDR for Calls to EC500 Destination	Determines whether a call detail record is generated for calls to the cell phone. **Note:** CDR reporting for EC500 calls relies on the CDR Reports field on the Trunk Group screen. If, on the Trunk Group screen, the CDR Reports field is set to **n**, no CDR is generated even if this field is set to **y**. • **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 not generate a CDR.
Configuration Set Description	Describes the purpose of the configuration set. A valid entry is up to 20 alphanumeric characters or blank. For example, EC500 handsets.
Fast Connect on Origination	Determines whether some additional processing occurs on the switch prior to connecting a call. You can use the **y** option to send CONNECT messages.
Post-Conn Signaling	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 when the switch has sent a CONNECT message back to the network. • **dtmf**: Expect digits from either in-band or out-of-band, but not simultaneously. The switch allocates a DTMF receiver whenever it needs to collect digits. This option is generally used for EC500 XMOBILE station calls. • **out-of-band**: Expect all digits to be delivered by out-of-band signaling only. The switch collects digits that it needs from the out-of-band channel (no touch-tone receiver). In addition, any digits received when the switch 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 to be 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 switch collects all digits that it needs from the out-

Table continues…

Field	Description
	of-band channel. No touch tone receive is allocated in order to prevent collecting double digits. End-to-end signaling occurs transparently to the switch through in-band transmission of DTMF. This option is in force for PHS XMOBILE station calls.
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. • **first-available**: The system searches for the first available regular or bridged Call Appearance. • **primary-first**: Only regular Call Appearances are used for call origination. If a regular call appearance is not available, the call is not allowed. 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. This is the default setting.
Calling Number Verification	Enables restrictions on the types of calls made to a cell phone with Extension to Cellular. • **y**: Prevents all calls, except for the following calls, from reaching the cell phone: - Network-provided - User-provided - Passed This setting has no effect on normal usage of the Extension to Cellular feature. This is the default setting. • **n**: No restrictions on calls to the cell phone.
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). • **phone-number**: The calling party on the CDR report is the 10-digit cell phone number. This is the default setting. • **extension**: The calling party on the CDR report is the internal office telephone phone extension

Table continues…

Field	Description
	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. • **none**: No restrictions on cellular voice mail. This is the default setting. • **timed**: Amount of time from 1 to 9 seconds. The default time 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 continues to ring at the office telephone. If unanswered, it will go to the corporate voice mail. This setting can be used for different types of network that is, GSM, CDMA, and ISDN. • **message**: The message option works with carriers who use non ISDN voice mail systems. Avoid using this option with ISDN-based voice mail systems.
Confirmed Answer	Enables Confirmed Answer on Extension to Cellular calls for this station. If you select this option, the user needs to input a digit to confirm receipt of a call sent to a cell phone using the Extension to Cellular feature. When the user answers the incoming call on the cell phone, the user hears a dial tone. The user must then press any one of the digits on the cell phone 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 phone 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 telephone device.

Table continues…

Field	Description
Configuration Set ID	The configuration set value that you selected in the Xmobile Configuration List. This is a display-only field.

Button	Description
Commit	Completes the action you initiate.
Schedule	Performs the action at the chosen time.
Reset	Clears the action and resets the field.
Clear	Clears all the entries.
Edit	Allows you to edit the fields in the page.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Automatic Alternate Routing Digit Conversion

AAR/ARS Digit Conversion

Use the Automatic Alternate Routing (AAR) Digit Conversion or Automatic Route Selection (ARS) Digit Conversion capability to configure your system to change a dialed number for efficient routing by inserting or deleting digits from the dialed number. For instance, you can configure the server running Communication Manager to delete **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.

Viewing Automatic Alternate Routing Digit Conversion data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Automatic Alternate Routing Digit Conversion**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the AAR Digit Conversion List, select the Automatic Alternate Routing Digit Conversion data you want to view.
6. Click **View**.

Related links

AAR/ARS Digit Conversion field descriptions on page 691

Editing Automatic Alternate Routing Digit Conversion data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Automatic Alternate Routing Digit Conversion**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the AAR Digit Conversion List, select the Automatic Alternate Routing Digit Conversion you want to edit.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit AAR Digit Conversion** page.
8. Click **Commit** to save the changes.

Related links

AAR/ARS Digit Conversion field descriptions on page 691

AAR/ARS Digit Conversion field descriptions

Field	Description
ANI Required	This field applies only if the Request Incoming ANI (non-AAR/ARS) field on the Multifrequency-Signaling-Related System Parameters screen is set to `n`. • **y** or **n**: Enter `y` to require ANI on incoming R2-MFC or Russian MF ANI calls. The entry must be set to `y` to enable EC500 origination features. • **r**: Restricted. Allowed only if the Allow ANI Restriction on AAR/ARS field is set to `y` on the Feature-Related System Parameters screen. Use this entry to drop a call on a Russian Shuttle trunk or Russian Rotary trunk if the ANI request fails. Other types of trunks treat **r** as **y**.
Conv	Provides the option to allow additional digit conversion.
Del	The number of digits you want the system to delete from the beginning of the dialed string. A valid entry ranges from **0** to **Min**.
Location	This is a display-only field. Typing the command `change aar digit-conversion` *n* or `change ars digit-conversion` *n* displays the all-locations screen, and populates this field with **all**.

Table continues…

Field	Description
	The *n* specifies that dialed strings beginning with the value *n* are displayed first. To access a per-location screen, type change `aar digit-conversion location` *`n`* or `change ars digit-conversion location` *`n`*, where *n* represents the number of a specific location. This field then displays the number of the specified location. For details on command options, see online help, or *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431. One of the following is a valid entry: • **1** to **64**: Specifies whether you require ANI on incoming R2-MFC or Russian MF ANI calls. Entry must be `y` to enable EC500 origination features. • **all**: Indicates that this AAR/ARS Digit Conversion Table is the default for all port network (cabinet) locations.
Matching Pattern	Specifies the number you want the server running Communication Manager to match to dialed numbers. If a prefix digit **1** is required for 10-digit direct distance dialing (DDD) numbers, be sure the matching pattern begins with a 1. A valid entry is a number ranging from **0** to **9** (1 to 18 digits) and wildcard characters asterisk (*****), **x**, and **X**.
Max	The maximum number of user-dialed digits the system collects to match to this Matching Pattern. A valid entry ranges from **Min** to **28**.
Min	The minimum number of user-dialed digits the system collects to match to this Matching Pattern. A valid entry ranges from **1** to **Max**.
Net	The call-processing server network used to analyze the converted number. The entries **ext**, **aar**, or **ars** analyze the converted digit-string as an extension number, an AAR address, or an ARS address.
Percent Full	Displays the percentage from **0** to **100** of the system memory resources that have been used by ARS. If the figure is close to 100 percent, you can free-up memory resources.
Replacement String	A valid entry ranges from **0** to **9** (1 to 18 digits), asterisk (*****), pound (**#**), or blank. Enter the digits that replace the deleted portion of the dialed number. If the pound character (**#**) is present in the string, it should be the last character in the string. This signifies the end of the modified digit string.

Table continues…

Field	Description
	Leave this field blank to simply delete the digits.

Button	Description
Commit	Completes the action you initiate.
Schedule	Performs the action at the chosen time.
Reset	Clears the action and resets the field.
Clear	Clears all the entries.
Edit	Allows you to edit the fields in the page.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Automatic Route Selection Digit Conversion

AAR/ARS Digit Conversion

Use the Automatic Alternate Routing (AAR) Digit Conversion or Automatic Route Selection (ARS) Digit Conversion capability to configure your system to change a dialed number for efficient routing by inserting or deleting digits from the dialed number. For instance, you can configure the server running Communication Manager to delete **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.

Viewing Automatic Route Selection Digit Conversion data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Automatic Route Selection Digit Conversion**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the ARS Digit Conversion List, select the Automatic Route Selection Digit Conversion you want to view.
6. Click **View**.

Related links

AAR/ARS Digit Conversion field descriptions on page 691

Editing Automatic Route Selection Digit Conversion data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Automatic Route Selection Digit Conversion**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Edit** or click **View** > **Edit**.
6. Edit the required fields on the **Edit ARS Digit Conversion** page.
7. Click **Commit** to save the changes.

Related links

AAR/ARS Digit Conversion field descriptions on page 691

AAR/ARS Digit Conversion field descriptions

Field	Description
ANI Required	This field applies only if the Request Incoming ANI (non-AAR/ARS) field on the Multifrequency-Signaling-Related System Parameters screen is set to `n`. • **y** or **n**: Enter `y` to require ANI on incoming R2-MFC or Russian MF ANI calls. The entry must be set to `y` to enable EC500 origination features. • **r**: Restricted. Allowed only if the Allow ANI Restriction on AAR/ARS field is set to `y` on the Feature-Related System Parameters screen. Use this entry to drop a call on a Russian Shuttle trunk or Russian Rotary trunk if the ANI request fails. Other types of trunks treat **r** as **y**.
Conv	Provides the option to allow additional digit conversion.
Del	The number of digits you want the system to delete from the beginning of the dialed string. A valid entry ranges from **0** to **Min**.
Location	This is a display-only field. Typing the command `change aar digit-conversion` *`n`* or `change ars digit-conversion` *`n`* displays the all-locations screen, and populates this field with **all**. The *n* specifies that dialed strings beginning with the value *n* are displayed first. To access a per-location screen, type change `aar digit-conversion location` *`n`* or `change ars digit-conversion location` *`n`*, where *n* represents the

Table continues…

Field	Description
	number of a specific location. This field then displays the number of the specified location. For details on command options, see online help, or *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers*, 03-300431. One of the following is a valid entry: • **1** to **64**: Specifies whether you require ANI on incoming R2-MFC or Russian MF ANI calls. Entry must be `y` to enable EC500 origination features. • **all**: Indicates that this AAR/ARS Digit Conversion Table is the default for all port network (cabinet) locations.
Matching Pattern	Specifies the number you want the server running Communication Manager to match to dialed numbers. If a prefix digit **1** is required for 10-digit direct distance dialing (DDD) numbers, be sure the matching pattern begins with a 1. A valid entry is a number ranging from **0** to **9** (1 to 18 digits) and wildcard characters asterisk (*****), **x**, and **X**.
Max	The maximum number of user-dialed digits the system collects to match to this Matching Pattern. A valid entry ranges from **Min** to **28**.
Min	The minimum number of user-dialed digits the system collects to match to this Matching Pattern. A valid entry ranges from **1** to **Max**.
Net	The call-processing server network used to analyze the converted number. The entries **ext**, **aar**, or **ars** analyze the converted digit-string as an extension number, an AAR address, or an ARS address.
Percent Full	Displays the percentage from **0** to **100** of the system memory resources that have been used by ARS. If the figure is close to 100 percent, you can free-up memory resources.
Replacement String	A valid entry ranges from **0** to **9** (1 to 18 digits), asterisk (*****), pound (**#**), or blank. Enter the digits that replace the deleted portion of the dialed number. If the pound character (**#**) is present in the string, it should be the last character in the string. This signifies the end of the modified digit string. Leave this field blank to simply delete the digits.

Button	Description
Commit	Completes the action you initiate.

Table continues…

Button	Description
Schedule	Performs the action at the chosen time.
Reset	Clears the action and resets the field.
Clear	Clears all the entries.
Edit	Allows you to edit the fields in the page.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Automatic Route Selection Toll

Automatic Route Selection Toll

With Automatic Route Selection Toll, you can specify whether calls to CO codes listed on the table are toll or non-toll calls. You can specify non-toll calls based on the last two digits of the distant-end of the trunk group.

Automatic Route Selection Toll List

Name	Description
ARS Toll Table	The Automatic Route Selection Toll table number.
From Office Code, **To Office Code**	The block of numbers for the associated Automatic Route Selection Toll table.
System	The name of the Communication Manager associated with the Automatic Route Selection Toll table.

Viewing Automatic Route Selection Toll data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Automatic Route Selection Toll**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Automatic Route Selection Toll List, select the Ars Toll Table you want to view.
6. Click **View**.

Related links

Automatic Route Selection Toll field descriptions on page 697

Editing Automatic Route Selection Toll data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Automatic Route Selection Toll**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Automatic Route Selection Toll List, select the Ars Toll Table you want to edit.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Automatic Route Selection Toll** page.
8. Click **Commit** to save the changes.

Related links

Automatic Route Selection Toll field descriptions on page 697

Automatic Route Selection Toll field descriptions

Name	Description
00: through **99:**	The last two digits of the codes within the 100-block of numbers. Designate each as a number toll or non-toll call.
Ars Toll Table	The number of the ARS Toll table. Valid entry ranges from **2** through **9**.
Office Codes	The block of numbers. Valid entry ranges from **200** to **299** through **900** to **999**.

Button	Description
Commit	Performs the action you initiate.
Schedule	Performs the action at the specified time.
Reset	Clears the action and resets the fields.
Clear	Clears all entries.
Done	Completes your current action and navigates to the subsequent page.
Cancel	Cancels your current action and navigates to the previous page.
Backup	Backs up the audio files that you select.
Now	Performs the action you initiate real time.

Data Modules

Data Modules

Use this capability to connect systems running Communication Manager with other communications equipment, changing protocol, connections, and timing as necessary. Communication Manager supports the following types of data modules:

- High speed links
- Data stands
- Modular-processor data module
- 7000-series data modules
- Modular-trunk data module
- Asynchronous Data Unit
- Asynchronous Data Module for ISDN-Basic Rate Interface telephones
- Terminal adapters

All of these data modules support industry standards and include options for setting the operating profile to match that of the data equipment.

Data Module List

Data Module List displays all the data modules under the Communication Manager you select. You can apply filters and sort each column in the Data Module List.

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

Name	Description
Extension	The extension assigned to the data module.
Port	The port location to which the selected data module is connected.
Type	The type of data module.
Name	The name of the user associated with the data module.
COS	The desired Class Of Service.
COR	The desired Class Of Restriction.
TN	The tenant number which determines the music source for callers on hold.
ISN	Information Systems Network. Used with Data Line and Processor/Trunk Data Modules.

Table continues…

Name	Description
System	The name of the Communication Manager associated with the data module.

Adding a Data Module

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Data Modules**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select **New**.
6. Complete the **Add Data Module** page and click **Commit**.

Related links

Data Modules field descriptions on page 700

Viewing a Data Module

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Data Modules**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Data Modules List, select the data module you want to view.
6. Click **View**.

Related links

Data Modules field descriptions on page 700

Editing a Data Module

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Data Modules**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Data Modules List, select the data module you want to edit.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Data Modules** page.

8. Click **Commit** to save the changes.

Related links

Data Modules field descriptions on page 700

Deleting Data Modules

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Data Modules**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Data Modules List, select the data modules you want to delete.
6. Click **Delete**.
7. Confirm to delete the data modules.

Related links

Data Modules field descriptions on page 700

Data Modules field descriptions

Field	Description
List Type	Indicates whether the type of list is group, personal, enhanced, or system type.
Special Dialing Option	Identifies the destination of all calls when this data module originates calls. The available dialing options are: • **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.
Personal/Group Number	The identifying number the server running Communication Manager assigns to the group when it is created.
Abbreviated Dialing Dial Code (From above list)	Used with 7500, Data Line, Netcon, Processor/ Trunk, Processor Interface, and World Class BRI Data Modules. System displays this field only when the Special Dialing Option field is default. When the user goes off-hook and enters a carriage return following the DIAL prompt, the system dials the abbreviated dialing number. The data call originator

Table continues…

Field	Description
	can also perform data-terminal dialing by specifying a dial string that may or may not contain alphanumeric names. Valid entry ranges from **0** through **999**. You need to enter a list number associated with the abbreviated dialing list.
BCC	Bearer Capability Class. A display-only field used with Data Line, Netcon, Processor Interface, Point-to-Point Protocol, Processor/Trunk (pdm selection), and System Port Data Modules. Appears when the ISDN-PRI or ISDN-BRI Trunks field is set to `y` on the System Parameters Customer-Options (Optional Features) screen. The value in this field corresponds to the speed setting of the data module. 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. See *Generalized Route Selection in Avaya Aura™ Communication Manager Feature Description and Implementation*, 555-245-205, for a detailed description of Bearer Capability Classes (BCC) and their ability to provide specialized routing for various types of voice and data calls. The BCC value is used to determine compatibility when non-ISDN-PRI facilities are connected to ISDN facilities (ISDN-PRI Interworking). The valid entries are: • **1**: Relates to 56-bkps • **2**, **3**, **4**: Relates to 64 kbps
Broadcast Address	Used with Ethernet data modules. Does not appear for S87XX Series IP-PNC.
Connected Data Module	This is the data module extension to which the link connects. Used with Processor Interface (used with DEFINITY CSI only) data modules.
Connected to	The Asynchronous Data Unit (ADU) to which the system is connected to. Used with Data Line and Processor/Trunk (pdm selection) Data Module. The valid entries are: • **dte**: Data Terminal Equipment. Used with Data Line and Processor/Trunk Data Modules. • **isn**: Information Systems Network. Used with Data Line and Processor/Trunk Data Modules.

Table continues…

Field	Description
Class Of Service	The desired class of service. Does not appear for Ethernet. The valid entries range from **0** to **15** to select the allowed features
Class Of Restriction	The desired class of restriction. Does not appear for Ethernet. The valid entries range from **0** to **999** to select the allowed restrictions.
Extension	Indicates the extension assigned to the data module. This is a display-only field.
Enable Link	Used with Point-to-Point and Processor Interface data modules.
Establish Connection	Used with Point-to-Point, and Processor Interface (used with DEFINITY CSI only) data modules.
IP Address Negotiation	Used with Point-to-Point data modules. Does not appear for S87XX Series IP-PNC.
ITC	Information Transfer Capability. Indicates type of transmission facilities to be used for ISDN calls originated from this endpoint. Appears only when, on the Trunk Group screen, the Comm Type field is 56k-data or 64k-data. Does not display for voice-only or BRI stations. Used with 7500, Announcement, data-line, Netcon, Processor/Trunk (pdm selection), Processor Interface, and System Port Data Modules. The valid entries are: • **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 (that is, a sequence of eight digital zeros is 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 (that is, digital information is sent exactly as is).
Link	A communication interface link number. Used with Ethernet, Point-to-Point, and Processor Interface (used with DEFINITY CSI only) data modules. This field is in different locations on the screen for different data module types. The valid entries range from **0** to **99**.
Extension	The extension number required to perform maintenance functions on the standby Netcon physical channel in a duplicated system. The

Table continues…

Field	Description
	standby remote loop around tests fails if this field is not administered. Used with Netcon and Processor Interface Data Modules.
MM Complex Voice Ext	This field contains the number of the associated telephone in the multimedia complex. This field appears only after you set the Multimedia field to`y`. This field is left blank until you enter the data module extension in MM Complex Data Ext on the Station screen. Used with 7500 and World Class BRI Data Modules. Does not appear on S87XX Series IP-PNC. Valid entries are valid values that conform to your dial plan. After you complete the field on the Station screen, the two extensions are associated as two parts of a one-number complex, which is the extension of the telephone.
Multimedia	Used with the 7500 and World Class BRI Data Modules. Appears only if, on the System Parameters Customer-Options (Optional Features) screen, the MM field is `y`. You can select this option to make this data module part of a multimedia complex.
Name	The name of the user associated with the data module. The name is optional and can be blank. It can contain up to 27 alphanumeric characters. **Note:** Avaya BRI stations support ASCII characters only. BRI stations do not support non-ASCII characters, such as Eurofont or Kanafont. Therefore, if you use non-ASCII characters in any Communication Manager Name field, such characters do not display correctly on a BRI station.
Network uses 1's for Broadcast Addresses	Indicates that a broadcast address is used to send the same message to all systems or clients on a local area network. Used with Ethernet data modules.
Node Name	Appears when the Data Module type is ppp. Used with Ethernet (not on S87XX Series IP-PNC) and Point-to-Point data modules.
PDATA Port	Used to relate the physical PDATA port to which the mode 3 portion of the system port is connected. You need to enter a seven-digit alphanumeric port location to which the data module is connected. This entry must be assigned to a port on a PDATA Line Board. Used with System Port Data Modules.

Table continues…

Field	Description
	The valid entries are: • **01** to **22**: First and second characters are the cabinet numbers • **01** to **64**: First and second characters are the cabinet numbers (S87XX Series IP-PNC) • **A** to **E**: Third character is the carrier • **01** to **20**: Fourth and fifth characters are the slot numbers in the carrier • **01** to **12**: Sixth and seventh characters are the circuit numbers
Physical Channel	The Physical Channel number is referred to on associated system forms as the Interface Link number. Used with Netcon and Processor Interface Data Modules. The valid entries are: • **01** to **08**: For Processor Interface Data Modules, enter the 2-digit circuit number of the Processor Interface port. A multi-carrier cabinet system supports the use of two Processor Interface circuit packs, the first circuit pack (mounted in Control Carrier A) supports physical channels or links 01through 04; the second (mounted in Control Carrier A) supports physical channels or links 05 through 08. A single-carrier cabinet system supports one Processor Interface circuit pack and physical channels or links 01 through 04 only. • **01** to **04**: For DEFINITY CSI configurations. For Netcon Data Modules, enter a netcon data channel.
Remote Loop-Around Test	Indicates whether data module supports a loop-back test at the EIA interface. Appears when the Data Module Type field is set to `pdm` or `tdm`. Used with Processor/Trunk Data Modules. In general, Avaya equipment supports this test but it is not required by Level 2 Digital Communications Protocol. To abort a request for this test, you may clear this check box.
Secondary Data Module	Indicates that this PDM is the secondary data module used for Dual I-channel AUDIX networking. Appears only when the Type field is `pdm`. Used with Processor/Trunk Data Modules. The primary data module must be administered before the secondary data module can be added. If the Port field entry is`x`,

Table continues…

Field	Description
	then do not select the Secondary Data Module option.
Subnet Mask	A 32-bit binary number that divides the network ID and the host ID in an IP address. Used with Point-to-Point data modules (for S87XX Series IP-PNC).
Tenant Number	Determines the music source for callers on hold. Valid entries range from **0** through **100**.

Board: Displays the five-character announcement circuit pack number that identifies the physical circuit pack to which the announcement module is connected. You can enter x in this field to indicate that there is no hardware associated with this port assignment. Used with Announcement Data Modules.

The five-character announcement board number consists of:

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 or X	**0** to **20**

Port: Specifies 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.

Note:

You can enter x in the Port field to indicate 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, that is secondary data module is set to y, you cannot enter x in this field. You cannot change the port of a primary data module to x if a secondary data module is administered.

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**
6 to **7**	Circuit Number	• **01** to **31** (S87XX Series IP-PNC (tdm, pdm) configurations) • **01** to **16** (ppp for S87XX Series IP-PNC) • **01** to **08** (system-port for S87XX Series IP-PNC) • **17/33** (Ethernet on S87XX Series IP-PNC)

Data Module Type: Displays 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 and/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 and is administered using the Announcement Data Module screen. 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	Assigns a Data Line Data Module. The Data Line Data Module (DLDM) screen assigns 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. 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. The DLC has 8 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. The DLC connects the following EIA 232C equipment to the system: • Printers

Table continues…

	• Non-Intelligent Data Terminals • Intelligent Terminals, Personal Computers • Host Computers • Information Systems Network (ISN), RS-232C Local Area Networks (LANs), or other data switches
ethernet	The name associated with an endpoint. The name you enter displays on called telephones that have display capabilities. In some messaging applications, such as Communication Manager Messaging, you can enter the user name (last name first) and their extension to identify the telephone. The name you enter is also used for the integrated directory.
ni-bri	Assigns an NI-BRI Data Module.
pdm	Assigns a DCE interface for Processor/Trunk Data Modules. These screens assign Modular Processor Data Modules (MPDMs) and Modular Trunk Data Modules (MTDMs). One screen is required for assigning MPDMs (700D), 7400B, 7400D or 8400B Data Module, and another screen for MTDMs (700B, 700C, 700E, 7400A). One screen must be completed for each MPDM, 7400B, 7400D, 8400B or MTDM. 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.) 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.

Table continues…

ppp	Assigns a Point-to-Point Protocol data module. The PPP Data Module screen assigns 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. See *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504, for more information on Point-to-Point data modules.
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.

Button	Description
Commit	Performs the action you initiate.
Schedule	Performs the action at the specified time.
Reset	Clears the action and resets the fields.
Clear	Clears all entries.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

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

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. In the left navigation pane, click **System** > **Class of Service**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the Class Of Service that you want to edit.
6. Click **Edit** or **View** > **Edit**.

7. Edit the required fields and click **Commit** to save the changes.

Related links

Class of Service field descriptions on page 709

Viewing Class Of Service data

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. In the left navigation pane, click **System** > **Class of Service**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the Class Of Service you want to view.
6. Click **View** to view the Class Of Service data.

Related links

Class of Service field descriptions on page 709

Filtering the Class Of Service list

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. In the left navigation pane, click **System** > **Class of Service**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Filter: Enable** in the Class Of Service List.
6. Filter the list 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 options that match the filter criteria.

Class of Service field descriptions

Name	Description
System	The name of the Communication Manager associated with the Class of Service.
Number	The Class of Service number.

General options

Name	Description
Ad-hoc video conferencing	Enables Ad-hoc Video Conferencing, so that up to six users can participate in a video conference call.
Automatic Callback	Allows users to request Automatic Callback.
Automatic Exclusion	Allows a user to activate automatically Exclusion when they go off hook on an endpoint that has an assigned Exclusion button.
Buttonless Auto Exclusion	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 by administering a feature exclusion button. This feature relaxes the requirement to use a feature button.
Call Forwarding Busy / DA	Allows users to forward calls to any extension when the dialed extension is busy or does not answer.
Call Forwarding Enhanced	Allows users to designate different preferred destinations for forwarding calls that originate from internal and external callers.
Call Forwarding All Calls	Allows users to forward all calls to any extension.
Client Room	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.
Conference Tones	This feature provides the conference tone as long as three or more calls are in a conference call. 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.
Console Permissions	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: • Activate Automatic Wakeup for another extension • Activate and deactivate controlled restrictions for another extension or group of extensions

Table continues…

Name	Description
	• Activate and deactivate Do Not Disturb for another extension or group of extensions • Activate Call Forwarding for another extension • Add and remove agent skills • Record integrated announcements
Contact Closure Activation	Allows a user to open and close a contact closure relay.
Data Privacy	Isolates a data call from call waiting or other interruptions.
MOC Control	The option to assign administrative control on Microsoft Office Communicator (MOC) for either of the 0-15 entries on COS or COS Group objects. By default, this check box is clear.
Extended Forwarding All	Allows a user to administer call forwarding (for all calls) from a remote location.
Extended Forwarding Busy / DA	Allows this user to administer call forwarding (when the dialed extension is busy or does not answer) from a remote location.
Intra-Switch CDR	Administers extensions for which Intra-Switch CDR is enabled.
Masking CPN / Name Override	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).
Off-Hook Alert	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.
Personal Station Access (PSA)	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.
Priority Calling	Allows users to dial a feature access code to originate a priority call. Such calls ring differently and override send all calls, if active.
Priority IP Video	Allows priority video calling, where video calls have an increased likelihood of receiving bandwidth and

Table continues…

Name	Description
	can also be allocated a larger maximum bandwidth per call.
QSIG Call Offer Originations	Allows users to invoke QSIG Call Offer services.
Restrict Call Fwd-Off Net	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.
Trk-To-Trk Tranfer Override	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.
VIP Caller	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.
Match BCA Display to Principal	The format of the incoming calls on the bridged call appearances of a COS Group. The possible values are: • **y**: Displays the incoming call in the <calling name/ number> format • **n**: Displays the incoming call in the <calling name/ number> to <principal station> format.

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

Authorization Code

Authorization Code

Use authorization code to control the calling privileges of system users. Authorization codes extend control of calling privileges and enhance security for remote access callers. You can use authorization codes to:

- Override a facilities restriction level (FRL) that is assigned to an originating station or trunk
- Restrict individual incoming tie trunks and remote access trunks from accessing outgoing trunks

- Track Call Detail Recording (CDR) calls for cost allocation
- Provide additional security control

Authorization Code List

Authorization Code List displays all the authorization codes under the Communication Manager you select. You can apply filters and sort each column in the Authorization Code List.

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

Name	Description
Authorization Code	The authorization code, which is a combination of 4 to 13 digits.
Class of Restriction	The associated Class Of Restriction.
System	The name of the Communication Manager associated with the authorization code.

Viewing Authorization Code

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **System** > **Authorization Code**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Authorization Code List, select the authorization code you want to view.
6. Click **View**.

Related links

Authorization Code field descriptions on page 714

Editing Authorization Code

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **System** > **Authorization Code**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Authorization Code List, select the authorization code you want to edit.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Authorization Code** page.
8. Click **Commit** to save the changes.

Related links

Authorization Code field descriptions on page 714

Authorization Code field descriptions

Field	Description
Authorization Code	Displays a combination of 4 to 13 digits. The number of digits must agree with the number assigned to the Authorization Code Length field on the Feature-Related System Parameters screen. To enhance system security, choose Authorization Codes of 13 random digits.
COR	Displays the Class Of Restriction. Valid entry ranges from **0** to **95**. When a user dials the associated authorization code, this is the COR that the telephone or other facility will assume for that call.

Button	Description
Commit	Performs the action you initiate.
Schedule	Performs the action at the specified time.
Reset	Clears the action and resets the fields.
Clear	Clears all entries.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Class of Service Group

Class Of Service Group

With Class Of Service Group, you can view the list of up to 100 Class Of Service (COS) groups on the screen. You can also change the configuration of individual COS group properties and edit up to 15 COS options within a group.

Class Of Service Group List

Class Of Service Group List displays the groups of Class Of Service under the Communication Manager you select. You can apply filters and sort each of the columns in the Class Of Service Group List.

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

Name	Description
Group Number	The number of the Class Of Service group. The group number ranges from 1 to 100.
Group Name	The name of the Class Of Service group.
System	The name of the Communication Manager associated with the Class Of Service Group.

Viewing Class Of Service Group

You can view the list of up to 100 Class of Service (COS) groups on this screen.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **System** > **Class of Service Group**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Class Of Service Group List, select the group number for which you want to view the data.
6. Click **View**.

Related links

Class Of Service Group field descriptions on page 716

Editing Class Of Service Group

You can change the configuration of individual Class Of Service (COS) group properties and edit up to 15 COS options within a group on this screen.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **System** > **Class of Service Group**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Class Of Service Group List, select the group number for which you want to edit the data.
6. Click **Edit** or click **View** > **Edit**.
7. Edit the required fields on the **Edit Class Of Service Group Data** page.
8. Click **Commit** to save the changes.

Related links

Class Of Service Group field descriptions on page 716

Class Of Service Group field descriptions

Name	Description
System	The name of the Communication Manager associated with the Class Of Service.
Group Number	The Class Of Service number. The group number can range from **1** to **100**. This field appears when, on the System Parameters Customer-Options (Optional Features) screen, the **Tenant Partitioning** field is set to `y`.
Group Name	The name of the Class Of Service Group. This field appears when, on the System Parameters Customer-Options (Optional Features) screen, the **Tenant Partitioning** field is set to `y`.
Ad-hoc video conferencing	Enables the ad-hoc video conference capability. Six users can participate in a video conference call.
Automatic Callback	Allows users to request Automatic Callback.
Automatic Exclusion	Allows a user to activate automatically Exclusion when they go off hook on an endpoint that has an assigned Exclusion button.
Buttonless Auto Exclusion	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 by administering a feature exclusion button. This feature relaxes the requirement to use a feature button.
Call Forwarding Busy / DA	Allows users to forward calls to any extension when the dialed extension is busy or does not answer.
Call Forwarding Enhanced	Allows users to designate different preferred destinations for forwarding calls that originate from internal and external callers.
Call Forwarding All Calls	Allows users to forward all calls to any extension.
Client Room	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 COS for Client Room only when you have Hospitality Services and a Property Management System interface.
Conference Tones	This feature provides the conference tone as long as three or more calls are in a conference call. 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

Table continues…

Name	Description
	independently administered or customized on the Tone Generation screen.
Console Permissions	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: • Activate Automatic Wakeup for another extension • Activate and deactivate controlled restrictions for another extension or group of extensions • Activate and deactivate Do Not Disturb for another extension or group of extensions • Activate Call Forwarding for another extension • Add and remove agent skills • Record integrated announcements
Contact Closure Activation	Allows a user to open and close a contact closure relay.
Data Privacy	Isolates a data call from call waiting or other interruptions.
Extended Forwarding All	Allows a user to administer call forwarding for all calls from a remote location.
Extended Forwarding Busy / DA	Allows this user to administer call forwarding when the dialed extension is busy or does not answer from a remote location.
Intra-Switch CDR	Administers extensions for which Intra-Switch CDR is enabled.
Masking CPN / Name Override	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.
Off-Hook Alert	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.
Personal Station Access (PSA)	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

Table continues…

Name	Description
	Enterprise Mobility User (EMU) feature at other endpoints.
Priority Calling	Allows users to dial a feature access code to originate a priority call. Such calls ring differently and override Send All Calls, if active.
Priority IP Video	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.
QSIG Call Offer Originations	Allows users to invoke QSIG Call Offer services.
Restrict Call Fwd- Off Net	Restricts users from forwarding calls to the public network. For security reasons, this should be enabled for all COS except the ones you use for very special circumstances.
Trk-To-Trk Tranfer Override	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.
VIP Caller	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.
Match BCA Display to Principal	The format of the incoming calls on the bridged call appearances of a COS Group. The possible values are: • **y**: Displays the incoming call in the <calling name/number> format • **n**: Displays the incoming call in the <calling name/number> to <principal station> format.

Button	Description
Commit	Performs the action you initiate.
Schedule	Performs the action at the specified time.
Reset	Clears the action and resets the fields.
Clear	Clears all entries.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.
Now	Performs the action you initiate real time.

Uniform Dial Plan Groups

Uniform Dial Plan Group

A Uniform Dial Plan Group is a set of Communication Manager systems that use the Uniform Dialing Plan (UDP) feature. You can use the Uniform Dial Plan Groups capability in System Manager to create, view, modify, and delete uniform dial plan (UDP) groups.

Adding a Uniform Dial Plan Group

About this task

Use this page to create a new UDP Group. While creating a new UDP Group, make sure that the Communication Manager systems you select share common extension ranges.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. Click **System** > **Uniform Dial Plan Groups** in the left navigation pane.
3. On the UDP Groups page, click **New**.
4. On the Add UDP Group page, enter the name for the UDP Group you want to create in the **Group Name** field.
5. Select the **Auto Update All** check box if you want the UDP tables of every Communication Manager system that you add to this group to be updated automatically.
6. Select the **Create local UDP table entry** check box if you want to create a local entry automatically in the UDP table of the Communication Manager system when you add an endpoint to it.
7. Enter the required information in the fields under the **Group Members** and **Group Ranges** tabs.
8. Click **Commit**.
9. On the System Manager console, click **Groups & Roles** > **Groups** to verify that the system added the group with the same name and resources.

Related links

Add UDP Groups field descriptions on page 720

Editing a Uniform Dial Plan Group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. Click **System** > **Uniform Dial Plan Groups** in the left navigation pane.
3. On the UDP Groups page, select the UDP Group that you want to modify from the UDP Group List.

4. Click **Edit**.
5. On the Edit UDP Groups page, modify the required fields.
6. Click **Commit**.

Related links

Add UDP Groups field descriptions on page 720

Viewing a Uniform Dial Plan Group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. Click **System** > **Uniform Dial Plan Groups** in the left navigation pane.
3. On the UDP Groups page, select the UDP Group that you want to view from the UDP Group List.
4. Click **View**. The system displays the **View UDP Group** page.

Related links

Add UDP Groups field descriptions on page 720

Deleting a Uniform Dial Plan Group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. Click **System** > **Uniform Dial Plan Groups** in the left navigation pane.
3. On the UDP Groups page, select the UDP Group that you want to delete from the UDP Group List.
4. Click Delete.

Related links

Add UDP Groups field descriptions on page 720

Add UDP Groups field descriptions

Name	Description
Group Name	To enter a name for the UDP group that you want to create.
Auto Update All	To automatically update the UDP tables of every Communication Manager that you add to this group .
Create local UDP table entry	To create a local entry automatically in the UDP table of the Communication Manager system when you add an endpoint.

Group Members

Name	Description
CM Systems	A list of Communication Manager systems from which you can select the Communication Manager that you want to add to the new UDP Group. A UDP Group can contain 2 to 10 systems.
Add	The link to add one or more Communication Manager systems to the new UDP Group. Is this a field or a group member?
Element Name	The name of the Communication Manager system that you added to the UDP group. This field is view only.
Software Version	The version of the Communication Manager system that you added to the UDP group. This field is view only.
Remove	The link to remove the Communication Manager systems that you selected from the **CM Systems** field list.

Group Ranges

Name	Description
System Dial Plan	A list of a common range of extensions available on the Communication Manager systems that you selected in the Group Members tab.
From	The starting range of extension numbers. The first extension number in the range.
To	The closing range of extension number. The last extension number in the range.
Add	The link to add the specified range of extension numbers.

Group Range Configuration

Name	Description
Range	The range of extension numbers.
UDP Type	Enter the initials of the call-processing server network that the system uses to analyze the converted number. Valid entries are **aar**, **ars**, and **ext**. First describe what is UDP type.
Delete Digits	The number of digits that the software deletes before the software routes a call. Valid entries are **0** through **3**.
Node/Location#	The extension number portability (ENP) node number. Valid entries are **1** to **999**.

Table continues…

Name	Description
Insert Digits	The specific digits or the number of administered location prefix digits inserted before routing the call. Select one of the following: • 0 to 9 (1 to 4 digits): The digits that replace the deleted portion of the dialed number. • Lx (1 to 5): The variable x represents the number of digits between 1 and 5 and is the number of leading digits taken from the administered location prefix. These digits are followed by the dialed string. The number of digits in the location prefix must be more than x. • The field to specify the location prefix digits. Leave the Insert Digits field blank if you do not want to specify the location prefix digits.
Conv	The range configurations used to create the **Uniform Dial Plan** entries on Communication Manager when an extension in the common ranges is added.

Button	Description
Commit	Performs the action that you start. .
Clear	Clears all entries.
Cancel	Cancels the current action and reverts to the previous page.

Uniform Dial Plan

Uniform Dial Plan field descriptions

Name	Description
Matching Pattern	The number that the Communication Manager instance uses to match the dialed numbers. You can enter up to 18 digits in the **Matching Pattern** field. You can also enter wildcard characters like x and X.
Length	The length of the dialed string for each type of call.
Del	The number of digits the system must delete from the initial digits of the dialed string.

Table continues…

Name	Description
Insert Digits	The specific digits or number of administered location prefix digits inserted before routing the call. Select one of the following: • **0 to 9 (1 to 4 digits)**: The digits that replace the deleted portion of the dialed number. • **Lx (1 to 5)**: The variable x represents the number of digits between 1 and 5 and is the number of leading digits taken from the administered location prefix. These digits are followed by the dialed string. x must be less than the number of digits in the location prefix. • **blank**: Leave the **Insert Digits** field blank if you do not want to specify the location prefix digits.
Net	The method that the call-processing server network uses to analyze the converted number. Select one of the following: • **ext**: If you use this option, the call-processing server network analyzes the converted digit-string as an extension number. • **aar**: If you use this option, the call-processing server network analyzes the converted digit-string as an AAR address. • **ars**: If you use this option, the call-processing server network analyzes the converted digit-string as an ARS address.
Conv	The field that enables additional digital conversion.
Node Number	The destination node number in a private network when the system uses node number routing or Distributed Communication System (DCS). The possible values are: • **blank**: Use this option if you do not want to enter the destination node number. This is the default option. • **1 to 999**: Use this option to enter the destination node number.
System	The name of the Communication Manager system.

Button	Description
New	Adds UDP entries.
Edit	Edits the UDP entry you select.
View	Displays the details of the UDP entry.
Update UDP Entries	Updates UDP entries.

Adding UDP entries

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **System** > **Uniform Dial Plan**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Type a qualifier in the **Enter Qualifier** field.
7. Click **Add(+)**.
8. On the SAT screen, type the details of the UDP entry.
9. Click **Enter**.

   The system adds the UDP entry to the UDP table.

Viewing UDP entries

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **System** > **Uniform Dial Plan**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Choose the UDP entry you want to view.
6. Click **View**.

   The system displays the SAT screen with the details of the UDP entry.

Editing UDP entries

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **System** > **Uniform Dial Plan**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the UDP entry you want to edit.
6. Click **Edit**.
7. On the SAT screen, edit the details for the UDP entry.
8. Click **Enter**.

   The system displays the status that the UDP was successfully edited on the UDP page.

Update UDP entries

Use **Update UDP entries** to add or delete an extension as an endpoint extension on any Communication Manager instance in the UDP group. The extension is then added or deleted in the UDP of that Communication Manager instance and as an AAR or ARS in the UDP of other Communication Manager instances in the UDP group.

Updating UDP entries

Before you begin

You must configure at least one UDP group before you update the UDP entries.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **System** > **Uniform Dial Plan**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Update UDP Entries**.
6. Complete the Update UDP Entries page.
7. Click **Commit**.

Related links

Updating UDP entries field descriptions on page 725

Updating UDP entries field descriptions

Name	Description
Update Mode	The mode by which you want to select the extensions for updating the UDP entries. The choices are: • **File Upload**: Select this option if you want to upload a .txt file with extensions. You can either enter comma separated values or individual extensions in the text file. • **Select Extension**: Select this option to choose an extension range from the text box. You can also enter the extensions manually.
Operation	The add or delete operation you want to perform on the UDP entries. • **Add**: Select **Add** to add an extension as an endpoint extension on any Communication Manager of the UDP group. The extension is then added in the UDP of that Communication

Table continues…

Name	Description
	Manager . The extension is also added as an AAR or ARS in the UDP of other Communication Managers in the UDP group. • **Delete**: Select **Delete** to delete an extension from the UDP of all the Communication Managers in the UDP group. The extension you want to delete must be present in one of the Communication Managers in the UDP group.
Select a File	Click **Select a File** to browse to the text file in your local computer.
Schedule Job	The possible values are: • **Run immediately**: Select this option to update the UDP entries immediately. • **Schedule later**: Select this option to update the UDP entries at the scheduled time.

Button	Description
Commit	Updates the UDP entries for the UDP groups you selected.
Cancel	Cancels the update action.

Related links

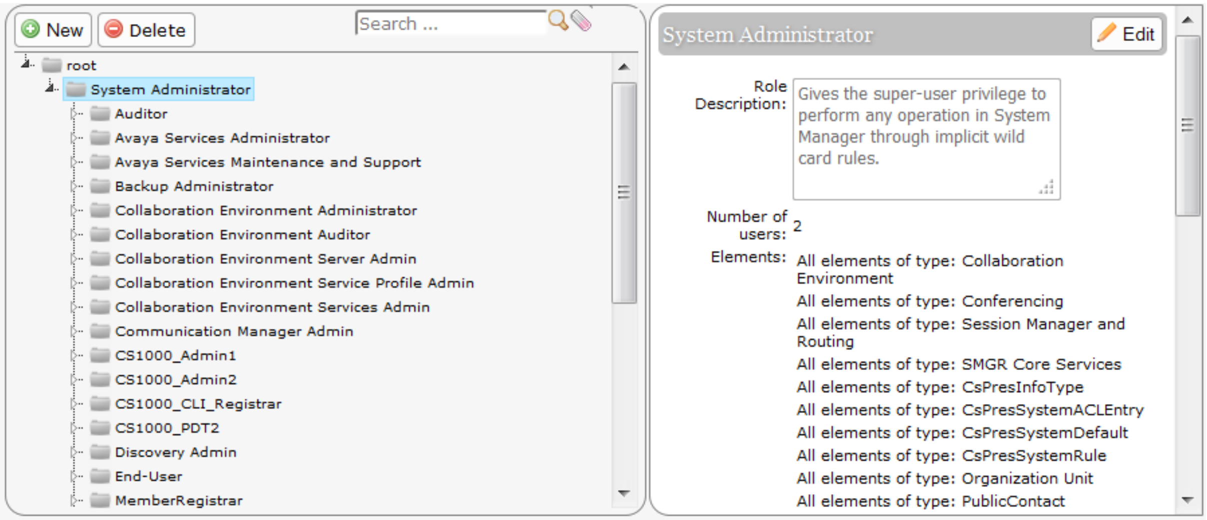
Updating UDP entries on page 725

Assigning permission to gain access UDP groups across Communication Manager instances

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and perform one of the following steps:
   - Click **New**
   - Right-click and select **New**.

   The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



New Delete Search ...

- root
  - System Administrator
    - Auditor
    - Avaya Services Administrator
    - Avaya Services Maintenance and Support
    - Backup Administrator
    - Collaboration Environment Administrator
    - Collaboration Environment Auditor
    - Collaboration Environment Server Admin
    - Collaboration Environment Service Profile Admin
    - Collaboration Environment Services Admin
    - Communication Manager Admin
    - CS1000_Admin1
    - CS1000_Admin2
    - CS1000_CLI_Registrar
    - CS1000_PDT2
    - Discovery Admin
    - End-User
    - MemberRegistrar

System Administrator Edit

Role Description: Gives the super-user privilege to perform any operation in System Manager through implicit wild card rules.

Number of users: 2

Elements: All elements of type: Collaboration Environment
All elements of type: Conferencing
All elements of type: Session Manager and Routing
All elements of type: SMGR Core Services
All elements of type: CsPresInfoType
All elements of type: CsPresSystemACLEntry
All elements of type: CsPresSystemDefault
All elements of type: CsPresSystemRule
All elements of type: Organization Unit
All elements of type: PublicContact

4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping**.
7. In **Group Name**, select the group of templates to which you want to apply this permission.

   You can leave **Group Name** blank if you do not want to select a group.
8. In the **Element or Resource Type** field, click **UDP Group**.
9. Click **Next**.
10. On the Permission Mapping page, apply the required permissions. For example, select **Edit**.
11. Click **Commit**.

Usage options

Endpoint options

Use **Usage Options** to add and remove internal dependencies to an endpoint. Use **Add Options** to add references of an endpoint to other endpoint related objects such as Intra Switch CDR Agent, Intra Switch CDR Endpoint, and Intra Switch CDR VDN. If you select **Add Options** and add an endpoint, the system updates the reference objects you selected automatically.

For example, if you select **Intra Switch CDR for Endpoints** and add a new entry in endpoints, the same entry is added on the Intra Switch CDR form. The system displays **station-user** in the **Type** field.

Use **Usage Options** to:

- Add dependencies between an endpoint and Intra-Switch CDR for Agent, Endpoint, and VDN.
- Remove this endpoint from the bridged extension of another station, if configured.

- Remove an endpoint from a hunt group.
- Remove an endpoint from an Intra-switch CDR, if configured.
- Remove an Off-PBX-Telephone Endpoint-Mapping for the endpoint, if configured.
- Remove an endpoint from another the **Team** button of another endpoint, if configured.
- Remove an endpoint from the **Port Extension** field on the Agents form, if configured.
- Remove an endpoint from the Vector steps, if configured.
- Clear the voice messages that are waiting by selecting the **Clear AMW** checkbox.

Note:

If an endpoint is referenced elsewhere and if you try to delete the endpoint, the Communication Manager gives an error. You must remove the reference before you delete the endpoint. You can remove the references using **Usage Option**.

Adding dependencies to an endpoint, agent, or VDN

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Options** > **Usage Options**.
3. Click the **Add Options** tab.
4. Select one of the following options for a Communication Manager:
    - **Intra-Switch CDR for Agent** to add an Intra-Switch CDR dependency while adding an agent to that Communication Manager
    - **Intra-Switch CDR for Endpoint** to add an Intra-Switch CDR dependency while adding an endpoint on that Communication Manager.
    - **Intra-Switch CDR for VDN** to add an Intra-Switch CDR dependency while adding a VDN on that Communication Manager.
5. Click **Commit**.

    To clear the settings you have chosen, click **Reset**.

Removing references to an endpoint

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Options** > **Usage Options**.
3. In the **Remove Options** tab, select the references you want to remove for the endpoint.
4. Click **Commit**.

Related links

Remove usage options field descriptions on page 729

Remove usage options field descriptions

Name	Description
System	The name of the Communication Manager. Select the checkbox next to **System** to select all the Communication Managers.
Bridged Extension	Select this checkbox to remove the reference between the bridged extension and the endpoint you choose.
Hunt Group	Select this checkbox to remove the reference between the huntgroup and the endpoint you choose.
Intra-Switch CDR	Select this checkbox to remove the reference between the Intra-Switch CDR and the endpoint you choose.
Off- PBX Telephone Station-Mapping	Select this checkbox to remove the reference between the Off-PBX Telephone Station-Mapping and the endpoint you choose.
Team Button	Select this checkbox to remove the reference between the **Team** Button and the endpoint you choose.
Clear AMW	Select the Automatic Message Waiting checkbox to clear all the voice messages that are waiting.
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.
Vector	Select this checkbox to remove the reference between the Vector and the endpoint you choose.

Button	Description
Commit	Click to apply the remove option for the options you select.
Reset	Click to undo all the changes you made.

NRP Group

Overview of NRP group

By using the Network Routing Policy (NRP) group, you can add or remove Communication Manager within the NRP group. Communication Manager of the NRP group can then create **Location** entries in Session Manager for the field **Controlled by this CM server** for that network region.

After you add Communication Manager to the NRP group, you can set the **Controlled by this CM server** field to **Yes** or **No**.

If you specify the IP Network Region for the field **Controlled by this CM server** value to **Yes**, the Session Manager location will generate with **IP Network Region**, **Name** and **IP Network Map** linked for that IP Network Region.

On the IP Network Region page, you can perform the following:

- In the **Details** column, you can either show or hide the **IP Network Maps**.
- You can edit the **Name** and **Controlled by this CM server** fields for the **IP Network Region** that you have selected.

Note:

If Communication Manager 1, Communication Manager 2, and Communication Manager 3 are in an NRP group, and you set the **Controlled by this CM Server** field to **Yes** for the **IP Network Region** X for Communication Manager 1.

Where **IP Network Region** X can be any **IP Network Region** other than **IP Network Region** 1, as **IP Network Region** 1 is an exception.

Important:

You cannot set the **Controlled by this CM Server** field to **Yes** for Communication Manager 2, and Communication Manager 3 in **IP Network Region** X because the these two Communication Manager instances are a part of the same NRP group.

NRP sync feature

By using the NRP synchronization feature, users with H.323 phones can move between offices and have appropriate E911 routing for their location.

For the NRP sync feature, ensure that the authoritative Communication Manager **IP Network Region** information is configured in the Session Manager routing table. A Communication Manager server is authoritative for a location if the location contains media gateways and SIP endpoints that are administered on that Communication Manager server.

Therefore, if you make any change to the **IP Network Map** for the **IP Network Region** that are controlled by Communication Manager, the updates are automatically detected. These updates are replicated to the corresponding **Location** entries in the Session Manager routing table.

Creating NRP groups

About this task

Perform this procedure to add or remove one or more Communication Manager instances from an NRP group. The Communication Manager instances that you select will be a part of the NRP group. These Communication Manager instances will be authoritative over specific **IP Network Regions**.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Options** > **NRP Group**.
3. In the **NRP Group** table, select the Communication Manager instances that you want to add to an NRP group.
4. Click **Commit**.

The Communication Manager instances that you selected are now a part of the NRP group. When you add a Communication Manager instance to the NRP group, the system changes the correlation flag of **IP Network Region** 1 to **Yes**, which means that Session Manager Location is created using **IP Network Region** 1.

Managing NRP groups

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **IP Network Regions**.
3. Select the specific Communication Manager instance from the list of Communication Manager instances.

Result

The IP Network Region page displays the **Details**, **Name**, and **Controlled by this CM Server** columns of that Communication Manager instance.

For more information, see Overview of NRP group.

Next steps

Controlled by this CM Server validation:

Controlled by this CM Server field is available on the IP Network Region List page. **Controlled by this CM Server** disables the validation check in place for using the same **IP Network Region** across multiple Communication Managers which are part of the **NRP Group**. **Network Region 1** is an exception to this validation check.

Set the **iptcm.properties** > **disableAuthValidation** property for using the **Controlled by this CM Server** validation.

iptcm.properties > disableAuthValidation value	Validation scope
True	You can set the value of the **Controlled by this CM Server** field to **Yes** for the same IP Network region on all Communication Manager servers that are part of **NRP Group**.
False	You can set the value of the **Controlled by this CM Server** field to **Yes** only for IP Network region 1 on all Communication Manager servers that are part of **NRP Group**.

Related links

Overview of NRP group on page 729

Correlation between Communication Manager and Session Manager

- The **Controlled by this CM Server** has two values: **Yes** and **No**.
- To edit the **Name** of the Communication Manager that controls that **IP Network Region** for a Communication Manager instance, set **Controlled by this CM Server** to **Yes**.

- To create a correlated Session Manager **Location**, set **Controlled by this CM Server** of **IP Network Region** of a Communication Manager that is a part of **NRP Group** to **Yes**.
- If **Controlled by the CM Server** is changed from **Yes** to **No** then the Session Manager location entry is deleted by the system.

Controlled by the CM Server to Yes

Setting **Controlled by the CM Server** to **Yes** on IP Network region page creates a location on Session Manager.

To verify the Session Manager location on System Manager web console, click **Elements** > **Routing** > **Locations.**

- The **Controlled by this CM Server** is set to **Yes** only if Session Manager location creation is successful at the Session Manager. On List IP Network Region page, click **Save**.
- The change in **Region Name** or **IP Network Map** of **IP Network Region** that has **Controlled by this CM server** set to **Yes** is displayed back in Session Manager when the update occurs in System Manager.

Note:

In case of a conflict or mismatch with the **Name** field on Session Manager, the system logs an error and the **Name** field remains unchanged on Session Manager. The system raises an alarm.

Correlation between Session Manager and System Manager

- System Manager disallows IPv6 type of **IP Network Map** while generating Session Manager location.
- System Manager disallows overlapping ranges while generating Session Manager location, which means setting **Controlled by this CM Server** to **Yes**.
- System Manager disallows generating the Session Manager **Location**, when Communication Manager **IP Network Region Name** is blank or if location exists with same name on Session Manager.
- The Communication Manager **IP Network Region** with **Controlled by this CM Server** and corresponding Session Manager **Location** are mapped using correlation ID.

Chapter 11: Managing IP Office

IP Office Element Manager

IP Office Element Manager

You can configure and manage IP Office, Unified Communications Module (UCM) and Application Server devices from System Manager. You can backup, restore and download the IP Office device configurations.

In System Manager, use inventory management through SNMPv1, to discover IP Office devices. The discovered IP Office devices appear in **Manage Inventory** > **Discovery** in **Inventory**.

With System Manager, you can support the following IP Office configurations:

- IP Office application

  Note:

  You can use this interface to view or edit the configuration values.

- UCM and Application Server

However, client computers need JRE for System Manager to support the IP Office application. See JRE requirement for client computers on page 734.

Use the administrative capabilities of IP Office in System Manager to:

- Edit and view system configuration data in **System Configuration**.
- Edit and view security configuration data in **Security Configuration**.
- Perform the backup and restore tasks of IP Office, UCM and Application Server device configuration that includes system configuration data and user data.
- Synchronize the IP Office, UCM and Application Server devices through the **Inventory** tab.

Note:

When you use System Manager to gain access to an IP Office device, System Manager locks the device you have selected. You cannot go to that IP Office device externally. To unlock the device, edit the security settings in System Manager. Edit the security settings only in critical scenarios.

To create and apply system configuration and endpoint templates for IP Office devices, use **IP Office Endpoint** and **IP Office System Configuration** pages. Use the **IP Office Endpoint** and **IP Office System Configuration** menus in template management to:

- Create, edit, view, duplicate, and delete the Endpoint Templates for IP Office, UCM and Application Server devices.
- Create, edit, view, duplicate, and delete the System Configuration Templates for IP Office, UCM and Application Server devices.
- Upload and convert audio files from a .WAV to a .C11 format.
- Apply IP Office System Configuration templates to IP Office, UCM and Application Server devices.

Related links

JRE requirement for client computers on page 734

JRE requirement for client computers

When launching IP Office Manager, client computers need Java Runtime Environment (JRE). JRE is required to open IP Office Manager through the Java Applet.

As an System Manager administrator, you must install JRE 1.7+ on your client machine to manage IP Office users, system configuration, and security configuration.

If JRE 1.7+ is not installed, the system displays the following message:

```
Failed to launch IP Office Manager.
```

```
IP Office Manager requires Java Runtime Environment to launch, System has
detected that there is no Java Runtime Environment present or version
present is below recommended Java Runtime Environment version 1.7+.
Download and install latest Java Runtime Environment version for Windows
operating system from the Oracle site http://www.oracle.com/technetwork/java/javase/downloads/index.html.
```

You can download the latest version of JRE from http://www.oracle.com/technetwork/java/javase/downloads/index.html.

Note:

Upgrade JRE to JRE 1.7.0_51+ and upgrade JDK plugin in the browser to JDK 7.0.510+. Because JRE 1.7 introduced security settings changes, you must clear the browser cache and temporary internet files of Java from Java Control Panel. To delete the cache of applications and applets, when you delete the temporary internet files from Java Control Panel, click **Installed Applications and Applets**.

Related links

IP Office Element Manager on page 733

Unlocking an IP Office device

Procedure

1. On the IP Office Manager, in **Security Settings** pane, click **Security** > **Services**.
2. In the **Services** pane, click **Configuration**.
3. In the **Service: Configuration** pane, in the **Service Details** section, do the following:
    a. Type a name for the service in the **Name** text area.
    b. Type a name for the host system in the **Host System** text area.
    c. Enter the value for the service port in the **Service Port** text area.
    d. Select the service security level in the **Service Security Level** drop down box.
    e. In the **Service Access Source** drop down box, select **Unrestricted**.
4. Save and exit the IP Office manager.

    This procedure unlocks the IP Office device for external access.

Next steps

This procedure does not permanently unlock the IP Office device. The device remains unlocked till the device receives a request through System Manager.

- The IP Office device can be locked using System Manager.
- The device can also be locked if you perform any operation on the device through System Manager .

Starting the IP Office Element Manager

The IP Office application is a prerequisite for successful completion of administrative tasks on the **Security Configuration** and **System Configuration** pages in **IP Office**, **IP Office Endpoint** and **IP Office System Configuration** pages in **Templates**, and the **IP Office Endpoint Profile** section in **User Management**.

When you newly install System Manager , set up System Manager to start the IP Office application, and to upgrade the IP Office application to the latest version available in PLDS.

Setting up System Manager to start IP Office element manager

About this task

Note:

This task is not required if you have downloaded the AdminLite-XXX.exe file using **Software Management** in System Manager .

Procedure

1. Download the IP Office element manager `AdminLite-XXX.exe` file from http://plds.avaya.com.

   XXX in AdminLite-XXX.exe specifies the version string. For example, B5800AdminLite-6.2(38).exe.

   Using IP Office element manager, (AdminLite-XXX.exe), you can manage IP Office and B5800 devices.

2. Transfer the downloaded `AdminLite-XXX.exe` or `B5800AdminLite-XXX.exe` file to the System Manager server using SFTP or SCP to the `/opt/Avaya/ABG/<version>/tools` directory. For example, `/opt/Avaya/ABG/6.2.12/tools`.

   `/opt/Avaya/ABG/<version>` is the same as $ABG_HOME.

3. Change this file into an executable file using the command: `chmod +x <file name>`.

4. You must create a soft link using the name *ManagerSFX.exe* for the uploaded file. Go to `$ABG_HOME/tools by doing cd $ABG_HOME/tools`, and create a soft link using the **`ln -sf target linkname`** command.

   If the filename uploaded to $ABG_HOME/tools is *B5800ManagerLite.exe*, then run the **`ln -sf B5800ManagerLite.exe ManagerSFX.exe`** command.

5. Update the `abg_b5800_mgr_version` parameter with the IP Office element manager version you downloaded from PLDS in the `/opt/Avaya/ABG/<version>/tools/ManagerSFXVersion.properties` file.

6. If you have an IP Office administration suite already installed on your computer using the IP Office Administration Applications DVD, update the *abg_b5800_mgr_version* parameter with the manager version of your computer in the `/opt/Avaya/ABG/<version>/tools/ManagerSFXVersion.properties` file on System Manager.

   Important:

   You must update the `abg_b5800_mgr_version` parameter each time you download a new version of IP Office element manager from PLDS, and transfer to System Manager. If you do not, an attempt to start the IP Office element manager through System Manager fails, and the system displays an error message to update the parameter.

7. On the administration computer that is used to launch IP Office, set the environment variable to match the version of the AdminLite-XXX.exe file. Depending on the version of Windows running on your computer, perform one of the following actions:

   - If the computer is running Windows XP, see Setting up the environment variable in Windows XP to match the version of AdminLite on page 737.
   - If the computer is running Windows 7, see Setting up the environment variable in Windows 7 to match the version of AdminLite on page 738.

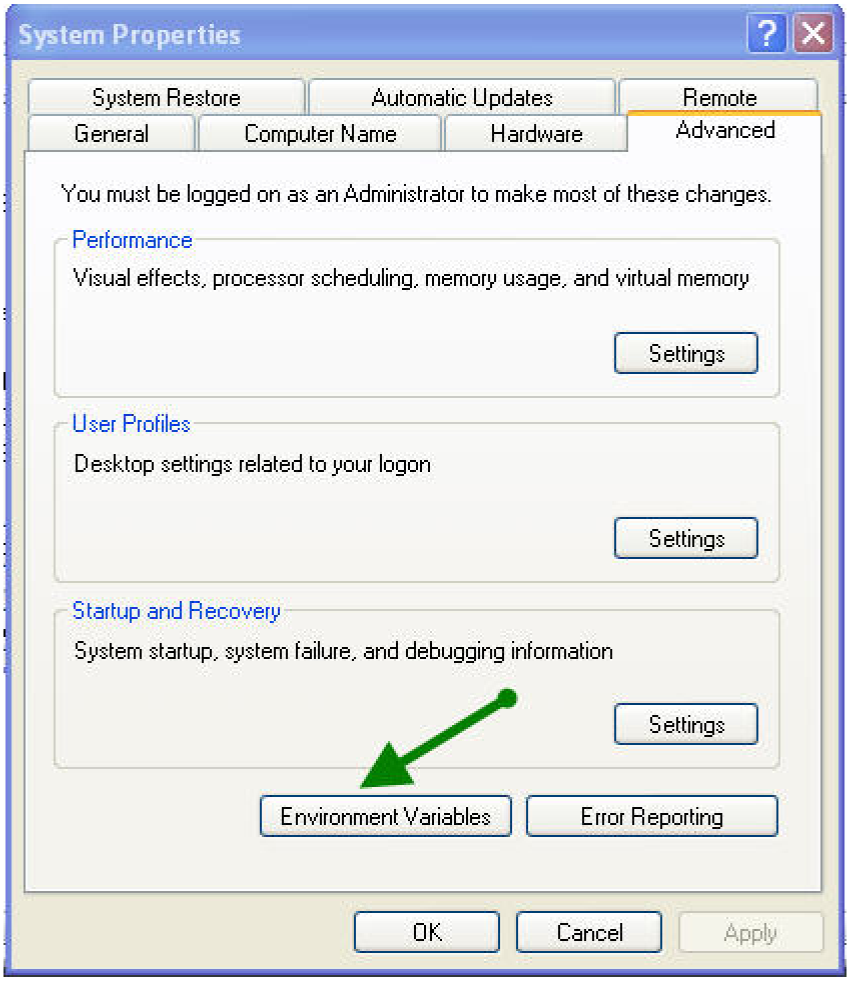
Setting up the environment variable in Windows XP to match the version of AdminLite

About this task

You must set the environment variable of your system to match the version of AdminLite that you install.

Procedure

1. Click **Start**, and then right-click **My Computer**.
2. Click **Properties**.
3. In the System Properties dialog box, click the **Advanced** tab.
4. Click **Environment Variables**.



You must be logged on as an Administrator to make most of these changes.

Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your logon

System startup, system failure, and debugging information

5. In the Environment Variables dialog box, in the **User variables for <name> area**, do one of the following:
   - If you have added IP Office as a device, select **IPOFFICEADMIN_VER**.
   - If you have not added any IP Office devices, select **AVAYAB5800_VER**.
6. Click **Edit**.
7. In the Edit User Variable dialog box, in the **Variable value** field, change the value to match the version of AdminLite.
8. Click **OK**.
9. For the subsequent dialog boxes, click **OK**.
10. Click **Apply**.

Setting up the environment variable in Windows 7 to match the version of AdminLite

About this task

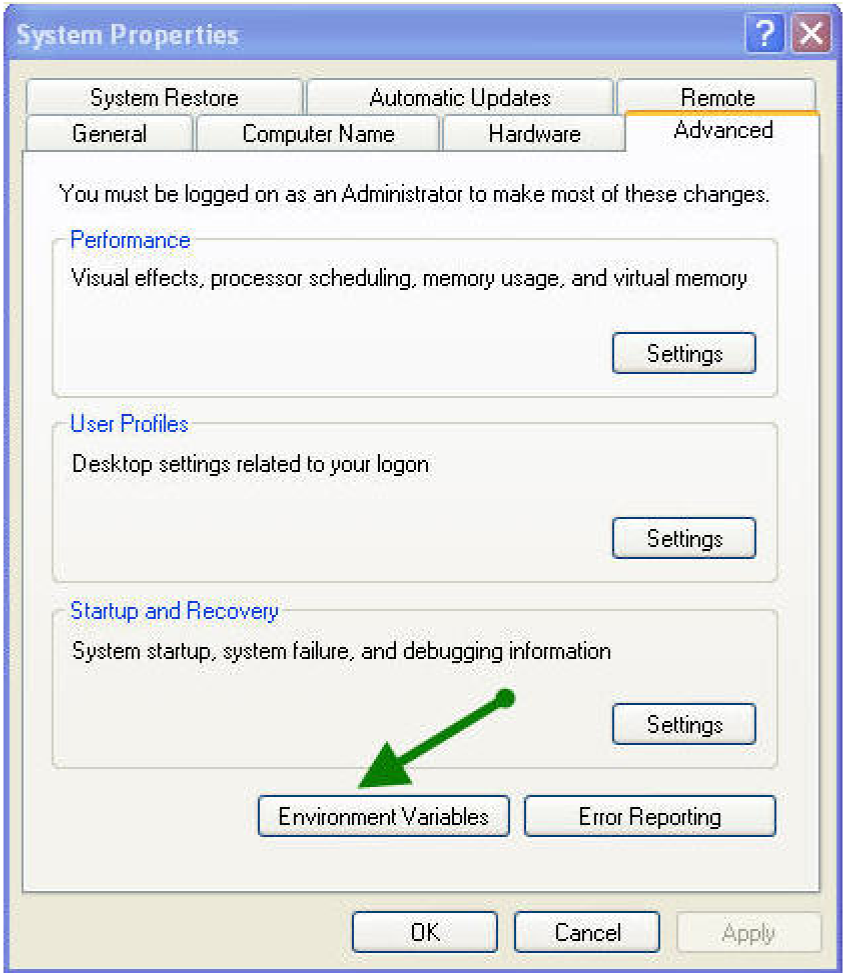
Follow this procedure to set the environment variable of your system to match with the version of AdminLite you install.

Procedure

1. Click **Start**.
2. Right click **Computer**.
3. Click **Properties**.
4. In the left navigation pane, click **Advanced system settings**.
5. In the System Properties dialog box, click **Environment Variables**.
6. In the Environment Variable dialog box, in the **User variables forandmp; lt;n ame>** area, select **IPOFFICEADMIN_VER**. The variable **IPOFFICEADMIN_VER** is applicable if you have added IP Office 9.0 as a device.

   You must select **AVAYAB5800_VER** as the variable if you have not added any IP Office device.

7. Click **Edit**.



You must be logged on as an Administrator to make most of these changes.

Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your logon

System startup, system failure, and debugging information

8. In the Edit User Variables dialog box, in the **Variable value** field, change the value to match the version of AdminLite.

   Set the value to `9.1`.

9. Click **OK**.
10. Click **OK** for each dialog box.
11. Click **Apply**.

Default login password for day one configuration of an IP Office device

For day one configuration for an IP Office device in **Manage Elements** in System Manager, use the default service login and password to gain access to an IP Office device through System Manager. On the Attributes tab of the New IP Office page, the following are the default values:

- **Service Login**: SMGRB5800Admin
- **Service Password**: SMGRB5800Admin

Note:

For IP Office 9.1 and later, the default values set in **Service Login** and **Service Password** are BranchAdmin.

To navigate to the New IP Office page in **Manage Elements** from the web console, click **Inventory** > **Manage Elements** > **New**.

You can use the service password only once. After you commit the service login and password, the system changes this default password internally and generates a random password. The system does not display the new password. To reset the login password, connect to the IP Office device locally by using IP Office Manager.

Important:

After you change the password, the system schedules a default Sync system configuration and a system configuration backup job everyday.

IP Office system configuration

System Configuration

Use the **System Configuration** pages to view and edit system configuration of IP Office, IP Office Application Server, and UCM devices through System Manager. However, client computers need JRE for System Manager to support the IP Office application. See JRE requirement for client computers on page 734.

To view or edit system configuration values, start the IP Office element manager in the *offline* mode through System Manager. System Manager uses web services to obtain the latest system configuration and passes the configuration to the IP Office element manager. After you save the IP Office element manager configuration, System Manager retrieves the modified system configuration file and pushes the file to the IP Office configuration.

Viewing an IP Office system configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **IP Office** > **System Configuration**.

3. On the IP Office System Configuration page, select the IP Office device whose system configuration you want to view.
4. Click **View**.

   In the right pane of the IP Office window, you can view the details of the selected IP Office system configuration.

   Note:

   All the fields are view only.

   The system starts the IP Office Manager application.
5. Click **File** > **Exit** to exit the IP Office Manager application.

   The IP Office System Configuration landing page opens.

Related links

IP Office system configuration field descriptions on page 742

Editing an IP Office system configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **IP Office** > **System Configuration**.
3. On the IP Office System Configuration page, select the IP Office device whose system configuration you want to edit.
4. Click **Edit**.

   The system starts the IP Office Manager application.
5. On the IP Office Manager window, edit the required fields on the right pane.
6. Click **File** > **Save Configuration and Exit** to save the modifications and exit the IP Office Manager application.

   On the IP Office System Configuration Edit page, the system displays the selected IP Office device in the device list. Perform one of the following:

   - To apply the changes immediately, click **Commit**.
   - To apply the changes at a specified time, click **Schedule**.

Related links

IP Office system configuration field descriptions on page 742

Downloading the IP Office system configuration

About this task

Use the procedure to copy the configuration of an IP Office device to the local machine.

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **IP Office** > **System Configuration**.
3. On the IP Office System Configuration page, select the device whose security configuration you want to download.
4. Click **Download**.
5. Do one of the following:
    - For Firefox, click **Save File** and click **OK**.

      The system saves the saves the configuration file with the device name to the default location.
    - For Internet Explorer, provide the file name and location, and click **Save**.

      The system saves the configuration file to the default location.

IP Office system configuration field descriptions

Name	Description
Device Name	The name of the IP Office device.
IP Address	The IP address associated with the IP Office device.
System Type	The type of system associated with the IP Office device. The valid options are: • **IP Office**: for IP Office core unit • **IP Office Select**: for IP Office Select core unit
Last Operation on Device	The operation that has been performed last on the device.
Status	The status of the operation that is currently running or was last run.
System Configuration Template	The current IP Office System Configuration template that exists on the IP Office device.
Last Modified Time of System Configuration	The date and time you last modified the system configuration.
Last Backup Time	The date and time when you last performed a backup.

Buttons

Name	Description
View	Click to view the IP Office system configuration field descriptions.

Table continues…

Name	Description
Edit	Click to edit the IP Office system configuration field descriptions.
Download	Click to download the IP Office system configuration field descriptions.

IP Office security configuration

Security Configuration

Use the **Security Configuration** pages to view and edit the security configuration values of IP Office, UCM, or Application Server devices through System Manager. However, Client computers need JRE for System Manager to support the IP Office application. See JRE requirement for client computers on page 734.

To view or edit security configuration values, you must launch the IP Office Manager in the *online* mode through System Manager. System Manager uses web services to obtain the latest security configuration from an IP Office, UCM, or Application Server device and passes the configuration to the IP Office element manager. After you save the modifications on the IP Office element manager, System Manager retrieves the modified security configuration file and pushes the file to the IP Office, UCM, or Application Server device. After the security configuration files are successfully uploaded to the device, System Manager deletes the local copy of these security configuration files.

Viewing a security configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **IP Office** > **Security Configuration**.
3. On the IP Office Security Configuration page, select the IP Office device whose Security Configuration you want to view.
4. Click **View**.

   In the right pane of the IP Office Manager window, you can view the details of the selected IP Office Security Configuration. All the fields are read-only.

   The system starts the IP Office Manager application.
5. To exit the IP OfficeManager application and return to the IP Office Security Configuration page, click **File** > **Exit**.

Related links

IP Office security configuration field descriptions on page 744

Editing a security configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **IP Office** > **Security Configuration**.
3. On the IP Office Security Configuration page, select the device whose security configuration you want to edit.
4. Click **Edit**.

   The system starts the IP Office Manager application.
5. On the IP Office Manager window, edit the required fields on the right pane.
6. Click **File** > **Save Security Settings and Exit** to save the modifications and exit the IP Office Manager application.

   The system directs you to the IP Office Security Configuration landing page.

   After you save the configuration, System Manager retrieves the edited security configuration file from the IP Office Manager application and pushes the file to the IP Office device.

Related links

IP Office security configuration field descriptions on page 744

IP Office security configuration field descriptions

Device list

Name	Description
Device Name	The name of the IP Office device.
IP Address	The IP address associated with the IP Office device.
System Type	The type of system associated with the IP Office device. The valid options are: • **IP Office**: for IP Office core unit • **IP Office Select**: for IP Office Select core unit
Last Operation on Device	The last operation that you performed on the device.
Status	The status of the operation that is currently running or was last run.
System Configuration Template	The current IP Office System Configuration template that exists on the IP Office device.
Last Modified Time of System Configuration	The date and time of the last system configuration operation.
Last BackupTime	The date and time when you last performed the backup activity on the IP Office device.

Buttons

Name	Description
View	Click to view the IP Office security configuration field descriptions.
Edit	Click to edit the IP Office security configuration field descriptions.

Backup and restore of the IP Office devices

IP Office device configuration backup

Use the **Backup** feature on the **IP Office Backup** page to back up the IP Office device configuration. The IP Office device configuration contains the system configuration data and the user data. You can create a backup locally or on a remote server.

Use the **IP Office Backup** page to create a local backup in the local storage attached to the IP Office device. The IP Office device stores only one copy of the backup file in the local storage. If you are backing up on a remote server, you can create five backup files for every device.

You can perform the backup task immediately or at a scheduled time. Use the **Scheduler** service in System Manager to set the time. You can view the logs of the backup task on the Log Harvesting pages in System Manager.

IP Office device configuration restoration

Use the **Restore** feature on the **IP Office Restore** page to restore the IP Office device configuration. The IP Office device configuration contains the system configuration data and the user data. You can perform the restore operation from a local storage or a remote server.

You can perform the restore task immediately or at a scheduled time. Use the **Scheduler** service in System Manager to set the time. You can view the logs of the restore tasks on the Log Harvesting pages in System Manager.

Configuring the http or https protocol for a remote server

About this task

Use this procedure to configure the remote server so that you can use the `HTTP` or `HTTPS` protocol.

Procedure

1. On the remote server, install and activate the `HTTPS` and `PHP` packages.
2. On the System Manager server, do the following:
    a. Navigate to `/opt/Avaya/ABG/6.3.8/httpfiles/`.
    b. Copy the files with the `.php` extension to the backup location on the remote server.
3. On the remote server, grant the full access permissions to the files that you copied in Step 2.

4. Start a browser and test the accessibility of the remote server in the network.

Creating a backup of the IP Office device configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation page, click **Backup**.
3. On the IP Office Backup page, select the IP Office device from the Device List for which you want to create a backup.
4. In the **Backup Options** field, click **Backup On Device** or **Backup On Remote Server**.
5. Click **Backup**.

   The system displays the IP Office device that you selected in the **Device List**.
6. Do one of the following:

Choice Option	Sub Steps
Backup On device	a. Click **Now** to perform the backup task immediately. b. Click **Schedule** to perform the backup task at a specified time.
Backup On Remote Server	a. In the **Select Remote Server** field, select a remote server where you want to save the backup. Alternatively, click **Add Server** to add a remote server. b. In the **Backup Label** field, type a name for the backup. c. Click **Now** or **Schedule**.

7. To view the status of the backup task for the selected device, click **Status**.

Related links

IP Office Backup field descriptions on page 747
IP Office Restore field descriptions on page 749

Restoring the IP Office device configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **Restore**.
3. On the IP Office Restore page, select the IP Office device or devices from the Device List whose backed up configuration you want to restore.
4. In the **Restore Options** field, click **Restore Backup Stored On Devices** or **Restore Backup Stored On Remote Server**.
5. Click **Restore**.
6. In the **Restore Options** field, do one of the following:

Choice Option	Choice Description
For Restore Backup Stored on Device(s), select one of the following :	• System Configuration • User • System Configuration and User • Restore Backup Stored on Devices
For Restore Backup Stored on Remote Server, do the following:	a. In the **Select Remote Server** field, select a remote server. Alternatively, click **Add Server** to add a remote server. b. Click **Get Restore Point**. c. Select **Restore Point** from the list.

7. Click **Now** to perform the restore activity immediately.
8. **(Optional)** Click **Schedule** to perform the restore activity at a specified time.

Result

You can view the status of the restore job in the **Scheduler** service.

Related links

IP Office Backup field descriptions on page 747
IP Office Restore field descriptions on page 749

IP Office Backup field descriptions

Backup Options

Name	Description
Backup Options	The options are: • Backup On Device • Backup On Remote Server **Note:** The Backup On Remote Server option is available for IP Office Manager Release 9.1 and later.

Backup On Device field descriptions

Name	Description
Device Name	The name of the IP Office device.
IP Address	The IP address associated with the IP Office device.
System Type	The type of system associated with the IP Office device. The options are: • **IP Office**: For the IP Office core unit

Table continues…

Name	Description
	• **B5800 device**: For the B5800 device
Last Operation on Device	The name of the last operation performed on the IP Office device.
Status	The status of the operation.
System Configuration Template	The current IP Office System Configuration template that exists on the IP Office device.
Last Modified Time of System Configuration	The last time that the system configuration was modified.
Last Backup Time	The last time that a backup was taken.

Button descriptions

Name	Description
Backup	Displays the IP Office Backup page.
Status	Displays the status of the last operation.
Stop	Stops the operation.

Backup On Device button descriptions

Button	Description
Now	Performs the backup operation, as applicable, immediately.
Schedule	Displays the IP Office Job Scheduler page to schedule a backup.
Cancel	Cancels the backup job and returns to the IP Office Backup page.

Backup On Remote Server field descriptions

Name	Description
Select Remote Server	The Remote Server location to store the backup. The options are: • **Select**: To select a remote server. • **Add Server**: To add a remote server.
Add Server	The configuration for a remote server: • **Backup Label**: The name of the backup • **New Server Name**: The name of the new server • **New Server IP**: The IP address of the new server • **Port**: The port number of the new server • **Backup Path**: The backup path of the new server • **Selected Protocol**: The protocol of the new server

Table continues…

Name	Description
	- **User Name**: The name of the user - **Password**: The password of the user
Selected Protocol	The protocol of the new server. The options are: - **http** - **https**

Backup On Remote Server button descriptions

Button	Description
Save	Saves the remote server and backup configuration.
Edit	Modifies the remote server and backup configuration.
Delete	Deletes the remote server and backup configuration.

IP Office Restore field descriptions

Restore Options

Name	Description
Restore Options	The options are: - Restore Backup Stored on Devices - Restore Backup Stored on Remote Server

Restore field descriptions

Name	Description
Device Name	The name of the IP Office device.
IP Address	The IP address associated with the IP Office device.
Last Operation on Device	The name of the last operation performed on the IP Office device.
Status	The status of the operation.
System Configuration Template	The current IP Office System Configuration template that exists on the IP Office device.
Last Modified Time of System Configuration	The date and time of the last system configuration operation.
Last Backup Time	The date when you last performed the Backup operation on the device.

Restore Backup Stored On Devices field descriptions

Name	Description
System Type	The type of system associated with the IP Office device. The option: • **IP Office and B5800 device**
Restore Backup Stored On Devices	The options are: • **System Configuration**: For restoring the system configuration • **User**: For restoring the user • **System Configuration and User**: For restoring the system configuration and the user • **Restore Backup Stored on Devices**: For restoring the backup stored on the devices

Button descriptions

Name	Description
Restore	Opens the IP Office Restore page.
Status	Displays the status of the operation that is currently running or was last run.
Stop	Stops the operation that is currently running.

Restore Backup Stored on Remote Server field descriptions

Name	Description
System Type	The type of system associated with the IP Office device. The option is: • **IP Office**: only for IP Office Manager version 9.1
Remote Server	The Remote Server location where the last backup was stored. Do one of the following: • **Select**: Select a remote server. • **Add Server**: Add a remote server.
Add Server	The configuration for a remote server: • **New Server Name**: The name of the new server • **New Server IP**: The IP address of the new server • **Port**: The port number of the new server • **Backup Path**: The backup path of the new server • **Selected Protocol**: The protocol of the new server • **User Name**: The name of the user

Table continues…

Name	Description
	• **Password**: The password of the user
Selected Protocol	The protocol of the new server. The options are: • **http** • **https**
Restore Point(s)	The restore point from where you want to restore the last backup

Restore Backup Stored on Remote Server Button descriptions

Name	Description
Get Restore Point	Creates a Restore Point from where you can restore the last backup.
Save	Saves the new remote server configuration.
Edit	Edits the new remote server configuration.
Delete	Deletes the new remote server configuration.

UCM or IP Office Application Server

UCM and Application Server field descriptions

Name	Description
Device Name	The name of the UCM and Application Server device.
IP Address	The IP address associated with the UCM and Application Server device.
System Type	The type of system associated with the UCM and Application Server device.
Last Operation on Device	The name of the last operation performed on the UCM and Application Server device.
Status	The status of the operation.
System Configuration Template	The current IP Office System Configuration template that exists on the IP Office device.
Last Modified Time of System Configuration	The last time that the system configuration was modified.
Last Backup Time	The last time that a backup was taken.

UCM and Application Server device configuration backup

Use the **Backup** feature on the UCM and Application Server Backup to back up the UCM and Application Server device configuration. The UCM and Application Server device configuration contains the following data:

- Voice mail— related configuration
- Messages

- Recordings
- One-X portal— related configuration

Use the UCM and Application Server Backup page to create a remote backup, where the system stores the backup in the selected remote server location. The UCM and Application Server device can store five copies of the backup file in the remote storage.

You can perform the backup task immediately or at a scheduled time. Use the **Scheduler** service in System Manager to set the time. You can view the logs of the backup tasks on the Log Harvesting pages in System Manager.

Related links

Creating a backup of the UCM and Application Server device configuration on page 752
Restoring the UCM and Application Server device configuration on page 753

UCM and Application Server device configuration restoration

Use the Restore feature on the UCM and Application Server Restore page to restore the UCM and Application Server device configuration. The UCM and Application Server device configuration contains the following data:

- Voice mail-related configuration
- Messages
- Recordings
- One-X portal-related configuration

Use the UCM and Application Server Restore page to restore the data from a remote server. The UCM and Application Server device stores five copies of the backup file in the remote storage.

You can perform the restore task immediately or at a scheduled time. Use the **Scheduler** service in System Manager to set the time. You can view the logs of the restore tasks on the Log Harvesting pages in System Manager.

Related links

Creating a backup of the UCM and Application Server device configuration on page 752
Restoring the UCM and Application Server device configuration on page 753

Creating a backup of the UCM and Application Server device configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **Backup**.
3. On the UCM and Application Server Backup page, in Device List, click the UCM and Application Server device for which you want to create a backup.
4. Click **Backup**.

   The system displays the UCM and Application Server device that you selected in **Device List**.

5. Select a remote server from the **Remote Server** field. Alternatively, click **Add Server** to add a remote server.
6. Configure the settings for **Backup Configuration** using the following parameters:
   - In the **Select Voicemail Pro Sets** field, choose voice mail pro sets.
   - In the **Select One-x Portal Sets** field, choose one-x portal sets.
   - In the **Select Contact Recorder Sets** field, choose contact recorder sets.
   - In the **Backup Label** field, type the backup file name.
7. Do one of the following:
   - Click **Now** to perform the backup task immediately.
   - Click **Schedule** to perform the backup task at a specified time.
8. To view the status of the backup task for the selected device, click **Status**.

Related links

UCM and Application Server Backup field descriptions on page 755
UCM and Application Server Restore field descriptions on page 756

Restoring the UCM and Application Server device configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation page, click **UCM and Application Server** > **Restore**.
3. On the UCM and Application Server Backup page, select the UCM and Application Server device whose backed— up configuration you want to restore.
4. Click **Restore**.

   The system displays the UCM and Application Server device that you selected in **Device List**.
5. Do the following:
   a. In the **Remote Server** field, click a Remote Server . Alternatively, click **Add Server** to add a remote server.

      The system activates the **Get Restore Point** button.

   b. Click **Get Restore Point**.

      The system displays the **Restore Points** list with the restore point that you added:

Field name	Field description
Restore Point	Displays the name of the restore point.
IP Address	Displays the IP address associated with the restore point.

Table continues…

Field name	Field description
Version	Displays the version of the restore point.
Set	Displays the set of the restore point.
Time Stamp	Displays the time stamp associated with the restore point.

6. Do one of the following:
   - Click **Now** to perform the restore task immediately.
   - Click **Schedule** to perform the restore task at a specified time.

   To view the status of the restoration task for the selected device, click **Status**.

Related links

UCM and Application Server Backup field descriptions on page 755
UCM and Application Server Restore field descriptions on page 756

Downloading the UCM and Application Server system configuration

About this task

Use this procedure to copy the configuration of UCM and Application Server instances to the local computer.

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **System Configuration**.
3. On the UCM and Application Server System Configuration page, select the device whose security configuration you want to download.
4. Click **Download**.
5. Do one of the following:
   - For Firefox, click **Save File**, and then click **OK**.

     The system saves the configuration file with the device name to the location that you specified.
   - For Microsoft Internet Explorer, type the file name and the location, and click **Save**.

     The system saves the configuration file to the location that you specified.

Related links

UCM and Application Server Backup field descriptions on page 755
UCM and Application Server Restore field descriptions on page 756

UCM and Application Server Backup field descriptions

Remote Server

Name	Description
Select Remote Server	The Remote server location to store the backup.

Backup On Remote Server

Name	Description
Select Remote Server	The Remote Server location to store the backup. The options are: • **Select**: To select a remote server. • **Add Server**: To add a remote server.
Add Server	The configuration parameters for adding a remote server. The parameters are: • **Backup Label**: The name of the backup • **New Server Name**: The name of the new server • **New Server IP**: The IP address of the new server • **Port**: The port number of the new server • **Backup Path**: The backup path of the new server • **Selected Protocol**: The protocol of the new server • **User Name**: The name of the user • **Password**: The password of the user
Selected Protocol	The protocol of the new server. The options are: • **http** • **https** • **scp** • **sftp** • **ftp**

Backup Configuration

Name	Description
Select voice mail Pro Sets	The voice mail pro sets.
Select one-X Portal Sets	The one-X Portal sets.
Select Contact Recorder Sets	The contact recorder sets.
Backup Label	The name of the backup file.

Buttons

Button	Description
Backup	Opens the UCM and Application Server Backup page.
Status	Displays the status of the last operation.
Save	Saves the remote server and backup configuration.
Edit	Modifies the remote server and backup configuration.
Delete	Deletes the remote server and backup configuration.
Now	Performs the backup job, as applicable, immediately.
Schedule	Schedules the backup at a later time and opens the UCM and Application Server Backup page.
Cancel	Cancels the backup job and opens the UCM and Application Server Backup page.
Stop	Stops the backup job.

UCM and Application Server Restore field descriptions

Remote Server

Name	Description
Select Remote Server	The list of available remote servers
New Server Name	The name of the new server
New Server IP	The IP address of the new server
Port	The port address
Backup Path	The path of the latest backup
Selected Protocol	The protocol for the new server
User Name	The user name for the new server
Password	The password for the new server

Button	Description
Restore	Opens the **UCM and Application Server Restore** page. Use this page to restore the backed up system configuration and the messages, the recording and the one-X configuration to a UCM and Application Server device.
Status	Displays the status of the operation that is currently running or was last run.
Save	Saves the remote server and backup configuration.
Now	Performs the restore operation immediately.
Schedule	Displays the **IP Office Job Scheduler** page. Use this page to schedule a Restore operation.

Table continues…

Button	Description
Cancel	Cancels the restore job, as applicable, and directs you to the **Restore** landing page.
Get Restore Point	Creates a restore point on the selected remote server.

Restore Backup stored on Remote Server

Name	Description
Remote Server	The Remote Server location where the last backup was stored. Do one of the following: • **Select**: Select a remote server. • **Add Server**: Add a remote server.
Add Server	The configuration for a remote server • **New Server Name**: Name of the new server • **New Server IP**: IP address of the new server • **Port**: Port number of the new server • **Backup Path**: Backup path of the new server • **Selected Protocol**: Protocol of the new server • **User Name**: Name of the user • **Password**: Password of the user
Selected Protocol	Protocol of the new server. Select a protocol from the following: • **http**: for the http protocol • **https**: for the https protocol • **scp**: for the scp protocol • **sftp**: for the sftp protocol • **ftp**: for the ftp protocol
Restore Point(s)	The restore point from where you want to restore the last backup

UCM or IP Office Application Server system configuration

Viewing a UCM and Application Server system configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **System Configuration**.
3. On the System Configuration page, select the UCM and Application Server device whose system configuration you want to view.

4. Click **View**.

   In the right pane of the UCM and Application Server window, you can view the details of the selected UCM and Application Server system configuration.

   > **Note:**
   >
   > All the fields are view only.

   The system starts the UCM and Application Server Manager application.

5. Click **File** > **Exit** to exit the UCM and Application Server Manager application.

   The UCM and Application Server System Configuration landing page opens.

Editing a UCM and Application Server system configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **System Configuration**.
3. On the UCM and Application Server System Configuration page, select the UCM and Application Server device whose system configuration you want to edit.
4. Click **Edit**.

   The system starts the UCM and Application Server Manager application.

5. On the UCM and Application Server Manager window, edit the required fields on the right pane.
6. Click **File** > **Save Configuration and Exit** to save the modifications and exit the UCM and Application Server Manager application.

   On the UCM and Application Server System Configuration Edit page, the system displays selected UCM and Application Server device in the device list. Perform one of the following:

   - Click **Commit** to apply the changes immediately.
   - Click **Schedule** to apply the changes at a specified time.

UCM and Application Server system configuration field descriptions

Name	Description
Device Name	The name of the UCM and Application Server device.
IP Address	The IP address associated with the UCM and Application Server device.
System Type	The type of system associated with the UCM and Application Server device.
Last Operation on Device	The operation that has been performed last on the device.

Table continues…

Name	Description
Status	The status of the operation that is currently running or was last run.
System Configuration Template	The current UCM and Application Server System Configuration template that exists on the UCM and Application Server device.
Last Modified Time of System Configuration	The date and time you last modified the system configuration.
Last Backup Time	The date and time when you last performed a backup.

Button

Name	Description
View	Click to view the UCM and Application Server system configuration field descriptions.
Edit	Click to edit the UCM and Application Server system configuration field descriptions.
Download	Click to download the UCM and Application Server system configuration field descriptions.

UCM or IP Office Application Server security configuration

Viewing UCM and Application Server security configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **Security Configuration**.
3. On the UCM and Application Server Security Configuration page, select the UCM and Application Server device whose Security Configuration you want to view.
4. Click **View**.

   The system starts the UCM and Application Server Manager application.
5. In the right pane of the UCM and Application Server Manager window, you can view the details of the selected UCM and Application Server Security Configuration. All the fields are read-only.
6. Click **File** > **Exit** to exit the UCM and Application Server Manager application and return to the UCM and Application Server Security Configuration landing page.

Editing UCM and Application Server security configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **Security Configuration**.

3. On the UCM and Application Server Security Configuration page, select the device whose security configuration you want to edit.
4. Click **Edit**.

   The system starts the UCM and Application Server Manager application.
5. The system starts the UCM and Application Server Manager window, edit the required fields on the right pane.
6. Click **File** > **Save Security Settings and Exit** to save the modifications and exit the UCM and Application Server Manager application.

   The system directs you to the IP Office Security Configuration landing page.

   After you save the configuration, System Manager retrieves the edited security configuration file from the UCM and Application Server Manager application and pushes the file to the UCM and Application Server device.

UCM and Application Server security configuration field descriptions

Device list

Name	Description
Device Name	The name of the UCM and Application Server device.
IP Address	The IP address of the UCM and Application Server device.
System Type	The type of system associated with the UCM and Application Server device.
Last Operation on Device	The last operation that you performed on the device.
Status	The status of the operation that is currently running or was last run.
System Configuration Template	The current system configuration template that exists on the UCM and Application Server device.
Last Modified Time of System Configuration	The date and time of the last system configuration operation.
Last Backup Time	The date and time when you last performed the backup activity on the UCM and Application Server device.

Buttons

Name	Description
View	Click to view the UCM and Application Server security configuration field descriptions.
Edit	Click to edit the UCM and Application Server security configuration field descriptions.

UCM or Application Server file transfer

Transferring custom prompt files to a UCM or Application Server device

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **UCM and Application Server** > **File Transfer**.
3. In **Select File Type**, click **Custom Prompts**.
4. In **Select Files to Upload**, click the audio file that you want to upload.

   List Audio Files displays the list of audio files that you have uploaded by using **Manage Custom Prompts** in the UCM or Application Server system configuration templates.

   In the **Enter Destination Folder Location to Push Files** field, the system displays the default location where you want to transfer the file.
5. In **Devices List**, select the IP Office Application Server or UCM device where you want to upload the audio file.
6. Click **Commit**.
7. On the File Transfer page, perform one of the following:
   - Click **Now** to upload the audio file to the IP Office Application Server or UCM device.
   - Click **Schedule** to upload the audio file at the scheduled time.

   Note:

   Until the transfer is complete, do not delete the file. The file transfer operation fails if you delete the file that you want to transfer.

   Using the file transfer capability, you cannot upload PLDS license files. For information about uploading a PLDS license file to the IP Office Application Server or UCM device, see *Deploying IP Office in an Avaya Aura® Branch Environment*. For uploading files to System Manager, see Uploading files to the System Manager repository. To delete a file, see Deleting an uploaded file.
8. To check the status of the file transfer, click **Services** > **Scheduler**.

Related links

Uploading files to the System Manager repository on page 768
Deleting an uploaded file on page 769
UCM or Application Server file transfer field descriptions on page 762

UCM or Application Server file transfer field descriptions

Select File Type

Name	Description
File Type	Select the type of file that you want to upload to the UCM or Application Server device. The options are: • **Custom Prompts**: Uploads the audio files to the UCM or Application Server device. • **Other**: Transfers other files such as phone settings, firmware files, and other UCM or Application Server files.

Select Files to Upload (Audio Files)

Name	Description
wav Audio File Name	The file name of the `.wav` type of audio file.
Last uploaded time of wav	The time when you last uploaded the `.wav` audio file in the system.

Select Files to Upload (Other files)

Name	Description
File Name	The name of the file that you want to upload to the UCM or Application Server device.

Enter Destination Folder Location to Push Files

Name	Description
Unified Communication Module / Application Server Destination Folder Location	The UCM and Application Server location of the `Custom Prompt` file. The default value for audio file location is `VMProCustomPrompts`. For other files, provide the location of the UCM and Application Server device. The default location for other files is `system\primary\`.

Select UCM (s) or Application Server(s)

Name	Description
Device Name	The name of the UCM and Application Server device where you want to upload the file.
IP Address	The IP address of the UCM and Application Server device where you want to upload the file.
System Type	The type of the system associated with the UCM and Application Server device.

Table continues…

Name	Description
Last Operation on Device	The last operation that you performed on the UCM and Application Server device.
Status	The status of the file transfer.
System Configuration Template	The current UCM or Application Server system configuration template that exists on the UCM or Application Server device.
Last Modified Time of System Configuration	The last time you modified the System Configuration template.
Last Backup Time	The last time you performed the backup operation for this system configuration.

Button	Description
Commit	Uploads the audio file or other file to the UCM or Application Server device.

Voice Mail Pro Call Flow and System Configuration

Viewing the Voice Mail Pro call flow

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **VMPro** > **Call Flow**.
3. On the VMPro Call Flow page, select the **Voice Mail Pro** device whose call flow you want to view.
4. Click **View**.

   The system starts the Voicemail Pro Client application in Offline and Read only mode.
5. To exit Voicemail Pro Client , click **File** > **Exit**.

   The system displays the VMPro Call Flow page.

Editing the Voice Mail Pro call flow

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **Applications**.
3. In the left navigation pane, click **VMPro** > **Call Flow**.
4. On the VMPro Call Flow page, select the IP Office device whose call flow you want to edit.
5. Click **Edit**.

   The system starts the Voicemail Pro Client application in Offline and Editable mode.

6. Do one of the following:
    - To exit Voicemail Pro Client without saving, click **File** > **Exit**.
    - To return to the Voicemail Pro Client page after saving, click **File** > **Save and Make Live**.

    The system displays the VMPro Call Flow page.

Downloading the Voice Mail Pro call flow

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **Applications**.
3. In the left navigation pane, click **VMPro** > **Call Flow**.
4. On the VMPro Call Flow page, select the IP Office device whose call flow you want to edit.
5. Click **Download**.
6. Do one of the following:
    - For Firefox, click **Save File** and click **OK**.

      The system saves the configuration file with the device name to the default location.
    - For Internet Explorer, provide the file name and location, and click **Save**.

      The system saves the configuration file to the default location.

Viewing the status of a Voice Mail Pro call flow

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **Applications**.
3. In the left navigation pane, click **VMPro** > **Call Flow**.
4. On the VMPro Call Flow page, select the **Voice Mail Pro** device whose call flow status you want to know.
5. Click **Status**.

    The system refreshes the VMPro Call Flow page and displays the status of the VMPro call flow in the Status column.

Saving Voice Mail Pro call flow as a template

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **VMPro** > **Call Flow**.
3. On the VMPro Call Flow page, select the **Voice Mail Pro** device whose call flow you want to save as a template.

4. Click **Save As Template**.
    a. Type the name for the Voice Mail Pro call flow template.
    b. Select the version.
    c. Click **Commit**.
5. On the System Manager web console, click **Services** > **Templates**.
6. In the left navigation pane, click **VMPro Callflow Template**.

    The VMPro Call Flow Templates page displays the VMPro call flow that you saved as a template.

VMPro Call Flow field descriptions

Device List

Name	Description
Device Name	The name of the IP Office device.
IP Address	The IP Address of the IP Office device.
Device Version	The version name of the IP Office device.
Last Operation on Device	The name of last operation performed on the IP Office device.
Status	The status of the IP Office device.
VMPro Call Flow Template	The name of the VMPro Call Flow Template applied to the IP Office device.
Last Modified Time of System Configuration	The time when the system configuration was last modified.
Last Backup Time	The time of the last back up.

Button	Description
View	Click to view the Voice Mail Pro call flow field descriptions.
Download	Click to download the Voice Mail Pro call flow field descriptions.
Save As Template	Saves the Voice Mail Pro call flow field descriptions as a template.
Edit	Click to edit the Voice Mail Pro call flow field descriptions.
Status	Displays the status of the operation that is currently running on or was last run.

Viewing the Voice Mail Pro system configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.

2. In the left navigation pane, click **VMPro** > **System Configuration**.
3. On the VMPro System Configuration page, select the IP Office device whose system configuration you want to view.
4. Click **View**.

   In the right pane, in the Voicemail Pro - System Preferences window, you can view the details of the selected **Voice Mail Pro** system configuration.

   The system starts **Voice Mail Pro** in **Read Only** mode.

Next steps

For Voice Mail Pro system preferences, see *Implementing Voice Mail Pro*.

Editing the Voice Mail Pro system configuration

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **VMPro** > **System Configuration**.
3. On the VMPro System Configuration page, select the **Voice Mail Pro** device whose system configuration you want to edit.
4. Click **Edit**.

   The system displays Voicemail Pro - System Preferences page.
5. In the right pane, on the Voicemail Pro - System Preferences page, edit the required fields.
6. Do one of the following:
   - To save the modifications, click **Update** .
   - To save the modification and exit, click **Save and Exit**.

Next steps

For Voice Mail Pro system preferences, see *Implementing Voice Mail Pro*.

Saving Voice Mail Pro system configuration as a template

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. In the left navigation pane, click **VMPro** > **System Configuration**.
3. On the VMPro System Configuration page, select the Voice Mail Pro device whose system configuration you want to save a template.
4. Click **Save As Template**.
   a. Type a name for the Voice Mail Pro system configuration template.
   b. Select the version.
   c. Click **Commit**.

5. On the System Manager web console, click **Services** > **Templates**.
6. In the left navigation pane, click **VMPro System Configuration Template**.

   The VMPro System Configuration Templates page displays the VMPro system configuration that you saved as a template.

VMPro system configuration field descriptions

Button	Description
View	Displays the Voice Mail Pro System Configuration page in read only format.
Edit	Displays the Voice Mail Pro System Configuration page where you can modify details.
Save As Template	Saves the Voice Mail Pro system configuration data as template.

IP Office file transfer

Transferring audio files to an IP Office device

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. Click **File Transfer**.
3. In **Select File Type**, click **Audio**.
4. In **Select Files to Upload**, click the audio file that you want to upload.

   List Audio Files displays the list of audio files that you have uploaded using Manage Audio in IP Office System Configuration Templates.

   In the **IP Office Destination Folder Location** field, the system displays the default location where you want to transfer the file.
5. In **Devices List**, select the IP Office device where you want to upload the audio file.
6. Click **Commit**.
7. On the IP Office File Transfer page, perform one of the following actions:
   - Click **Now** to upload the audio file to the IP Office device.
   - Click **Schedule** to upload the audio file at the scheduled time.

Note:

After you schedule a file transfer do not delete the file until the transfer is complete. The file transfer operation fails if you delete the file you want to transfer.

Using the file transfer capability you cannot upload PLDS license files. See *Deploying IP Office in an Avaya Aura® Branch Environment* to view details on uploading a PLDS license file to the IP Office device, if applicable.

8. To check the status of the file transfer, click **Services** > **Scheduler**.

Transferring files to an IP Office device

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. Click **File Transfer**.
3. In **Select File Type**, click **Other**.
4. In **Select Files to Upload**, select the file you want to upload.
5. In the **IP Office Destination Folder Location** field, enter the location of the IP Office device where you want to transfer the file.
6. From **Select IP Office(s)**, select the IP Office device where you want to upload the file.
7. Click **Commit**.
8. On the IP Office File Transfer page, perform one of the following actions:
   - Click **Now** to upload the greeting file to the IP Office device.
   - Click **Schedule** to upload the greeting file at the scheduled time.

   Note:

   After you schedule a file transfer do not delete the file till the transfer is complete. The file transfer operation fails if you delete the file you want to transfer.

   Using the file transfer capability you cannot upload PLDS license files. See *Deploying IP Office in an Avaya Aura® Branch Environment* to view details on uploading a PLDS license file to the IP Office device, if applicable.
9. To check the status of the file transfer, click **Services** > **Scheduler**.

Uploading files to the System Manager repository

About this task

If you select **Other** as the file type, you can upload files up to 300MB in the System Manager repository.

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. Click **IP Office** > **File Transfer**.
3. In **Select Files to Upload**, select the file that you want to upload to System Manager.
4. Browse to the file in your local computer, and select the file you want to upload.
5. Click **Save**.

   The system displays the uploaded file in the List Uploaded Files table. You cannot upload a file greater than 30MB.

   Note:

   The current versions of Firefox, Google Chrome, Safari, Opera and Android support file size validation, but Internet Explorer 9.0 does not support file size validation. Internet Explorer 10.0 is likely to support file size validation.

Deleting an uploaded file

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. Click **IP Office** > **File Transfer**.
3. In **Select File Type**, click **Other**.
4. In **List Uploaded Files**, select the files that you want to delete.
5. Click **Delete**.

IP Office file transfer field descriptions

Select File Type

Name	Description
File Type	Select the type of file you want to upload to the IP Office device. The values are: • Audio: Uploads the audio files to the IP Office device. • Other: Transfers other files such as phone settings, firmware files, and other IP Office files.

Select Files to Upload (Audio Files)

Name	Description
wav Audio File Name	The file name of the `.wav` type of audio file.
Last uploaded time of wav	The time when you last uploaded the `.wav` audio file in the system.
Recording Label	The recording label of the `.wav` file.
c11 Audio File Name	The file name of the `.C11` type of audio file.
Last converted time of wav to c11	The time when you last converted a `.wav` file to a `.C11` audio file.

Select Files to Upload (Other files)

Name	Description
File Name	The name of the file that you want to upload to the IP Office device.

Enter IP Office Destination Folder Location to Push Files

Name	Description
IP Office Destination Folder Location	The IP Office location of the auto attendant file. The default value for audio is `SYSTEM\DYNAMIC\LVMAIL\AAG\`. For other files, provide the location of the IP Office device. The default location for other files is `SYSTEM\PRIMARY\`.

Select IP Office(s)

Name	Description
Device Name	The name of the IP Office device where you want to upload the file.
IP Address	The IP address of the IP Office device where you want to upload the file.
System Type	The type of the system associated with the IP Office device.
Last Operation on Device	The last operation that you performed on the IP Office device.
Status	The status of the file transfer.
System Configuration Template	The current IP Office System Configuration template that exists on the IP Office device.
Last Modified Time of System Configuration	The last time you modified the System Configuration template.
Last Backup Time	The last time you performed the backup operation for this system configuration.

Button	Description
Commit	Uploads the audio file or other file to the IP Office device.

Initiating manual failback

Failback policy

The failback policy feature is used to determine how the Centralized SIP phones failback to normal operation after connectivity to Avaya Aura® Session Manager is restored. You must use two different parameters to configure this feature. One parameter is the global failback policy parameter that is configured through Avaya Aura® System Manager for the Session Manager and impacts all Session Manager SIP phones in the enterprise. The other parameter is the IP Office failback policy parameter that is configured on each IP Office and impacts the operation of that IP Office. The settings for these two parameters must match.

The global failback policy parameter configured in System Manager can be set to Auto (the default) or Manual. The setting is applied to all phones in all branches in the network. It cannot be set per-branch. When set to Auto, the centralized SIP phones will automatically failback to normal (sunny-day) operation when connectivity to Session Manager is restored. In addition, for networks that include two Session Managers for redundancy, when connection to the primary Session Manager is lost, failback from the secondary Session Manager to the primary Session Manager will occur automatically when the primary Session Manager comes back into service.

When the global failback policy is set to Manual, the failback to normal operation must be initiated manually when connectivity to Session Manager is restored. For networks that include two Session Managers for redundancy, when connection to the primary Session Manager is lost, failback from the secondary Session Manager to the primary Session Manager must also be performed manually when the primary Session Manager comes back into service.

The option to set the global failback policy to Manual is provided because there may be occasions when you do not want the SIP phones to automatically failback to normal operation when connectivity to Session Manager is restored. For example, if the network is experiencing constant fluctuations causing frequent switching between the Sunny day and Rainy day mode with service interruptions during the transitions, you might want to first verify the network is stable before failback to normal operation occurs. When you set the global failback policy to Manual, you can manually initiate the failback after you determine that the network is stable.

Initiating failback

Before you begin

You must configure the failback settings in the IP Office manager.

Procedure

1. On the System Manager web console, click **Elements** > **IP Office**.
2. Click **Initiate Failback**.
3. On the IP Office Manual Failback page, select the devices for which you want to initiate manual failback.

   System Manager lists only those devices that have manual failback settings.
4. Perform one of the following actions:
   - Click **Now** to initiate manual failback.
   - Click **Schedule** to initiate manual failback at the scheduled time.

IP Office failback field descriptions

Name	Description
Device Name	The name of the IP Office device with manual failback configuration.
IP Address	The IP address of the IP Office device with manual failback configuration.
System Type	The type of system associated with the IP Office device.
Last Operation on Device	The latest operation you performed on the IP Office device.
Status	The status of the operation that you performed last on the IP Office device.
System Configuration Template	The current IP Office System Configuration template that exists on the IP Office device.
Last Modified Time of System Configuration	The last time you modified the System Configuration template.
Last Backup Time	The last time you performed the backup operation for this system configuration.

Button	Description
Now	Click to initiate failback for the devices you have selected.
Schedule	Click to schedule failback for the devices you have selected.

Upgrading IP Office

Overview of managing software

Use Manage Software from **Services** > **Solution Deployment Manager** to:

- Analyze the current software and get recommendations on the available version for the device.
- Download the compatible software and upgrade the devices.
- Collect the inventory and the components of a device in System Manager using **Get inventory**.
- Upgrade IP Office, Unified Communications Module (UCM) and Application Server devices
- Install software patches for IP Office, Unified Communications Module (UCM) and Application Server devices

Get inventory

Before you begin

Enable SNMP so that the devices are discovered for upgrades. Set the corresponding SNMPv1 communities for the devices in System Manager through **Inventory** > **Manage Elements**.

Important:

Configure SNMP parameters on the device before you configure the same device in System Manager. You must use the same SNMP credentials for the device in System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Manage Software**.
5. On the Manage Software page, Click **IP Office** > **Get Inventory** to obtain the inventory for the IP Office devices.
6. Perform one of the following actions:
   - Click **Now** to collect the inventory or the components of the device.
   - Click **Schedule** to get the inventory at a later time.

Analyzing the software

Before you begin

Get the inventory

Configure user settings

Ensure that the inventory is populated.

About this task

Using the analyze feature, you can identify if a new software is available for the inventory, and if you have permissions to download the software.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Manage Software**.
3. On the Manage Software page, click **IP Office** > **Analyze** > **Now** to analyze if any new IP Office software is available.

   Click **Analyze** > **Schedule** to perform the operation at a later time.

Downloading the software

About this task

You can download the software releases that you are entitled from Avaya PLDS, or from an alternate source to System Manager.

Before you begin

Refresh the elements in the inventory.

Analyze the software.

Create a software library.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. **(Optional)** In the left navigation pane, click **Manage Software**.
3. On the Manage Software page, click **IP Office**, select a device, and click **Download**.

   The system displays the File Download Manager page where the required download files are listed.
4. To change the display settings, click one of the following:
   - **Tree View**: To view the list of elements in the tree format. The system displays each element with the list of components associated with the element that you selected.

- **List View**: To view the list of elements in the list format. Every element is displayed individually.

5. In **Select Software/Hardware Types**, select the software or firmware that you want to download.
6. Click **Show Files**.
7. In **Select Files Download Details**, do the following:
    a. In **Source**, click the source from which you want to download the files.

       The options are Avaya PLDS/Alternate Source and My Computer.

    b. Select the files that you want to download.

    c. Click **Download**.

Result

In **File Download Status**, the system displays the file that you selected for download.

Upgrading an IP Office device

Before you begin

- Obtain the inventory.
- Analyze the software.
- Download the software.

For preupgrade tasks that you must complete, see Solution deployment and upgrade.

About this task

Use the procedure to upgrade IP Office, UCM, and Application Server devices and their components.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Manage Software**.
3. On the Manage Software page, perform one of the following:
    - To update **IP Office**, click **IP Office**.
    - To upgrade UCM or Application Server, click **IP Office** > **UCM or IP Office Application Server**.
4. Select the device that you want to upgrade, and click **Upgrade**.

   Note:

   The **Upgrade** button is available only if the analyze operation is complete.
5. On the Download Manager page, in the **Release** column, select a version.

You can configure a specific version other than the recommended version by selecting an option of your choice from the field.

6. In the **Library** field, select the software library.

   ❗ **Important:**

   The system lists only those software libraries with the HTTP protocol.

7. Click one of the following:

   - **Now**: To upgrade the device immediately.
   - **Schedule**: To upgrade the device at a specified time.

   Status on the IP Office page displays the status of the upgrade. Click the status of the IP Office device to view the logs and the description of the upgrade operation.

   ✱ **Note:**

   When you upgrade B5800 Branch Gateway to IP Office, the **Status** in the Operation Status table displays **Processing**. After the upgrade is successful, the system continues to display **Processing** in the **Status** column.

   On the IP Office page, in the second table, the system displays the **Status** as IDLE for the device that you upgraded. The **Current Version** displays the new version of the IP Office device. This information indicates that the upgrade was successful.

   You cannot downgrade an IP Office device by using Solution Deployment Manager. Use the IP Office Manager to downgrade an IP Office. For more information on downgrading an IP Office device, see the IP Office documentation.

Chapter 12: Managing backup and restore

Backup and restore

Use the backup and restore functionality of System Manager to back up and restore the data and configuration files. The data and configuration files for the entire system are kept centrally on System Manager.

Note:

Release 7.0 does not support deployments or upgrades on System Platform. Therefore, for System Manager upgrades by using data migration utility, create a backup of System Manager configuration files and the System Manager database only from the System Manager web console.

You can perform either a backup or a restore operation at a specified time. The restore operation fails if a backup operation is in progress. When a restore operation is in progress, the system skips all backup jobs that you scheduled.

You can restore the data on System Manager that has the same software version and IP address or FQDN as that of System Manager on which you created the backup.

The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

To perform the backup and restore operations, you must map the user to the role with the following permissions:

Resource type	Permissions
OnDemand	add
All elements of type:SMGR Core Services	backup and restore
All elements of type:alarmoperation	view and modify
All elements of type:elements	add, change, delete, and view

For instructions to create a custom role, see Adding a custom role.

Note:

While restoring backup on System Manager with different Out of Band Management network details, the restore operation fails at validation phase.

Disk space management for System Manager backup

Ensure that sufficient disk space is available before you create a local backup.

The system generates an alarm when the disk space reaches the threshold value. On the System Manager web console, you can configure the disk space and threshold value on the View Profile:SMGR Element Manager page from **Settings** > **SMGR** > **SMGR Element Manager**.

When the system runs out of disk space, the system deletes the older backup files to accommodate the new backup files.

For scheduled backups, the system cleans the backup files that local scheduled jobs create every 24 hours. If the number of backup files for each job exceeds 10, the system deletes the older backup files from the file system and removes the corresponding entry from the database.

For remote scheduled backups, the system removes the entries of older backup archive files from the database. However, the system does not delete the backup archive files from the file system.

When a local backup job is running and disk space reaches the maximum limit, the backup job fails. The system displays a message about the insufficient disk space and suggests you to remove older backup files to create additional disk space.

Related links

Disk space required for backup on page 787

Backup and restore on System Manager that is configured for Geographic Redundancy

When you create a backup of the System Manager data or restore the data on System Manager that is configured for Geographic Redundancy, you must understand the following facts:

- The secondary System Manager that is in the standby mode does not display the **Backup and Restore** link on the web console.
- You can view the backups that you created on a standalone System Manager only on the web console of that standalone System Manager and after you convert the standalone server to primary System Manager server.
- You can view the backups that you created on a primary System Manager only on the web console of that primary System Manager.
- You can view the backups that you created on a secondary System Manager only on the web console of that secondary System Manager.
- You can restore the backup data from System Manager that is configured for Geographic Redundancy on a standalone System Manager. However, you cannot restore the backup data from a standalone System Manager on System Manager that is configured for Geographic Redundancy.

- You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.
- After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.
- When you enable the Geographic Redundancy replication, the system replicates the backup job that is scheduled on the primary System Manager as the scheduled backup job on the secondary System Manager. The subsequent scheduled backup job runs on both the primary and secondary System Manager separately.

Accessing the Backup and Restore service

Procedure

On System Manager Web Console, click **Services** > **Backup and Restore**.

✱ **Note:**

The secondary System Manager that is in the standby mode does not display the **Backup and Restore** link on the web console.

Result

The system displays the Backup and Restore page.

Related links

Backup and restore on page 777

Viewing list of backup files

Procedure

On the System Manager web console, click **Services** > **Backup and Restore**.

Result

The system displays the Backup and Restore page with the list of backup files.

Related links

Backup and Restore field descriptions on page 789

Creating a data backup on a local server

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local**.
4. In the **File name** field, enter the backup file that you want to create.
5. Click **Now**.

   If the backup is successful, the Backup and Restore page displays `Backup job submitted successfully. Please check the status detail below!!`

Related links

Backup and restore on System Manager that is configured for Geographic Redundancy on page 778

Backup field descriptions on page 790

Creating a data backup on a remote server

Before you begin

Ensure that the backup server supports the required algorithms for the System Manager remote backup. For more information, see Supported ciphers, key exchange algorithms, and mac algorithms.

System Manager requires password authentication to enable the Remote Backup Servers for the successful backups.

Note:

Other mechanisms such as Keyboard-Interactive and public key based support are not supported.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - Perform the following:
     a. In **File transfer protocol**, click `SCP` or `SFTP`.
     b. Enter the remote server IP address, remote server port, user name, password, and name and the path of the backup file that you create.

- Select the **Use Default** check box.

  Important:

  To use the **Use Default** option, provide the remote server IP address, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations**and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

5. Click **Now**.

   If the backup is successful, the Backup and Restore page displays `Backup job submitted successfully. Please check the status detail below!!`

Related links

Backup and restore on System Manager that is configured for Geographic Redundancy on page 778
Supported ciphers, key exchange algorithms, and mac algorithms on page 788
Backup field descriptions on page 790

Scheduling a data backup on a local server

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local**.
4. In the **File name** field, enter the name of the backup file that you want to create.
5. Click **Schedule**.
6. On the Schedule Backup page, specify the following details in the appropriate fields:
   - Job name
   - Date and time when the system must run the job
   - Frequency at which the system must run the job
   - Range
7. Click **Commit**.

Related links

Backup field descriptions on page 790
Schedule Backup field descriptions on page 791

Scheduling a data backup on a remote server

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
   - Select the **Use Default** check box.

     Important:

     To use the **Use Default** option, provide the remote server IP address, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations**and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
5. Click **Schedule**.
6. On the Schedule Backup page, specify the following details in the appropriate fields:
   - Job name
   - Date and time when the system must run the job
   - Frequency at which the system must run the job
   - Range
7. Click **Commit**.

Related links

Supported ciphers, key exchange algorithms, and mac algorithms on page 788
Backup field descriptions on page 790
Schedule Backup field descriptions on page 791

Editing a scheduled backup job

To change the backup parameters of a scheduled backup, delete the scheduled backup job and schedule a new backup with the required parameters.

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Click **Pending Jobs**.

3. On the Pending Jobs page, select the backup job.
4. Delete the backup job.

   For instructions to delete the scheduled backup job, see Deleting the scheduled backup job.
5. Schedule a new backup job with the changed parameters using one of the following procedures:
   - Scheduling a data backup on a local server.
   - Scheduling a data backup on a remote server.

Related links

Scheduling a data backup on a remote server on page 782
Scheduling a data backup on a local server on page 781
Deleting the scheduled backup job on page 783

Deleting the scheduled backup job

Before you begin

Log on to the system as an administrator.

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Click **Pending Jobs**.
3. On the Pending Jobs page, select the backup job that you must delete.
4. Perform one of the following steps:
   - If the backup job that you must delete is currently running, click **More Actions** > **Stop** to stop the job.
   - If the backup job that you must delete is in the enabled state, click **More Actions** > **Disable** to disable the job.

     For instructions, see Disabling a job on page 1015.
5. Click **Delete**.
6. On the Delete Confirmation page, click **OK**.

   System Manager deletes the backup job from the database.

Next steps

You can create a new scheduled backup job from **Services** > **Backup and Restore**.

Related links

Editing a scheduled backup job on page 782

Restoring data backup from a local server

About this task

Note:

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Local**.
4. In the **File name** field, type the file name that you must restore.

   If the file name does not appear in the list, specify the absolute path to the backup file and the file name that you must restore.

   Note:

   The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

5. Click **Restore**.

   On the Restore Confirmation page, the system displays the following message:

   ```
   The Restore operation will terminate all sessions and no services
   will be available until the operation completes. So, the System
   Manager console will not be available for approximately 45 minutes
   but this time may vary based on Database size. Click on Continue to
   go ahead with the Restore operation or click on Cancel to abort the
   operation.
   ```

6. Click **Continue**.

   The system logs you out of the System Manager web console and then shuts down.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Related links

Backup and restore on System Manager that is configured for Geographic Redundancy on page 778

Restore field descriptions on page 792

Restoring a backup from a remote server

About this task

Note:

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

To restore the original system at any point of time, you must restore the backup on the same release and the same software patch of that of the original System Manager. For example, if you have created a backup of System Manager xyz with 1234 software patch installed, System Manager on which you restore the backup must run xyz that has 1234 software patch installed.

If the System Manager release on which you restore the backup does not match, the restore operation fails.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Remote**.
4. To specify the file name for the restore operation, perform one of the following:
   - Click the Backup List tab, and select a file name.

     Use this method if the path of the backup file on the remote server is valid, and the credentials used while creating the backup file is unaltered.
   - Click the Parameterized Restore tab, enter a valid file name, the file transfer protocol, the remote server IP address, remote server port, user name, and the password to access the remote computer in the respective fields.

     Note:

     The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.
   - Click the Parameterized Restore tab, select the **Use Default** check box.

     Important:

     To use the **Use Default** option, provide the remote server IP address, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations**and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
5. Click **Restore**.

   On the Restore Confirmation page, the system displays the following message:

   ```
   The Restore operation will terminate all sessions and no services
   will be available until the operation completes. So, the System
   ```

```
Manager console will not be available for approximately 45 minutes
but this time may vary based on Database size. Click on Continue to
go ahead with the Restore operation or click on Cancel to abort the
operation.
```

6. Click **Continue**.

   The system logs you out of the System Manager web console and then shuts down.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Related links

Backup and restore on System Manager that is configured for Geographic Redundancy on page 778

Restore field descriptions on page 792

Restoring the backup through the command line interface

Before you begin

Start an SSH session and provide the correct IP address and the port number.

About this task

You can restore the data through the command line when the machine is in an unstable state and the system does not display the Web console.

Procedure

1. Log in to System Manager using the command line interface as root.
2. At the prompt, type `$MGMT_HOME/pem/fileRestoreCLIUtility`.
3. In the `restorecli.properties` file, enter the build number of the machine in the **version** field.
4. In the properties file, ensure that `fq_backup_file_name` displays the complete path of the backup zip file.
5. In the `fileRestoreCLIUtility.properties` file, ensure that `backup_name` points to the backup zip file.
6. Type `sh $MGMT_HOME/pem/fileRestoreCLIUtility/file_restore.sh<full path of fileRestoreClIUtility><0/1>`

   Where, *0* denotes only the file restore and *1* denotes a full restore.

Note:

The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

7. Complete the steps on the screen to perform the restore operation successfully.

Disk space required for backup

Table 8: System Manager backup file size

Number of users	Database size	Approximate backup file size	
		System Manager	
		Local	Remote
1k	524MB	27M	27M
5k	2253MB	29M	29M
25k	2774MB	34M	34M
50k	4066MB	42M	42M
75k	5601MB	49M	49M
100k	6482MB	56M	56M
150k	7855MB	69M	69M
200k	8219MB	81M	81M
250k	8537MB	94M	94M

Time duration for backup and restore

Backup and Restore Time Duration		
Number of users	System Manager	
	Backup	Restore
1k	57 sec	22 min 41 sec
5k	1 min 15 sec	36 min 23 sec
25k	1 min 46 sec	48 min 23 sec
50k	2 min 03 sec	50 min 27 sec
75k	2 min 32 sec	56 min 11 sec

Table continues…

Backup and Restore Time Duration		
Number of users	System Manager	
	Backup	Restore
100k	2 min 54 sec	1 hr 4 min 03 sec
150k	4 min 02 sec	1 hr 6 min 52 sec
200k	4 min 55 sec	1 hr 14 min 40 sec
250k	5 min 54 sec	1 hr 20 min 40 sec

Supported ciphers, key exchange algorithms, and mac algorithms

For a successful System Manager remote backup, the remote backup server must support at least one algorithm from each of the following categories:

- Kex algorithms
  - diffie-hellman-group1-sha1
  - diffie-hellman-group-exchange-sha1
- Encryption algorithms for Client to Server
  - aes128-cbc
  - twofish192-cbc
  - cast128-cbc
  - twofish256-cbc
  - twofish128-cbc
  - 3des-cbc
  - blowfish-cbc
  - aes256-cbc
  - aes192-cbc
- Mac algorithm for Client to Server
  - hmac-sha1
  - hmac-md5

Backup and Restore field descriptions

Name	Description
Operation	The type of operation. The values are: • Backup • Restore
File Name	• For the backup operation, the name of the backup file. • For the restore operation, the name of the backup file that was used for the restore.
Path	• For the backup operation, the path of the backup file. • For the restore operation, the path of the backup file that was used for the restore.
Status	The status of the backup or restore operation. The values are: • SUCCESS • FAILED • PLANNED • RUNNING
Status Description	The error details of the backup or restore operation that has failed.
Operation Time	The time of the backup or restore operation.
Operation Type	Defines whether the backup or restore operation is local or remote.
User	The user who performed the operation.

Button	Description
Backup	Opens the Backup page from where you can backup the System Manager data.
Restore	Opens the Restore page from where you can restore the data to System Manager.

Backup field descriptions

Name	Description
Type	The type of computer on which you can back up the application data. The options are: • **Local**: The system backs up the data on a local computer. • **Remote**: The system backs up the data on a remote computer.

The page displays the following fields when you choose to create a backup of System Manager data in a location that is local to the System Manager file system.

Name	Description
File Name	The file name that identifies the backup. System Manager creates a backup file in the home directory of the specified user.

The page displays the following fields when you choose to create a backup of the System Manager data on a remote server.

Name	Description
Use Default	The option to use the default configured values. To use the **Use Default** option, provide the remote server IP address, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations**and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
File transfer protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.
Remote Server IP	The IP address of the remote server.
Remote Server Port	The SSH port of the remote server.
User Name	The user name for logging into the remote server.
Password	The password for logging on to the remote server.
Test Credentials	Validates the login credential. The validation gives the connection result with the remote backup server.
File Name	The absolute path to the backup file and the file name. For example, `home/admin/smgr_backup_filename`. You can specify a

Table continues…

Name	Description
	different path for the backup file on the SMGR Element Manager Container page. To open the SMGR Element Manager Container page, click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

Button	Description
Now	Creates a backs up of the data in the specified location immediately.
Schedule	Displays the Schedule Backup page where you can enter the details to schedule a backup.
Cancel	Closes the Backup page and returns to the Backup and Restore page.

Schedule Backup field descriptions

Use this page to schedule a job for backing up data by specifying the date and time.

Job Details

Name	Description
Job Name	The name of the job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	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 time interval of recurrence. The options are: • Execute task one time only. • Tasks are repeated.
Range	The settings define the number of recurrences or date after which the job stops to recur. The options are: • No End Date • End After occurrences • End By Date

Button	Description
Commit	Schedules the backup job.
Cancel	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.

Field	Description
Type	The type of computer from where you restore the application data. The options are: • **Local**. The data is restored from a local machine. • **Remote**. The data is restored from a remote machine.

The page displays the following fields, when you select **Local** as **Type**.

Field	Description
Select File Name	The list of files from where you select the backup file that you must restore.
File Name	The name of the backup file that you must restore. If the system does not display the file that you must restore, specify the complete path of the backup file. **Note:** The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

Backup List

The page displays the following fields when you select **Remote** as **Type**.

The **Backup List** tab displays the list of remote backup files that are created using the SFTP or SCP protocol. Select a backup and click the **Parameterized Restore** tab to change the restore details. For example, if the location of a backup file is modified, specify the correct location of the file in the **File Name** field.

Parameterized Restore

The page displays the following fields when you select **Remote** as **Type**.

Field	Description
File Name	The name and complete path of the backup file that you want to restore.
File transfer protocol	The protocol that you can use to restore the backup. The values are SCP and SFTP.
Remote Server IP	The IP address of the SFTP or SCP server.
Remote Server Port	The SSH port of the SFTP or SCP server.
User Name	The user name for logging in to the SFTP or SCP server.
Password	Password for logging in to the SFTP or SCP server.
Use Default	Select this check box to use the default configured values. To use the **Use Default** option, provide the remote server IP address, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations**and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

Button	Description
Restore	Restores the data from the specified backup file.
Cancel	Cancels any operation in progress, closes the Restore page, and opens the Backup and Restore page.

Chapter 13: Bulk import and export

Using System Manager, you can import and export user profiles and elements. The system performs the bulk import of data using an XML file that is validated against an XML schema definition or an Excel file that System Manager supports. The output of a bulk export operation is an XML file and Excel file.

You can perform the System Manager bulk import through System Manager web console. When you initiate the bulk import function from the Web interface, System Manager schedules the import as a job. The System Manager web console provides the file for bulk import. You can run the job immediately or schedule an import job for a later date or time.

Important:

System Manager does not support import and export of roles in bulk.

You can perform bulk export in System Manager through the web console and the command line interface (CLI).

The System Manager bulk import and export feature supports:

- User-related data. Identity data, communication profile set and handles, communication profiles such as the endpoint data, the Presence profile data, the Messaging data, and the Session Manager data
- Global settings. Public Contact Lists, Shared Addresses, and Default ACLs
- Element data

The following are the key features of the bulk import:

- You can add, modify, and delete user records.
- Supports a maximum of 250000 users in bulk export or import in multiple files.
- You can configure skip, replace, merge, or delete a matching record that already exists.
- You must perform the import task using System Manager web console to bulk import user logs for failed records.
- You can download failed records in an XML file format during bulk import of users. The XML file must conform to the XML schema definition. You can modify and reimport the failed records.
- You can choose the continue on error option if you encounter problem in any record during the import.
- You can perform a complete import or a partial import while importing users. To add a subset of user data, use partial import. For example, you can replace only the communication profile, the

user contact lists, or the user ACLs. When you import new users in the database, you must perform complete import.

Chapter 14: System Manager configuration

Managing data retention rules

Accessing the Data Retention Rules service

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Data Retention**.

   The system displays the Data Retention page with the Rule list.

Result

The system displays the Data Retention page.

Data retention rules

You can configure data retention rules to specify the number of days you want the system to retain the following records:

- Logs
- Backup files
- Cleared alarms
- Aged alarms

Viewing data retention rules

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Data Retention**.

   The system displays the Data Retention page with the Rule list.

Related links

Data Retention field descriptions on page 797

Modifying data retention rules

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Data Retention**.

   The system displays the Data Retention page with the Rule list.
3. Select a rule from the Rule list.
4. Click **Edit**.
5. Modify the value in the **Retention Interval (Days)** field.
6. Click **Update** to save the value.

Related links

Data Retention field descriptions on page 797

Data Retention field descriptions

Use this page to view and edit data retention rules.

Name	Description
Option button	The option to select a data retention rule.
Rule Name	The 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.

Configuring applications

Configuration management

Configuration management provides a configuration repository for System Manager services. Configuration management is responsible for storing configuration data, also called as profiles, for System Manager services and notifying the services of configuration changes.

You can view and edit a profile of a service using Configuration management.

Related links

Edit Profile:SMGR field descriptions on page 811
View Profile SMGR field descriptions on page 810

View Profile: Agent Management field descriptions

Name	Description
Alarm aging keep time	This field is not used for System Manager.
Enterprise auto download	The value in this field specifies whether to enable or disable enterprise auto downloading. The default value is false. If the value is set to true, the enterprise downloads the base rules for all registered agents.
Enterprise customer reference	The customer reference for the Enterprise. For example, Avaya. A value in this field is required only if polling to upstream enterprise is enabled.
Enterprise heartbeat interval	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.
Enterprise heartbeat threshold	The heartbeat threshold in seconds for the Enterprise. A value in this field is required only if polling to upstream enterprise is enabled.
Enterprise platform name	The value in this field specifies a fully-qualified DataTransport address of the host Enterprise. For example: The value of this field will be "avaya.com., Enterprise-dtxjbss01", if the OrganizationFQDN value is "avaya.com." and

Table continues…

Name	Description
	SpiritPlatformQualifier value is "Enterprise-dtxjbss01". A value in this field is required only if polling to upstream enterprise is enabled.
Enterprise tenancy support	This field is for tenancy support of SAL. This field is not used for System Manager.
Enterprise upstream platform name	The value specifies a fully-qualified Data Transport address of the upstream enterprise. 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". A value in this field is required only if polling to upstream enterprise is enabled.
Enterprise upstream polling	The value in this field specifies whether polling upstream enterprise is enabled or not. The default value is false. A false value disables upstream Enterprise polling or Cascading Enterprise.
Inventory aging keep time	This field is not used for System Manager.
Inventory change keep time	This field is not used for System Manager.
Out Of Service delete time	This field is not used for System Manager.

Button	Description
Edit	Opens the Edit Profile: Agent Management page. Use this page to edit the parameters in the Agent Management profile.
Done	Closes the View Profile: Agent Management page.

View Profile: Alarm Management field descriptions

Name	Description
Email from address	The value is the e-mail address of the alarm manager. For example: alarmgr@avaya.com
Email hostname	The value is the name of the SMTP e-mail host. For example, “306181anex4.global.avaya.com”

Table continues…

Name	Description
Email to addresses	The values are comma separated list of e-mail addresses to which alarms are forwarded.
Email user id	The value is the e-mail address of the user.
Federation member platform name	A fully qualified data transport address to which alarms are forwarded. 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".
NMS forward	The value specifies whether alarms are to be forwarded to Network Management System (NMS). The default value is false. If set to true, the SAL forwards the alarms to the NMS
NMS urls	A comma separated list of NMS (Network Management System) URLS. For example, "[155.184.73.11:162]" There are no default values from SAL Enterprise and you need to update them later.
SPIRIT ui url	The URL for gaining access to the SAL Web interface for viewing a specific alarm.
Trouble ticket url	The URL for accessing the Trouble Ticket Web interface. ✱ **Note:** Do not change this value.

Button	Description
Edit	Opens the Edit Profile: Alarm Management page. Use this page to edit the parameters in the Alarm Management profile.
Done	Closes the View Profile: Alarm Management page.

Configuring IP Office

Procedure

1. On the System Manager console, click **Services** > **Configurations**.
2. Click **Settings** > **IP Office** > **Configuration**.
3. On the View Profile: Configuration page click **Edit**.

4. Edit the table properties and general properties in the Edit Profile: Configuration page.
5. Click **Commit**.

IP Office profile field descriptions

IP Office table Properties

Name	Description
Maximum Records for Select All in table	The maximum number of records that is used for selection if **Select All** is used in list pages.
Maximum Records on single page of table	The maximum number of records displayed in the table.

General Properties

Name	Description
Application Prefix	The default value in this field is IPO. This application prefix appears as the prefix in the Communication System Management job names.

Button	Description
Edit	System displays the Edit
Done	Insert a description of what happens when this button is clicked.
Commit	Saves the changes you make on the Edit: Profile page.
Cancel	Cancels your action and takes you to the View: Profile page.

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
Application Prefix	The default value in this field is CSM. This application prefix appears as the prefix in the Communication System Management job names.

Telephony Properties

Name	Description
Clean-up Old Backup Announcement Files interval (Days)	The time between every clean up of the backed up announcement files. The default value is 30 days.
Pre-populate extension values in User Management	Enter `true` in this field if you want the system to pre populate the extension value in User Management, Communication Managercommunication profile.
Incremental sync interval (Hours)	The time between every incremental synchronization. By default, the value for the **incremental_sync_interval_in_hours** field is 24.
Maximum Records for select All in table	The maximum number of records that is used for selection if **Select All** is used in list pages.
Maximum Records on single page of table	The maximum number of records displayed in the table.

Button	Description
Edit	Click to open the Edit Profile:Communication System Management Configuration page. Use this page to edit the parameters in the Scheduler profile.
Done	Click to close the Edit Profile:Communication System Management Configuration page.

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
Application Prefix	The default value in this field is CSM. This application prefix appears as the prefix in the Communication System Management job names.

Telephony Properties

Name	Description
Clean-up Old Backup Announcement Files interval (Days)	The time between every clean up of the backed up announcement files. The default value is 30 days.
Pre-populate extension values in User Management	Enter `true` in this field if you want the system to pre populate the extension value in User Management, Communication Managercommunication profile.

Table continues…

Name	Description
Incremental sync interval (Hours)	The time between every incremental synchronization. By default, the value for the incremental_sync_interval_in_hours field is 24.
Maximum Records for select All in table	The maximum number of records that is used for selection if **Select All** is used in list pages.
Maximum Records on single page of table	The maximum number of records displayed in the table.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the Edit Profile:Communication System Management Configuration page.

View Profile: Event processor field descriptions

Name	Description
EP mechanism class name 1	This field is not used for System Manager.
EP mechanism XSD type	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 <Attributes > element below: 1. The first is a <string> 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. 2. The second is an <string> element named "EPMechanismClassName.N" where N matches

Table continues…

Name	Description
	the appropriate 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>
EP transport address	This field is not used for System Manager.

Button	Description
Edit	Opens the Edit Profile: Event processor page. Use this page to edit the parameters in the Event processor profile.
Done	Closes the View Profile: Event processor page.

View Profile:Configuration field descriptions

Reports cleanup properties

Field	Description
Reports periodic Cleanup Interval (in days)	The interval in days when the system performsthe cleanup. By default, the system deletes reports after 60 days.

Reports Output Directory

Field	Description
Reports Output Directory	The name of the directory where the system saves the reports. The default location is /opt/Avaya/reports_data.
Reports Output Directory Size	The maximum size of the output directory that is allocated on System Manager to save the reports. The maximum size is 1 GB.

Reports Alarm Properties

Field	Description
Raise critical alarm in case Reports Output Directory fills (in percent)	The percentage of space in the output directory when the system must raise a critical alarm. The default is 95%.
Raise major alarm in case Reports Output Directory fills (in percent)	The percentage of space in the output directory when the system must raise a major alarm. The default is 85%.

Table continues…

Field	Description
Raise minor alarm in case Reports Output Directory fills (in percent)	The percentage of space in the output directory when the system must raise a minor alarm. The default is 70%.

Button	Description
Edit	Displays the View Profile:Configuration page. Use the View Profile:Configuration page to configure the **Configuration** parameter.
Done	Closes the View Profile:Configuration page.

View profile:Inventory field descriptions

To navigate to this page, click **Services** > **Configurations** > **Settings** > **Inventory** > **Configuration**.

General Properties

Name	Description
Maximum number of threads for the step Collecting Inventory Information	The maximum number of Java threads created and used for the step Collecting Inventory Information.
Maximum number of threads for the step Probing Network Elements	The maximum number of Java threads created and used for the step Probing Network Elements.
Maximum Records on single page of table	The total number of rows displayed in a table.

Button	Description
Edit	Takes you to the Edit Profile: Configuration page in **Inventory**.
Done	Closes the View Profile: Configuration page.

Edit Profile:Inventory field descriptions

General Properties

Name	Description
Maximum number of threads for the step Collecting Inventory Information	The maximum number of Java threads created and used for the step Collecting Inventory Information.
Maximum number of threads for the step Probing Network Elements	The maximum number of Java threads created and used for the step Probing Network Elements.
Maximum Records on single page of table	The total number of rows displayed in a table.

Button	Description
Commit	Saves the changes and closes the Edit Profile: Configuration page
Cancel	Cancels your action and takes you to the previous page.

View and Edit profile Messaging field descriptions

General Properties

Field	Description
Application Prefix	The text that the system prefixes to the Communication System Management job names. The default is MM.

Telephony Properties

Field	Description
Maximum Records for select All in table	The maximum number of records that the system selects if **Select All** is used in list pages.
Maximum Records on single page of table	The maximum number of records that the system displays in the table.

View Profile: Configuration buttons

Button	Description
Edit	Click to edit the properties in the View Profile: Messaging Configuration page.
Done	Click to go to the previous page.

Edit Profile: Configuration buttons

Button	Description
Commit	Save the changes in the Edit Profile: Messaging Configuration page.
Cancel	Cancels the changes and displays the earlier page.

View Profile: Data Transport Config field descriptions

Name	Description
Connection Avaya production FQDN	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
Connection Avaya production keyAlias	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. This is an optional field.
Connection Avaya production platform qualifier	The value is a logical name for the target enterprise, that applies irrespective of primary of backup. 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.
Connection Avaya production primary URL	The value is a primary URL of the platform
Connection Avaya production useProxy	The value specifies whether to use proxies for this platform or not. The values are true or false.
Connection set	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.
Https session timeout	The value specifies the maximum duration of HTTPS authentication sessions before they need to be re-negotiated.
Max message exchange size	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: • B for bytes • M for megabytes • k for kilobytes

Table continues…

Name	Description
	Note: Do not change the default value unless there is a need.
Max queue memory	The value specifies the maximum amount of memory on disk that the queue can occupy. The following are the units of memory: • B for bytes • M for megabytes • k for kilobytes **Note:** Do not change the default value unless there is a need.
Max send transaction time	The value specifies the maximum amount of time spent in a transaction when trying to send upstream. **Note:** Do not change the default value unless there is a need.
Organization FQDN	The value specifies a fully qualified domain name that uniquely identifies the business organization that the SAL Platform resides in.
Polling interval	The time between polling for messages from each enterprise platform. Specify 0 to turn polling off. The following are the units: • h for Hours • m for Minutes 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.
Proxy address	The domain name or IP address of the proxy to use.
Proxy password	The password to use with the proxy. They are stored in a plain text.
Proxy port	The port of the proxy server.

Table continues…

Name	Description
Proxy type	The type of proxy based on whether the proxy supports HTTP or SOCKS.
Proxy use authentication	The value specifies whether an authentication is required to access the proxy server. The values are true and false. If the value is true, an authentication is required to access the server.
Proxy user	
Server status reset interval	The time between the server marking an URL as unreachable and reattempting to connect to that URL. The following are the units of time: • h for hours • m for minutes • s for seconds
SAL platform qualifier	A logical name for the target Enterprise, that applies irrespective of primary of 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
Edit	Opens the Edit Profile: Data Transport Config page. Use this page to edit the parameters in the Data Transport Configuration profile.
Done	Closes the View Profile: Data Transport Config page.

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.

View Profile SMGR field descriptions

Auto Transliteration Properties

Name	Description
Auto Transliteration Flag	Available options: • True: Enables transliteration. The default is True. • False: Disables transliteration.

Self Provisioning Properties

Name	Description
Self Provisioning Status	The option for the end user to change the H323 and SIP passwords. The options are True and False.

Email Configuration Properties

Name	Description
From Email Address	The email ID that the system uses to send the email.
From Email Password	The email password that the system uses for authentication before sending the email.
Email Host	URL for email server.
Email Host Port	The port for email server. The default port is 25.

Multi Tenancy Properties

Name	Description
Multi Tenancy Status	The status of the Multi Tenancy feature on the system. The available options are: • True: The system enables the Multi Tenancy feature on the system. • False: The system disables the Multi Tenancy feature on the system. The default is False.

Edit Profile:SMGR field descriptions

Auto Transliteration Properties

Name	Description
Auto Transliteration Flag	Available options: • True: Enables transliteration. The default is True. • False: Disables transliteration.

Self Provisioning Properties

Name	Description
Self Provisioning Status	The option for the end user to change the H323 and SIP passwords. The options are True and False.

Email Configuration Properties

Name	Description
From Email Address	The email ID that the system uses to send the email.
From Email Password	The email password that the system uses for authentication before sending the email.
Email Host	URL for email server.
Email Host Port	The port for email server. The default port is 25.

Multi Tenancy Properties

Name	Description
Multi Tenancy Status	The status of the Multi Tenancy feature on the system. The available options are: • True: The system enables the Multi Tenancy feature on the system. • False: The system disables the Multi Tenancy feature on the system. The default is False.

View Profile:Alarming UI field descriptions

Use this page to view the parameters in the Alarming profile.

Color Codes

Name	Description
Cleared	The color code for cleared alarms.
Critical	The color code for critical alarms.
Indeterminate	The color code for the indeterminate alarms. You can change the values to specify a different color code.
Major	The color code for the major alarms.
Minor	The color code for the minor alarms. You can change the values to specify a different color code.
Warning	The color code for the warning alarms. You can change the values to specify a different color code.

Auto Refresh

Name	Description
Time Interval (millisec)	The time interval in milliseconds after which the Alarming module refreshes the alarms on the Alarming page.

Button	Description
Edit	Opens the Edit Profile:Alarming UI page. Use this page to edit the parameters in the Alarming Profile.
Done	Closes the View Profile:Alarming UI page.

Edit Profile:Alarming UI field descriptions

Use this page to edit the parameters in the Alarming profile.

Color Codes

Name	Description
Cleared	The color code for alarms that are cleared.
Critical	The color code for critical alarms.
Indeterminate	The color code for the indeterminate alarms. You can change the values to specify a different color code.
Major	The color code for the major alarms.

Table continues…

Name	Description
Minor	The color code for the minor alarms. You can change the values to specify a different color code.
Warning	The color code for the warning alarms. You can change the values to specify a different color code.

Auto Refresh

Name	Description
Time Interval (millisec)	The time interval in milliseconds after which the Alarming module refreshes the alarms on the Alarming page.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Alarming UI page.

View Profile:Common Console field descriptions

Use this page to view the common console profile.

Note:

For the changes to be effective, log out from the system and log on again to the system.

Name	Description
Max No of tabs that you can open on landing page	The maximum number of tabs that you can open from the Home page. The default is 5. If you set the number to more than 5, for example 7 and open more than 7 tabs, the system displays `You have exceeded the maximum numbers of tabs. Close any one of the tabs to open a new tab.`
Maximum number of user preferences that can be saved and seen on dashboard	The maximum number of user preferences that you can save and view on the Home page. The default is 15.
Number of rows	Number of rows that you want the system to display in a table. The default is 15. The range of minimum rows is 15 and maximum rows is 100.
Max No of Records Selectable (Table)	The maximum number of records that you can select at a time from a table.

Button	Description
Edit	Opens the Edit Profile: Common Console page. Use this page to edit the parameters in the Common Console profile.
Done	Closes the View Profile: Common Console page.

Edit Profile:Common Console field descriptions

Use this page to edit the common console profile.

Note:

For the changes to be effective, log out from the system and log on again to the system.

Name	Description
Max No of tabs that you can open on landing page	The maximum number of tabs that you can open from the Home page. The default is 5. If you set the number to more than 5, for example 7 and open more than 7 tabs, the system displays `You have exceeded the maximum numbers of tabs. Close any one of the tabs to open a new tab.`
Maximum number of user preferences that can be saved and seen on dashboard	The maximum number of user preferences that you can save and view on the Home page. The default is 15.
Number of rows	Number of rows that you want the system to display in a table. The default is 15. The range of minimum rows is 15 and maximum rows is 100.
Max No of Records Selectable (Table)	The maximum number of records that you can select at a time from a table.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation.

View Profile:Shutdown field descriptions

Name	Description
Grace Period (In Minutes)	The time in minutes within which the active users must finish their operations before the administrator shuts down System Manager.

Button	Description
Edit	Displays the Edit. Profile:Shutdown page where you can change the grace period.
Close	Closes the View Profile:Shutdown page.

Edit Profile:Shutdown field descriptions

Field	Description
Grace Period (In Minutes)	The time in minutes within which the active users must finish their operations before the administrator shuts down System Manager.

Button	Description
Commit	Saves the changes that you made on the Edit Profile:Shutdown page.
Cancel	Cancels the changes that you made on the Edit Profile:Shutdown page, and returns to the View Profile :Shutdown page.

View Profile:HealthMonitor field descriptions

HealthMonitor Configuration Parameters

Name	Description
HealthMonitor interval	The time interval, in seconds, within which the Health Monitoring service polls for the information on the system status.
HealthMonitor Retention Days	The number of days the system retains the Heath Monitoring data.
HealthMonitor Retries	The number of successive attempts that the Health Monitoring service makes before the system raises an alarm.

Button	Description
Edit	Opens the Edit Profile:HealthMonitor page. Use the Edit Profile:HealthMonitor page to configure the HealthMonitor parameters.
Done	Closes the View Profile:HealthMonitor page.

Related links

Edit Profile:HealthMonitor field descriptions on page 816

Edit Profile:HealthMonitor field descriptions

Use this page to edit the Health Monitor parameters.

✱ **Note:**

Click **Edit** to open the Edit Profile:HealthMonitor page.

HealthMonitor Configuration Parameters

Name	Description
HealthMonitor interval	The time interval, in seconds, within which the Health Monitoring service polls for the information on the system status.
HealthMonitor Retention Days	The number of days the system retains the Heath Monitoring data.
HealthMonitor Retries	The number of successive attempts that the Health Monitoring service makes before the system raises an alarm.

Button	Description
Commits	Saves the changes you make on the View Profile:HealthMonitor page.
Cancels	Cancels the edit profile operation and takes you back to the View Profile:HealthMonitor page.

Related links

View Profile:HealthMonitor field descriptions on page 815

View Profile:Licenses field descriptions

Name	Description
WebLM Usages UsageCount	This count represents the number of usage reports the server must maintain and display for each WebLM server.
WebLM LicenseAllocation Backup FileSize	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
Edit	Opens the Edit Profile:Licenses (WebLM) page. Use this page to edit the parameters in the WebLM profile.
Done	Closes the View Profile:Licenses (WebLM) page.

Edit Profile:Licenses field descriptions

Name	Description
WebLM Usages UsageCount	This count represents the number of usage reports the server must maintain and display for each WebLM server.
WebLM LicenseAllocation Backup FileSize	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
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Licenses (WebLM) page.

View Profile:Logging UI field descriptions

Log Severity Levels

Name	Description
Alert	The color code for the log messages that are logged under the Alert severity level.
Critical	The color code for the log messages that are logged under the Critical severity level.
Debug	The color code for the log messages that are logged under the Debug severity level.
Emergency	The color code for the log messages that are logged under the Emergency severity level.
Error	The color code for the log messages that are logged under the Error severity level.
Informational	The color code for the log messages that are logged under the Informational severity level.

Table continues…

Name	Description
Notice	The color code for the log messages that are logged under the Notice severity level.
Warning	The color code for the log messages that are logged under the Notice severity level.

Auto Refresh

Name	Description
Time Interval(millisec)	The time interval in milliseconds after which the log messages are auto refreshed on the Logging page .

Button	Description
Edit	Opens the Edit Profile:Logging page. Use this page to edit the parameters in the Logging profile.
Done	Closes the View Profile:Logging page.

Edit Profile:Logging UI field descriptions

Log Severity Levels

Name	Description
Alert	The color code for the log messages that are logged under the Alert severity level.
Critical	The color code for the log messages that are logged under the Critical severity level.
Debug	The color code for the log messages that are logged under the Debug security level.
Emergency	The color code for the log messages that are logged under the Emergency severity level.
Error	The color code for the log messages that are logged under the Error severity level.
Informational	The color code for the log messages that are logged under the Informational severity level.
Notice	The color code for the log messages that are logged under the Notice severity level.
Warning	The color code for the log messages that are logged under the Notice severity level.

Auto Refresh

Name	Description
Time Interval(millisec)	The time interval in milliseconds after which the log messages are auto refreshed on the Logging page.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels 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
Max time interval to wait	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 10800000 milliseconds.
Directory path for harvested files	The directory where all the harvested files are stored. The default path is `/var/log/Avaya/mgmt/downloads`.
No. of Lines/Page(All harvested archives will be re-indexed)	The maximum number of lines that you can view on the log browser page for a harvested log file.
Maximum allowed size of harvest directory (In GB)	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.
No. of files for File rotation	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
Edit	Opens the Edit Logging Service Profile page. Use this page to edit the values of the log harvesting parameters.
Done	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
Max time interval to wait	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 10800000 milliseconds.
Directory path for harvested files	The directory where all the harvested files are stored. The default path is `/var/log/Avaya/mgmt/downloads`.
No. of Lines/Page(All harvested archives will be re-indexed)	The maximum number of lines that you can view on the log browser page for a harvested log file.
Maximum allowed size of harvest directory (In GB)	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.
No. of files for File rotation	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
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Logging Service page.

View Profile: SMGR Element Manager field descriptions

Name	Description
Backup Directory	The name of the directory on the database server where Element Manager creates backup archives. The default directory is `swlibrary/backup`. **Note:** The database user must have write privileges on this directory.
Database Utilities Path	The name of the directory on the database server that contains the PostgreSQL backup and restore utilities.

Table continues…

Name	Description
	Note: The database user must have execute permissions on these utilities.
Database Type	The type of the database. For example, Oracle, Postgres.
Database server	The hostname of the database server.
Database Super-User Password	Database super user password.
Confirm Database Super-User Password	Database super user password that you retype to confirm.
Database Port	The port number for database server.
Database SCP Port	The port on the database server on which the SSH server is running.
Database Super-User	The super user for the database. This user can establish an SSH connection to the database.
Disk Space Allocated (GB)	The disk space allocated for backup archives.
Disk Space Threshold (%)	The percentage of the **diskSpaceAllocated** property. When this percentage is reached, the system generates an alarm. For example, if the **diskSpaceAllocated** is 100 MB and **diskSpaceThreshold** is 90 percent, the system generates an alarm when the disk space occupied by the backup archives reaches 90 MB.
Job Interface URL	The lookup URL for the Element Manager.
Maximum Backup Files	The maximum number of backup files that you can create. The valid values are 1 through 5, and the default is 3. When the maximum limit reaches, the system rotates backup archives.
Maximum Data Retention Limit (days)	The maximum data retention limit in days that you can set for any data retention rule.
Maximum size for log data stored	The maximum size for log data stored. This is the upper limit on the number of records on the log_store table.
Maximum Transaction Timeout Limit (Hours)	The transaction timeout maximum limit in hours.
Remote Utility Directory	The directory on the database server that contains the Element Manager backup or restore utilities.
Scheduler URL	The URL for gaining access to the Scheduler.
Remote Server Password	The password for accessing the SCP server.

Table continues…

Name	Description
	Important: To use the **Use Default** option on the Backup or Restore page, ensure that you specify the remote server IP, user name, password, and name and path of the backup file on this page.
Confirm Remote Server Password	The SCP server password that you retype to confirm.
Remote Server Port	The SSH port for the SCP server.
Remote server	The hostname of the SCP server.
Remote Server User	The username to access the secure access server.

Button	Description
Edit	Displays the Edit Profile:SMGR Element Manager page where you edit System Manager Element Manager Profile parameters.
Done	Closes the View Profile:SMGR Element Manager page.

View Profile:SNMP field descriptions

Avaya IM System Manager subagent attributes

Name	Description
Master Agent IPAddress	IP address of machine on which master agent is running.
Master Agent TCP Port	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 starts listening on the configured TCP port and then the subagent establishes connection with the master agent via this port.
Sub Agent IPAddress	IP address of machine on which sub agent is deployed

View Profile:Scheduler field descriptions

Scheduler Feature

Name	Description
Number Of Retry	A count that defines the number of attempts to start the scheduler MBEAN.
Retry Delay	Delay in time in seconds between each retry.

Scheduler Look Up Details

Name	Description
Initial Context Factory	User name for secured Java Naming and Directory Interface (JNDI).
Naming Server User Name	
Provider URL	The PROVIDER_URL which gives the server name and port on which a service is running. **Note:** This parameter is currently not in use.

Button	Description
Edit	Opens the Edit Profile:Scheduler page. Use this page to edit the parameters in the Scheduler profile.
Done	Closes the View Profile:Scheduler page.

Edit Profile:Scheduler field descriptions

Scheduler Feature

Name	Description
Number Of Retry	A count that defines the number of attempts to start the scheduler MBEAN.
Retry Delay	Delay in time in seconds between each retry.

Scheduler Look Up Details

Name	Description
Initial Context Factory	User name for secured Java Naming and Directory Interface (JNDI).
Naming Server User Name	

Table continues…

Name	Description
Provider URL	The PROVIDER_URL which gives the server name and port on which a service is running. **Note:** This parameter is currently not in use.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and takes you back to the View Profile:Scheduler page.

Configuring the TrapListener service

Procedure

1. On the System Manager console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Settings** > **SMGR**.
3. Click **TrapListener**.
4. On the View Profile: TrapListener Service page, click **Edit**.
5. Edit the required fields in the Edit Profile: TrapListener Service page.
6. Click **Commit**.

Related links

TrapListener service on page 948
TrapListener service field descriptions on page 824

TrapListener service field descriptions

Name	Description
Authentication Password	The password used to authenticate the user. The default is avaya123.
Authentication Protocol	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The options are: • md5 • SHA The default is md5.
Community	The community for TrapListener.

Table continues…

Name	Description
Privacy Password	The password that you use to encrypt the SNMP data. The default is avaya123.
Privacy Protocol	The encryption policy for an SNMP V3 user. The options are: • **DES**: Use the DES encryption for the SNMP-based communication. • **AES**: Use the AES encryption for the SNMP-based communication. The default is AES.
TrapListener Port	The port on which TrapListener listens. The default is 10162. The field is read-only.
V3 UserName	The SNMP V3 user name. The default is initial. Although you can change the SNMP V3 user name, use the default value.

Note:

The system configures the **Privacy Password**, **Authentication Password**, **Users**, and **Community** fields with default values. You must change the values immediately after you deploy System Manager.

Button	Description
Commit	Saves the changes you have made in the **TrapListener Configuration Parameters** section.
Cancel	Cancels the edit and returns to the previous page.

View Profile: TrustManagement field descriptions

Field	Description
Threshold (in days) for raising an alarm for certificate expiration (1-60)	The number of days prior to the certificate expiry when an alarm is generated.
Auto-renew Certificates (true/false)	The status of the auto renewal of certificates from the Trust Management agent. Set this field to True if you want auto renewal of certificates.
Threshold (in days) for triggering auto-renewal of certificates (1-60)	The number of days prior to the certificate expiry when the auto renewal of certificates is triggered.
Preference setting for the signing algorithm to be used by the CA. Valid values - "1" or "2". 1 = Use SHA2 for all certificate requests. 2 = Use SHA2 for 2048-bit or higher keys based certificate	The preference setting for the signing algorithm that CA can use. The valid values are: • **1**: To use SHA2 for all certificate requests.

Table continues…

Field	Description
request. Use SHA1 for 1024-bit keys based certificate requests.	• **2**: To use SHA2 for 2048-bit or higher keys-based certificate request and SHA1 for 1024-bit keys-based certificate request.

Button	Description
Edit	Returns to the Edit Profile: TrustManagement page.
Done	Returns to the previous page.

Edit Profile: TrustManagement field descriptions

Field	Description
Threshold (in days) for raising an alarm for certificate expiration (1-60)	The number of days prior to the certificate expiry when an alarm is generated.
Auto-renew Certificates (true/false)	The status of the auto renewal of certificates from the Trust Management agent. Set this field to True if you want auto renewal of certificates.
Threshold (in days) for triggering auto-renewal of certificates (1-60)	The number of days prior to the certificate expiry when the auto renewal of certificates is triggered.
Preference setting for the signing algorithm to be used by the CA. Valid values - "1" or "2". 1 = Use SHA2 for all certificate requests. 2 = Use SHA2 for 2048-bit or higher keys based certificate request. Use SHA1 for 1024-bit keys based certificate requests.	The preference setting for the signing algorithm that CA can use. The valid values are: • **1**: To use SHA2 for all certificate requests. • **2**: To use SHA2 for 2048-bit or higher keys-based certificate request and SHA1 for 1024-bit keys-based certificate request.

Button	Description
Commit	Saves your changes in the Edit Profile: TrustManagement page.
Cancel	Cancels your changes and takes you to the previous page.

View Profile: User Bulk Import Profile field descriptions

User Bulk Import Module

Name	Description
Default Error Configuration	The value in this field specifies what action the system performs when an error is encountered

Table continues…

Name	Description
	during bulk importing users record in the system. The options are: • **True**: The system skips the erroneous record in the input file and continue to import other records. The default is **True**. If this parameter is set to true, the **Continue processing other records** option is set as the default in the **Select error configuration** field on the Import Users page. • **False**: The system aborts the import operation on encountering the first error in the input file. If this parameter is set to false, the **Abort on first error** option is set as default in the **Select error configuration** field on the Import Users page. To access the Import Users page, click **Manage Users** > **More Actions** > **Import Users**
Enable Error File Generation	The option to generate error file during the importing users job. The options are: • **True**: The system generates an error file for a failed import. • **False**: The system does not generate an error file for a failed import.
Maximum Number of Error records to be displayed	The maximum number of error records that the Job Details page can display for a user import job that has failed to import user records completely or partially. To access the Import Users page, click **Manage Users** > **More Actions** > **Import Users** > **View Job**. Select a failed job from the table before you click **View Job**.
Maximum Number of Job records to be displayed	The maximum number of job records that the system displays on the Import Users page.
Default Action for a matching record	A default action that the system performs when the system finds a matching record in the database while bulk importing users. The options are: • **0**: The system does not import user records from the input file that already exists in the database. If you enter 0, the **Skip** option is set as the default option for the **If a matching record already exists** field on the Import Users page. • **1**: The system appends the records for an attribute.

Table continues…

Name	Description
	If you enter 1, the **Merge** option is set as the default option for the **If a matching record already exists** field on the Import Users page. • **2**: The system replaces the record with the record in the input file if a matching record is found. If you enter 2, the **Replace** option is set as the default option for the **If a matching record already exists** field on the Import Users page. • **3**: The system deletes the records from the database that matches the records in the input file. If you enter 3, the **Delete** option is set as the default option for the **If a matching record already exists** field. To access the Import Users page, click **Manage Users** > **More Actions** > **Import Users**.

Button	Description
Edit	Displays the Edit Profile: User Bulk Import Profile page where you can change bulk import parameters of the user.

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
Default Error Configuration	The action that the system performs when an error is encountered during bulk importing users record in the system. The options are: • ***True***: The system skips the erroneous record in the input file and continue to import other records. This is the default value. If this parameter is set to true, the **Continue processing other records** option is set as the default option for the **Select error configuration** field on the Import Users page. • **False**: The system aborts the importing process on encountering the first error in the input file.

Table continues…

Name	Description
	If this parameter is set to false, the **Abort on first error** option is set as default option for the **Select error configuration** field on the Import Users page. To access the Import Users page, click **Manage Users** > **More Actions** > **Import Users**.
Enable Error File Generation	The option to generate the error file for an import users job. The options are: • **True**: The system generates an error file for a failed import job. • **False**: The system does not generate an error file for a failed import job.
Maximum Number of Error records to be displayed	The maximum number of error records that the Job Details page can display for a user import job that has failed to import user records completely or partially. To access the Import Users page, click **Manage Users** > **More Actions** > **Import Users** > **View Job**. Select a failed job from the table before you click **View Job**.
Maximum Number of Job records to be displayed	The maximum number of job records that the system displays on the Import Users page.
Default Action for a matching record	The default action that the system performs when the system finds a matching record in the database while bulk importing users. The options are: • **0**: The system does not import user records from the input file that already exists in the database. If you enter 0, the **Skip** option is set as default in the **If a matching record already exists** field on the Import Users page. • **1**: The system appends the records for an attribute. If you enter 1, the **Merge** option is set as default in the **If a matching record already exists** field on the Import Users page. • **2**: The system replaces the record with the record in the input file if a matching record is found. If you enter 2, the **Replace** option is set as default in the **If a matching record already exists** field on the Import Users page. • **3**: The system deletes the records from the database that matches the records in the input file.

Table continues…

Name	Description
	If you enter 3, the **Delete** option is set as default in the **If a matching record already exists** field. To access the Import Users page, click **Manage Users** > **More Actions** > **Import Users**.

Button	Description
Edit	Displays the Edit Profile:User Bulk Import Profile page where you can change the user bulk import parameters.

Chapter 15: Managing inventory

Element management

Inventory maintains a repository that records elements deployed on System Manager, including the runtime relationships. An element in the inventory refers to a single instance or clustered instance of a managed element. Inventory provides a mechanism for creating, modifying, searching, and deleting elements and the access point information from the repository. Inventory retrieves information about elements that are added or deleted from the repository.

Inventory integrates the adopting applications with the common console of System Manager. Through Inventory, elements can provide a link that redirects to the webpage of the element manager. Such links appear for only specific element types.

When you deploy an Avaya Aura® application OVA by using Solution Deployment Manager, the system displays the application in the System Manager inventory.

To upgrade an Avaya Aura® application by using Solution Deployment Manager, you must add applications such as Communication Manager, Session Manager, and Branch Session Manager in the inventory.

Note:

You must add Appliance Virtualization Platform or ESXi host from VM Management on Solution Deployment Manager. The system displays Appliance Virtualization Platform or ESXi host on the Manage Elements page.

Note:

On the Manage Elements page, links to Corporate Directory, IPsec, Numbering Groups, Patches, Secure FTP Token, SNMP Profiles, and Software Deployment might not be active. You can gain access to the elements from **Users** > **Administrators**.

Using Manage Elements, you can add elements in the following methods:

- Manually add elements to the System Manager inventory.
- Perform automatic inventory collection from the Discovery tab that automatically adds elements to the System Manager inventory.
- Add elements to the System Manager inventory in bulk from the **More Actions** > **Import** link.

Using Manage Elements you can:

- Add or modify elements

- Delete elements
- Assign and remove entries for elements
- Provide a certificate to an element
- Replace a certificate
- Import elements in bulk

For System Manager Geographic Redundancy:

- Manage or unmanage elements
- Get current status of elements

Manage Elements access

You require access to the **Inventory** > **Manage Elements** page on the System Manager web console. The role must have the following permissions assigned:

For resource type elements, all permissions in the **Role Resource Type Actions** section.

Bulk import

Inventory supports the creation and updation of elements by importing data from an XML file. You can import elements only through the graphical user interface.

Inventory provides the following configuration options for each import operation:

- Abort on first error: The system stops the import operation if any exception occurs.
- Continue processing other records: The system does not stop the import operation even if any exception occurs, and the import operation continues.
- Replace: Reimports all data for the element that you import. The replace function replaces an element and the related data with a new one.
- Merge: Merges the data of an element with the import data from an input XML file.
- Skip: Skips the import operation. As an administrator, you reimport the elements to recover from failures. If you reimport the same file to recover from failures, RTS does not overwrite any record that you have successfully added. Inventory continues to process other records from the file.
- Delete: Deletes an element.
- Schedule: Schedules the import of the element.

Methods to add elements to System Manager

Manual addition of elements

You can manually add an element to the System Manager inventory from the Manage Elements page. For example, System Platform.

You must add the ESXi host from VM Management on Solution Deployment Manager. The system displays the ESXi host on the Manage Elements page.

Related links

Creating a new element on page 833
Creating a new element on page 833

Creating a new element

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Click **New**.
4. On the New Elements page, in the **Type** field, click the element type that you want to create.
5. On the New <element-name> page, on the **General** and **Attributes** tabs, complete the required fields.
6. Click **Commit**.

   The system creates a new element.

Related links

Manual addition of elements on page 832
Creating a new element on page 833

Bulk import of elements

You can add elements to the System Manager inventory in bulk from the Manage Elements page, by using the **More Actions** > **Import** link.

Related links

Importing elements on page 833

Importing elements

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **More Actions** > **Import**.
4. On the Import Elements page, click **Browse** to select the XML file that you want to import.
5. Click **Import**.

Related links

Bulk import of elements on page 833

Discovering elements

Discovery of Avaya Aura® applications and associated devices

To manage and upgrade software from System Manager, you must discover elements in the network. The system performs the discovery by using discovery profiles, where you configure subnetwork, SNMP access profiles, and element types to be discovered.

On the Discovery tab of **Inventory** > **Manage Elements**, you can create discovery profiles and use the profiles to discover elements. The Manage Elements page displays the discovered elements.

You must configure the applicable discovery parameters for System Manager to discover the Avaya Aura® application. System Manager uses SNMPv1 or SNMPv3 to discover Avaya Aura® applications.

For applications such as Communication Manager, you can use SNMP discovery or add the application from Manage Elements.

Note:

To upgrade an Avaya Aura® application by using Solution Deployment Manager, discovery of applications, such as Communication Manager, Session Manager, and Branch Session Manager is a mandatory task.

Creating discovery profiles and discovering elements

Before you begin

Configure the subnetwork profiles, SNMP profiles, and element type profiles on the **Discovery** tab by using the links available at the beginning of the Discovery Profile List page or from the following links:

- **Inventory** > **Subnet Configuration**
- **Inventory** > **Element Type Configuration**
- **Configurations** > **Settings** > **SMGR** > **Global SNMP Configuration**

About this task

You can create discovery profiles and use the profiles to discover elements in System Manager. The Manage Elements page displays the discovered elements.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Click the **Discovery** tab.

   The system displays the Discovery Profile List page.
4. Click **New**.

   The system displays the Create Discovery Profile page.

5. In the **Discovery Profile Name** field, type a name for the discovery profile.
6. In the **Subnet Configurations** section, perform the following:
    a. Click a subnetwork that you configured in **Inventory** > **Subnet Configuration**.
    b. Click an element type that you configured on **Inventory** > **Element Type Configuration**.

       The **Discovery Element Type Access Profiles** column displays all access profiles of an element type.
    c. To select or clear profiles, in the **Choose Element Type Access Profiles** column, click **Choose Element Access**.
    d. In the **Profile List** section, click the global SNMP profile that you configured on **Configurations** > **Settings** > **SMGR** > **Global SNMP Configuration**.
7. Click **Commit**.

   The system displays the new discovery profile on the Discovery Profile List page in the **Discovery Profiles** section.
8. Select the discovery profile and perform one of the following:
    - Click **Discover Now**.
    - To discover the element later, click **Schedule Discovery**, and provide the date and time when the discovery must run.

   The system displays a dialog box with the message `Discovery is Running` and the number of elements that are discovered. The system lists the discovered elements on the Manage Elements page in the **Elements** section. The system closes the dialog box when the discovery is complete.

   While the discovery is in progress, the system blocks any action that you perform on the **Discovery** tab.

Related links

Device list on page 835
Discovery Profile List field descriptions on page 836
Element Access Profile Management field descriptions on page 846
Subnet Configurations field descriptions on page 844
SNMP Access Profiles field descriptions on page 840
Create or Edit Discovery Profile field descriptions on page 837

Device list

The table lists the minimum requirements for an SNMP discovery. For successful discovery, you must configure the following on the Avaya equipment.

Device for discovery	Protocol used	Ports used	Access	Notes
Communication Manager	SNMPv1 and SNMPv3	SSH to 22 or 5022	Direct	-
Session Manager, Branch Session Manager	SNMPv1 and SNMPv3	SSH to 22 or 5022	Direct	
Appliance Virtualization Platform	SNMPv1 and SNMPv3		Direct	Manually added from VM Management
Engagement Development Platform				
Application Enablement Services				
IP Office	SNMPv1	-	-	-
CLAN (TN799DP)	SNMPv1	-	Direct	Static community publicclan read-only and read-write strings
MedPro (TN2302, TN2602)	SNMPv1	-	Through Communication Manager	-
G250, G350	SNMPv1 and SNMPv3	SSH to 22	Direct	-
G430, G450	SNMPv1 and SNMPv3	SSH to 22	Direct	-
G700	SNMPv1	-	Direct	-

Discovery Profile List field descriptions

Discovery Profiles

Field	Description
Discovery Profile	The name of the discovery profile.
Subnet Profiles	The name of the subnetwork profile. For each subnetwork profile name, the system provides a cut-through that displays the subnetwork profile details.
Access Profiles	The name of the access profile. For each access profile name, the system provides a cut-through that displays the access profile details.
Element Types	The element type.

Discovery Job Status

Field	Description
Job Name	The name of the discovery job.
Start Time	The start date and time of the discovery job.
End Time	The end date and time of the discovery job.
Status	The current status of the discovery job.

Button	Description
New	Displays the Create Discovery Profile page where you create a new discovery profile.
Edit	Displays the Edit Discovery Profile page where you can change the discovery profile information.
Delete	Displays the Discovery Profile Delete Confirmation page where you can delete the discovery profile.
Discover Now	Starts the process of discovering the element.
Schedule Discovery	Schedules the discovery process to run at the specified time.

Create or Edit Discovery Profile field descriptions

Field	Description
Discovery Profile Name	The name of the discovery profile.

Subnet Configurations

Field	Description
Name	The name of the subnetwork.
IPaddress	The IP address of the subnetwork.
Mask	The IP subnetwork mask.

Element Type Access Profiles

Field	Description
Element Types	The element type.
Discovery Element Type Access Profiles	The discovery profiles for the element type access.
Choose Element Type Access Profiles	The link to the **Element Type Access Profiles** section where you can select or clear the discovery profiles for the element type access.

Profile List

Field	Description
Profile Name	The name of the profile.
Type	The SNMP protocol type. The options are V1 and V3.
Read Community	The read community of the device. **Read Community** applies only to the SNMP V1 protocol.
Write Community	The write community of the device. **Write Community** applies only to the SNMP V1 protocol.
User	The user name of the SNMP V3 protocol operation.
Auth Type	The authentication protocol to authenticate the source of traffic from SNMP V3 users. The options are: • **MD5** The default is **MD5**. • **SHA** • **None** **Auth Type** applies only to the SNMP V3 protocol.
Priv Type	The encryption policy for an SNMP V3 user. The options are: • **DES**: For SNMP-based communication. The default is **DES**. • **AES**: For SNMP-based communication. • **None**: Does not encrypt traffic for this user. Set **Priv Type** only for an SNMP V3 user.
Privileges	The privileges that determine the operations that you can perform on MIBs. • **Read/Write**: To perform the GET and SET operations. • **Read**: To perform only the GET operation. • **None** The default is **None**.
Timeout	The time in milliseconds for which the element waits for a response from the device that the element polls.

Table continues…

Field	Description
Retries	The number of times that the element polls a device and fails to receive a response. After the retries, the element times out.
Description	A brief description of the profile.

Button	Description
Commit	Saves the changes that you make on the Create Discovery Profile or Edit Discovery Profile page.

Managing SNMP Access Profiles

Adding an SNMP access profile

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Settings** > **SMGR** > **Global SNMP Configuration**.
3. Click **New**.
4. On the New SNMP Access Profile page, perform the following:
    a. In the **Type** field, click the type of the SNMP protocol.

       For more information, see SNMP Access Profile field descriptions.

    b. In the **Profile Name** and **Description** fields, type the name of the profile and a description.

    c. Complete the remaining fields on the page.
5. Click **Commit**.

Related links

SNMP Access Profile field descriptions on page 841
SNMP Access Profiles field descriptions on page 840

Editing the SNMP access profile

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Settings** > **SMGR** > **Global SNMP Configuration**.
3. In the profile list, select the SNMP access profile that you want to change.
4. Click **Edit**.
5. On the Edit SNMP Access Profile page, change the details as appropriate.

   For more information, see SNMP Access Profile field descriptions.
6. Click **Commit**.

Related links

SNMP Access Profile field descriptions on page 841
SNMP Access Profiles field descriptions on page 840

Deleting an SNMP access profile

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Settings** > **SMGR** > **Global SNMP Configuration**.
3. In the profile list, click the SNMP access profile that you want to delete.
4. Click **Delete**.
5. On the Snmp Access Profile/s Delete Confirmation page, click **Delete** to confirm the deletion.

SNMP Access Profiles field descriptions

Field	Description
Profile Name	The name of the profile.
Type	The SNMP protocol type. The options are V1 and V3.
Read Community	The read community of the device. **Read Community** applies only to the SNMP V1 protocol.
Write Community	The write community of the device. **Write Community** applies only to the SNMP V1 protocol.
User	The user name of the SNMP V3 protocol operation.
Auth Type	The authentication protocol to authenticate the source of traffic from SNMP V3 users. The options are: • **MD5** The default is **MD5**. • **SHA** • **None** **Auth Type** applies only to the SNMP V3 protocol.
Priv Type	The encryption policy for an SNMP V3 user. The options are: • **DES**: For SNMP-based communication. The default is **DES**. • **AES**: For SNMP-based communication. • **None**: Does not encrypt traffic for this user.

Table continues…

Field	Description
	Set **Priv Type** only for an SNMP V3 user.
Privileges	The privileges that determine the operations that you can perform on MIBs. - **Read/Write**: To perform the GET and SET operations. - **Read**: To perform only the GET operation. - **None** The default is **None**.
Timeout	The time in milliseconds for which the element waits for a response from the device that the element polls.
Retries	The number of times that the element polls a device and fails to receive a response. After the retries, the element times out.
Description	A brief description of the profile.

Button	Description
New	Displays the New SNMP Access Profile page where you can add a new SNMP access profile.
Edit	Displays the Edit SNMP Access Profile page where you can change an SNMP access profile.
Delete	Displays the Snmp Access Profile/s Delete Confirmation page where you can confirm the deletion of the access profile.

SNMP Access Profile field descriptions

For SNMP protocol V3

The system displays the following fields when you click **V3** in the **Type** field:

Field	Description
Profile Name	The name of the profile.
Description	A brief description of the profile.
Type	The SNMP protocol type.
User	The user name as defined in the element.
Authentication Type	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The possible values are: - **MD5** The default is **MD5**.

Table continues…

Field	Description
	• **SHA** • **None** **Authorization Type** applies only to the SNMP V3 protocol.
Authentication Password	The password to authenticate the user. The password must contain at least eight characters. **Note:** The password is mandatory.
Confirm Authentication Password	The SNMP V3 protocol authentication password that you retype for confirmation.
Privacy Type	The encryption policy for an SNMP V3 user. The possible values are: • **DES**: For SNMP-based communication. The default is **DES**. • **AES**: For SNMP-based communication. • **None**: Does not encrypt traffic for this user. Set **Privacy Type** only for an SNMP V3 user.
Privacy Password	The password used to enable the **DES** or **AES** encryption. DES passwords must contain at least eight characters.
Confirm Privacy Password	The privacy password that you retype for confirmation.
Privileges	The privileges that determine the operations that you can perform on MIBs. • **Read/Write**: To perform GET and SET operations. • **Read**: To perform only the GET operation. • **None** The default is None.
Timeout	The time in milliseconds for which the element waits for a response from the device being polled during discovery.
Retries	The number of times that the element polls a device without receiving a response before timing out.

For SNMP protocol V1

The system displays the following fields when you click **V1** in the **Type** field:

Field	Description
Profile Name	The name of the profile.
Description	A brief description of the profile.
Type	The SNMP protocol type. **Note:** To upgrade Communication Manager using SNMP protocol, you must select SNMPV1.
Read Community	The read community of the device. **Read Community** applies only to the SNMP V1 protocol.
Write Community	The write community of the device. **Write Community** applies only to the SNMP V1 protocol.
Timeout	The time in milliseconds for which the element waits for a response from the device that the element polls.
Retries	The number of times that the element polls a device and fails to receive a response. After the retries, the element times out.

Button	Description
Commit	Adds or edits the SNMP access profile depending on the option you select.
Cancel	Returns to the previous page.

Configuring subnets

Adding a subnetwork

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Subnet Configuration**.
3. On the Subnet Configurations page, click **New**.

   The system adds a new row where you can add the details.
4. Type the name, IP address, and subnetwork mask.
5. Click **Save**.
6. To add more than one subnetworks, repeat Step 3.

Related links

Subnet Configurations field descriptions on page 844

Editing the subnetwork

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Subnet Configuration**.
3. On the Subnet Configurations page, select the subnetwork that you want to change.
4. Change the name, IP address, and subnetwork mask as appropriate.
5. Repeat Step 3 to change the information for more than one subnetworks.
6. Click **Save**.

Related links

Subnet Configurations field descriptions on page 844

Deleting a subnetwork

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Subnet Configuration**.
3. On the Subnet Configurations page, select the subnetworks that you want to delete.
4. Click **Delete**.
5. To confirm the deletion, click **Delete**.

   The system deletes the subnetwork.

Subnet Configurations field descriptions

Field	Description
Name	The name of the subnetwork.
IPaddress	The IP address of the subnetwork.
Mask	The IP subnetwork mask.

Button	Description
New	Adds a new row where you can provide the details of the subnetwork that you want to add.
Delete	Deletes a subnetwork.

Button	Description
Save	Adds or edits the subnetwork.
Cancel	Cancels your current action.

Managing Element Access Profile

Adding an element access profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Element Type Configuration**.
3. On the Element Access Profile Management page, in the **Element Type** field, click an element to which you want to provide access.

   For more information, see Element Access Profile Management field descriptions.
4. Click **New**.
5. On the Access Profile Entry page, in the **Protocol** field, click a protocol.
6. Click **Commit**.

Related links

Modify Access Profile Entry field descriptions on page 846
Element Access Profile Management field descriptions on page 846

Editing an element access profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Element Type Configuration**.
3. On the Element Access Profile Management page, in the **Element Access Profiles** section, select an element access profile that you want to edit.

   For more information, see Element Access Profile Management field descriptions.
4. Perform one of the following:
   - Click **Edit**.
   - Click **View**, and on the View Access Profile Entry page, click **Edit**.
5. On the Modify Access Profile Entry page, change the appropriate fields.
6. Click **Commit**.

Related links

Modify Access Profile Entry field descriptions on page 846
Element Access Profile Management field descriptions on page 846

Deleting an element access profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Element Type Configuration**.

3. On the Element Access Profile Management page, in the **Element Access Profiles** section, select an element access profile that you want to delete.

   For more information, see Element Access Profile Management field descriptions.
4. Click **Delete**.
5. On the Confirmation page, click **Continue**.

   The system deletes the element access profile from the **Element Access Profiles** section.

Element Access Profile Management field descriptions

Field	Description
Element Type	The type of the element for which you want to provide the access.
Name	The name of the element.
Protocol	The protocol that you use to access the element.
Login User Name	The login name of the user as configured on the element.
System Profile	The system protocol. The available options are: • true • false

Button	Description
New	Displays the Add Access Profile Entry page where you can add a new access profile for the element.
View	Displays the View Access Profile Entry page where you can view the access profile of an element.
Edit	Displays the Modify Access Profile Entry page where you can change an access profile of an element.
Delete	Deletes the access profile of an element that you select.

Modify Access Profile Entry field descriptions

Field	Description
Protocol	The protocol that you use to access the element. The field is read-only.
Name	The name of the element access profile.
Description	A description of the element access profile.
URI	The URI to reach the element access profile.

Button	Description
Commit	Commits the changes that you made to element access details.
Cancel	Cancels the modify action and returns to the Element Access Profile Management page.

Create profiles and discover SRS and SCS servers

Discover SRS and SCS servers

Use the **Create Profiles and Discover SRS/SCS** option to automatically discover survivable remote servers (SRS) and survivable core servers (SCS) from the main Communication Manager. System Manager uses the `list survivable-processor` command to discover the SRS and SCS servers that are associated with the main Communication Manager. The servers that are discovered are stored in **Manage Elements**.

Additionally, the SRS and SCS servers are automatically added in the System Manager inventory. The Communication Manager servers are automatically identified as survivable servers in **Inventory**.

Creating profiles and discovering SRS and SCS servers

Before you begin

Create the login profiles for Communication Manager devices with the **Element Type Configuration** option.

About this task

Use the **Create Profiles and Discover SRS/SCS servers** option to create login profiles for devices, and use the login profiles to discover the Communication Manager devices.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Create Profiles and Discover SRS/SCS**.
3. On the Create Profiles and Discover SRS/SCS page, in**Select Devices to Create Profiles** table, select the devices for which you want to discover and create the login profile.
4. In **Select Profiles to Create on Devices**, select the login profile.
5. Select the **Discover SRS/SCS and Create Profile on SRS/SCS** option.
6. Perform one of the following actions:
    - Click **Now** to create the login profile and discover the device.
    - Click **Schedule** to schedule the login profile creation and device discovery at a later time.

Related links

Create Profiles and Discover SRS/SCS server field descriptions on page 849

Overwriting login profiles on devices

Before you begin

You must create login profiles for Communication Manager devices with the **Element Type Configuration** option.

About this task

Perform this task to overwrite profiles that exist on the devices.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Create Profiles and Discover SRS/SCS**.
3. On the Collected Inventory page, in the **Select Devices to Create Profiles** table, perform the following actions.
    a. Select the devices for which you want to overwrite the login profile to discover the SRS and the SCS server.
    b. Select **Add to Manage Elements** for the devices that you have selected.
4. In the **Select Profiles to Create on Devices** table, perform the following actions:
    a. Select the new profile that you want to assign.
    b. Select the **Add to Manage Elements** for the profiles that you have selected.
5. Select the **Overwrite Profiles on Devices** option.
6. Perform one of the following actions:
    - Click **Now** to overwrite the profile that you selected on the devices.
    - Click **Schedule** to overwrite the profile at a later time.

Related links

Create Profiles and Discover SRS/SCS server field descriptions on page 849

Resetting the password

About this task

Perform this task to reset the password for a profile on the device.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Create Profiles and Discover SRS/SCS**.
3. On the Collected Inventory page, in the **Select Devices to Create Profiles** table, perform the following actions.
    a. Select the devices for which you want to overwrite the login profile to discover the SRS and the SCS server.
    b. Select **Add to Manage Elements** for the devices that you have selected.

4. Select the **Reset Password** option.
5. Perform one of the following actions:
    - Select **Use Profile Password** to reset the password.
    - Select **Auto Generate Password** to automatically generate a password.
6. Perform one of the following actions:
    - Click **Now** to reset the password.
    - Click **Schedule** to reset the password at a later time.

Related links

Create Profiles and Discover SRS/SCS server field descriptions on page 849

Create Profiles and Discover SRS/SCS server field descriptions

Select Devices to Create Profiles

Name	Description
Name	The name of the device.
IP	The IP address of the device.
Family	The device family to which the device belongs to.
Type	The device type.
Login Profile	The existing login profile for the device.
Software/Firmware Version	The firmware version for the device.
Hardware Version	The hardware version of the device.
Module	The device module.
Description	The description you choose to add for the device.
Location	The location of the device.
Serial Number	The serial number of the device.

Select Profiles to Create on Devices

Name	Description
Profile Type	The type of profile. Possible values include: SSH, SNMP, CM, GW.
Profile Name/IP	The name of the profile.
CM Profile Type/SNMP V3 Groups	The SNMP V3 profile type.
Add to Manage Elements	The option to add this profile in **Manage Elements**.

Name	Description
Discover SRS/SCS and Create Profile on SRS/SCS	Create the login profile and discovers the SRS or SCS server.

Table continues…

Name	Description
Overwrite Profiles on Devices	Overwrite the existing profile on the device.
Reset Password	Reset the password of the existing profile.

Button	Description
Now	Performs the discovery, overwrite profile, or reset password action.
Schedule	Performs the discovery, overwrite profile, or reset password action at a later time.

Working with Elements in System Manager

Additional information required for creating the Communication Manager or Messaging element

Communication Manager element

When you add the Communication Manager element from **Inventory** > **Manage Elements**, the element in turn starts a synchronization job in the background to bring all the relevant data from the elements to the System Manager database. To check the status of this synchronization job on System Manager Web Console, navigate to **System Manager Data** > **Scheduler** or reach the log files on the System Manager server.

Messaging element

If you are creating the Messaging element:

- The FQDN or IP address details in the **Node** field for a Messaging element must correspond to that of Messaging Storage Server (MSS) and not Messaging Application Server (MAS).
- Before adding the Messaging server in the System Manager applications, add the System Manager server details in the Trusted Server list on the Messaging server on the Messaging Administration/ Trusted Servers screen.
- The login credentials between the Messaging server trusted servers screen and the Session Manager application, entity, or attributes for a Messaging type of application must match.
- The **Trusted Server Name** field on the Trusted Server page maps to the **Login** field in the Attributes section. Similarly, the **Password** field on the Trusted Server page maps to the **Password** field in the Attributes section.
- To allow LDAP access to this Messaging server from the trusted server that you add, set the **LDAP Access Allowed** field on the Trusted Server page to `Yes`.

Manage elements in System Manager configured with Geographic Redundancy

The primary or the secondary System Manager server can manage a GR-aware element. However, only the primary System Manager server manages the GR-unaware element. You must know the elements that each System Manager manages during the scenario such as normal operation and split network.

Related links

Determining the System Manager that manages a GR-aware element on page 851

Determining the System Manager that manages a GR-aware element

Before you begin

Log on to the System Manager web console of the primary server.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Verify the status of the elements in the **Managed by** column:
   - For GR-unaware elements, the system must display Not Supported.
   - For GR-aware elements, the system must display one of the following status:
     - Primary: Indicates that the primary System Manager manages the element.
     - Secondary: Indicates that the secondary System Manager manages the element.
     - Unknown: Indicates that the manageability status of the element is unavailable.
     - Unmanaged: Indicates that the current System Manager does not manage the element.
       - To refresh the **Managed by** status for an element, click **Get Current Status**.
       - To make the System Manager manage an element, the administrator must click **More Actions** > **Manage**.

   For example, for managing Session Manager in a Geographic Redundancy setup, see *Administering Avaya Aura® Session Manager*.

Viewing details of an element

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element.
4. Click **View**.

   The system displays the details of the selected element.

Modifying an element

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element.
4. Perform one of the following:
   - Click **Edit**.
   - Click **View** > **Edit**.

   Note:

   If the Communication Manager system that you require to edit contains a **:** (colon) character in the name, the system disables the **Edit** button. Remove the **:** character from the Communication Manager name to enable **Edit**.
5. On the Edit <element name> page, modify the required fields.
6. Click **Commit**.

   The system saves the changes.

Deleting an element

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element.
4. Click **Delete**.

5. On the Delete Application Confirmation page, click **Delete**.

Exporting elements from the System Manager command line interface

Before you begin

- Ensure that System Manager is installed and the server is running.

  The bulk export utility requires System Manager to include runtime libraries.

- Ensure that JBoss is installed on the same server where you run the export utility.

About this task

Use the bulk export utility to export system records of an element to an xml file. The System Manager installer creates the `bulkExport` folder in the `<MGMT_HOME>\rts\` location.

Procedure

1. Start an SSH session.
2. Log in to the System Manager server by using the command line interface.
3. At the prompt, to navigate to the `bulkExport` directory, type `cd <MGMT_HOME>\rts\bulkExport`.
4. Run the following command:

   ```
   sh ./runRTSCli.sh [-u username] [-w password][-p filePrefix] [-c perFileRecords] [-ddestinationFolder] [-n application-type-name] [-v application-type-version]
   ```

   The element generates a zip file with filePrefix as prefix and contains the xml data file in the destination folder. The system generates log files in the `/var/log/Avaya/mgmt/logs/rtsutility.log` location.

   For example, **`sh ./runRTSCli.sh`** -c *100* -d *./* -p *rts* -u *admin* -w *Admin123$*.

5. **(Optional)** Change the log configuration in the `<MGMT_HOME>\rts\bulkExport\conf\log4.properties` file.

Related links

runRTSCli.sh command on page 853

runRTSCli.sh command

The **`runRTSCli.sh`** utility exports element system records to an xml file.

Syntax

```
sh ./runRTSCli.sh [-u username] [-w password][-p filePrefix] [-c perFileRecords] [-ddestinationFolder] [-n application-type-name] [-v application-type-version]
```

-c,--numberOfRecordsPerFile *numberOfRecordsPerFile*	The number of records in a file.
-d,--output-directory *destinationFolder*	The name of the output folder.
-f,--config-file *configurationFile*	The configuration file if you do not use the default configuration file.
-h,--help	The option to print help options.
-n,--application-type-name *applicationTypeName*	The element type name. The parameter is optional.
-p,--filename-prefix *filePrefix*	The prefix for the zip file.
-s,--ssl	Secure. The parameter is optional.
-u,--username *System ManagerUsername*	System Manager username.
-v,--application-type-version *applicationTypeVersion*	Element type version. The parameter is optional.
-w,--password *System ManagerPassword*	System Manager password.

Return values

A zip file that contains an xml file with element system data.

Description

The export utility generates a zip file with the specified prefix. The file contains the xml data file in the destination folder.

Example

The example command creates the element data in the `rtsFileName` zip file with 100 records in the root folder `./`.

```
cd Mgmt_Home\rts\bulkExport
sh ./runRTSCli.sh -c 100 -d ./ -p rts -u admin -w Admin123$
```

Files

The following files are associated with the **`runRTSCli.sh`** command:

- `<MGMT_HOME>\rts\bulkExport`: Location where you run the command.
- `/var/log/Avaya/mgmt/logs/rtsutility.log`: Location where the system generates the log files.
- `<MGMT_HOME>\rts\bulkExport\conf\log4.properties`: The properties file where you can change the log configuration.

Assigning elements to an element

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, perform one of the following steps:
    - Select an element and click **Edit**.
    - To assign elements to an existing element in the view mode, select an element and click **View** > **Edit**.
4. In the Assign elements area, click **Assign elements**.
5. On the Assign elements page, select elements and click **Assign**.

    Note:

    Assignment name for Communication Manager must match the switch connection on the Edit Application Enablement Services:<name> page. If the assignment name is blank, the system does not establish the SSL connection between Presence and AES.

Removing assigned elements

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, perform one of the following steps to remove assigned elements from an existing element:
    - Select an element and click **Edit**.
    - Select an element and click **View** > **Edit**.
4. Select the elements that you must remove and click **Unassign Elements** in the Assign Elements section.

Managing access profiles and ports

Creating an access profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.

3. On the Manage Elements page, perform one of the following steps:
    - Click **New**.
    - To create an access profile for an existing element, click the element and then click **Edit** or **View** > **Edit**.
4. On the **General** tab, in the **Access Profile** section, click **New**.

    The system displays the **Application System Supported Protocol** section.
5. In the **Protocol** field, select the protocol.

    The system displays the **Access Profile Details** section.
6. Enter the information about the access profile in the mandatory fields.
7. Click **Save**.

Modifying an access profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **Edit** or **View** > **Edit**.
4. In the **Access Profile** section, select the access profile that you want to change and click **Edit**.
5. Modify the access profile information in the fields.
6. Click **Save**.

Deleting an access profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **Edit** or click **View** > **Edit**.
4. In the **Access Profile** section, select the access profile that you want to delete and click **Delete**.

    Note:

    You cannot delete the Trust Management access profile.

Creating a new port

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.

3. On the Manage Elements 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** or click **View** > **Edit**.
4. Click **New** in the Port section.
5. Enter the information about the port in the following mandatory fields: **Name**, **Protocol**, and **Port**.
6. Click **Save**.

Result

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

Modifying a port

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. To configure a port for an existing element, perform one of the following steps on the Manage Elements page:
    - Select an element and click **Edit**.
    - Select an element and click **View** > **Edit**.
4. Click **Edit** in the **Port** section.
5. Modify the port information in the following fields: **Name**, **Port**, **Protocol**, and **Description**.
6. Click **Save** to save the changes to the database.

Deleting a port

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select the application instance and click **Edit** or click **View** > **Edit**.
4. In the Port section, select the port you want to delete and click **Delete**.

    The system deletes the port you selected from the table in the Port section.

Managing and unmanaging elements from System Manager

Manage elements

In a Geographic Redundancy-enabled system, the administrator can select elements and click **Manage** for the current System Manager to manage the elements. The system sends a notification to the element whose manageability status you must change. On receiving the notification, the element switches to the specific System Manager server from where you performed the Manage operation.

Note:

Session Manager from Release 6.3 and Communication Manager support the Manage operation.

During the split network, the administrator must ensure that the primary or the secondary System Manager server manages an element at a time, and not both systems.

Note:

At any given point of time, you can perform **Get Current Status**, **Manage**, or **Unmanage** operation.

Related links

Manage Elements field descriptions on page 862

Unmanage elements

In a Geographic Redundancy-enabled system, the administrator can select to unmanage an element. The system sends a notification to the element whose manageability status you must change. On receiving the notification, the element unmanages from the current System Manager.

Communication Manager supports the Unmanage operation.

In a specific split network scenario, the primary System Manager server fails to communicate with the secondary System Manager server, but the element can communicate with both System Manager systems. If the primary System Manager server manages the element and the administrator wants to manage the element from the secondary System Manager server, on the primary System Manager server, the administrator must set the manageability status to Unmanaged.

Note:

At any given point of time, you can perform **Get Current Status**, **Manage**, or **Unmanage** operation.

Related links

Manage Elements field descriptions on page 862

Adding Platform type elements to System Manager

Adding System Platform to System Manager

About this task

Use the procedure to manually add System Platform to System Manager. You can also use the System Manager discovery operation to discover System Platform in the network.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On the New Elements page, in the **Type** field, click **System Platform**.

   The page displays the On the New System Platform page.
5. On the General tab, provide the following information:
   - **Name**: The console domain (C-Dom) name.
   - **Type**: System Platform. A read-only field. The application type that the system populates from the **Type** field on the New Elements page.
   - **Description**: A description of the C-Dom.
   - **Node**: The IP address of C-Dom.
   - **Device Type**: System Platform.
6. On the Attributes tab, provide the following information:
   - **Login**: The use name with administrator permissions.
   - **Password**. The password.
   - **Confirm Password**: The password that you reenter.
   - **Dom0 IP Address**: The Dom-0 IP address.
   - **Cdom Root Password**: The C-Dom root password. A mandatory field.
   - **Confirm Cdom Root Password**. The C-Dom root password that you reenter. A mandatory field.

     Note:

     If you do not complete the **Cdom Root Password** and **Confirm Cdom Root Password** fields, the upgrade operation fails.
7. In the Access Profile section, click **New** and provide the access profile details.

> **Note:**
>
> The root access password must be identical in System Manager and System Platform.

8. Click **Commit**.

   On the Manage Elements page, the system displays the System Platform instance that you added.

Adding Application type elements to System Manager

Adding a Communication Manager instance to System Manager

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On the New Elements page, in the **Type** field, click **Communication Manager**.

   The system displays the Add Communication Manager page.
5. On the General Attributes tab, provide the following information:
   - **Name**: The Communication Manager server name.

     For Branch Session Manager upgrades, provide the survivable remote server name.
   - **Hostname or IP address**: The hostname of the Communication Manager server.

     For duplex Communication Manager upgrades, you must provide the IP address for the active Communication Manager server.
   - **Login**. The customer login name that is required to access Communication Manager.

     For Branch Session Manager upgrades, provide the customer login name required to access the survivable remote server.
   - **Authentication Type**. The **Password** option.
   - **Password**. The password that is required to access Communication Manager.
   - **Confirm Password**: The password that you reenter.
   - **Device Type**: The type of Communication Manager. The options are:
     - **Avaya Aura(R) Communication Manager SP** for Communication Manager 6.3.100 on System Platform.
     - **Avaya Aura(R) Communication Manager VE** for Virtualized Environment-based Communication Manager 6.3.100 and Release 7.0.

- **Add to Communication Manager** check box: The option to view this Communication Manager system in the list.

6. On the SNMP Attributes tab, provide the following information:

    a. **Version**: V1.

    The page displays the remaining fields.

    b. Fill the required fields.

7. Click **Commit**.

    The system displays the Communication Manager instance that you added on the Manage Elements page.

Related links

Add Communication Manager field descriptions on page 876

Adding a Session Manager instance to System Manager

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Click **New**.
4. On the New Elements page, in the **Type** field, click **Session Manager**.
5. When the screen refreshes, select **Core Session Manager**.
6. Click **Continue**.
7. In the General section, enter the following information:

    a. In the **SIP Entity Name** field, enter the name of Session Manager.

    b. In the **Description** field, add a description for this entity. This field is optional.

    c. In the **Management Access Point Host Name/IP** field, enter the IP address of the management interface of the Session Manager server.

    d. **Maintenance Mode** is enabled by default. Clear the **Maintenance Mode** check box if you are not:

    - Staging a non-operational Session Manager or Branch Session Manager.
    - Pre-administering a Session Manager or Branch Session Manager on System Manager prior to host installation.

8. Enter or select the appropriate information in the remaining required fields.
9. Click **Commit**.

Adding a G430 or G450 gateway to System Manager

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On the New Elements page, in the **Type** field, click **Communication Manager and G860 Gateways**.
5. On the New Communication Manager and G860 Media Gateways page, do the following:
    a. In the **Device Type** field, click **Avaya G430** or **Avaya G450**.
    b. In **Access Profile**, configure the parameters.
    c. In **Port**, configure the parameters.
6. On General and Attributes tabs, provide the required details.

    ✱ **Note:**

    The following parameters must be identical in System Manager and G430 Branch Gateway or G450 Branch Gateway:

    - The root access password
    - The SNMPv1 credentials
7. Click **Commit**.

    On the Manage Elements page, the system displays the gateway that you added.

Field descriptions

Manage Elements field descriptions

Field	Description
Name	The name of the element.
Node	The node on which the element runs.
Type	The type of the element to which the element belongs.

Table continues…

Field	Description
	Note: You can view this field only if you gain access to the Manage Elements page from **Inventory**.
Device Type	The device type of the element. For example, for IP Office, the device type can be IP Office or B5800.

The system also provides the following fields on System Manager that is configured with Geographic Redundancy.

Reachable	The state that mentions whether the element is reachable from the current server. The values are Yes and No.
Managed by	The field that specifies the server that manages this element. The options are Primary and Secondary. For a non-GR element, the field displays Not Supported.
Last Updated Time	The time when the system updates the status of the element
Error	A red cross icon (❌) if the system generates errors. For more information, click the icon.
Warning	An yellow triangle icon (⚠) if the system generates warnings. For more information, click the icon.

Note:

At any given point of time, you can perform **Get Current Status**, **Manage**, or **Unmanage** operation.

Button	Description
View	The View <Element-name> page. Use this page to view the details of the selected element.
Edit	The Edit <Element-name> page. Use this page to modify the information of the instance.
New	The New Elements page. Use this page to create a new element.
Delete	The Delete <Element-name> page. Use this page to delete a selected element.
Get Current Status	The real-time connectivity status and the manageability status of elements on the active server. When the request is in progress for at least one element, the system displays the progress bar and

Table continues…

Button	Description
	the selected elements. When the request is complete, the system updates the time stamp and the status. **Note:** • On the secondary System Manager server in the standby mode, the system displays only the connectivity status of elements and not the manageability status. • On a standalone server, the system disables **Get Current Status**.
More Actions > **Configure Trusted Certificates**	The Trusted Certificates page. Use this page to view, add, export, and delete the trusted certificates for the element.
More Actions > **Configure Identity Certificates**	The Identity Certificates page. Use this page to view, export, renew, and replace the identity certificates for the element.
More Actions > **Manage**	System Manager starts managing the element that you select.
More Actions > **Unmanage**	System Manager stops managing the element that you select.
More Actions > **Import**	The Import Applications page. Use this page to import application data in bulk from a valid XML file.
More Actions > **View Notification Status**	The status of notifications. The valid status values are Failed and Inprogress. The system displays the progress bar if a notification is pending. The system displays the **Resend Notification** button only when there are no notifications in progress and when you select the rows of the same event type. If you click **Resend Notification**, the system displays a progress bar until the resend operation is complete or fails. If the notification status is Inprogress, use **Get Current Status** to find the connectivity status and the manageability status of elements. However, you cannot use **Manage** or **Unmanage** to start or stop managing the elements. **Note:** **View Notification Status** is available only on the primary or the secondary System Manager server that is in the active state.

Table continues…

Button	Description
Filter: Enable	The fields where you can set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Disable	Hides the column filter fields. **Filter: Disable** is a toggle button.
Filter: Apply	Filters elements based on the filter criteria.
Select: All	All elements in the table.
Select: None	Clears the selection for the users that you select.
Refresh	Refreshes the element information in the table.

Element details field descriptions

The fields on this page varies with the element that you manage.

General

Field	Description
Name	The name of the element.
Type	The type of the application to which the element belongs.
Description	A brief description of the element.
Node	The node on which you run the element. ✱ **Note:** The system displays the **Node** field when you select **Other** from the **Node** field.
Device Type	The device type of the element. For example, for IP Office, the device type can be IP Office or B5800.

Access Profile

Field	Description
Name	The name of the access profile.
Access Profile Type	The type of the access profile. The options are: • **URI**: For system web services API. • **SSH**: For application upgrade functions. • **SNMP**: For discovering elements.

Table continues…

Field	Description
Access Profile Sub Type	The sub type of the URI access profile. The options are: • **EMURL**: To create a URL type access profile. • **WS**: To create a web service access profile. • **GUI**: To create a GUI access profile. • **GRCommunication**: To create a GR-aware element. • **TenantURL**: To create the tenant-related access profile. • **Other**
Protocol	The protocol that the element supports to communicate with other communication devices.
Host	The name of the host on which the element is running.
Port	The port on which the element is running.
Order	The order in which you gain access to access profiles.

Button	Description
View	Displays fields in the Access Profile section that you can use to view access profile details.
New	Displays fields in the Access Profile section that you can use to add access profile details.
Edit	Displays fields in the Access Profile section using which you can modify the access profile details that you select.
Delete	Deletes the selected access profile.

Application System Supported Protocol

The system displays the following fields when you click **New** or **Edit** in the **Access Profile** section:

Field	Description
Protocol	The protocol used to access profiles. The options are: • **URI**: For system web services API. • **SSH**: For application upgrade functions. • **SNMP**: For discovering elements. ✱ **Note:** The page displays the button only when you click **Add** or **Edit** in the Access Profile section.

Access Profile Details

The page displays the following fields when you click **URI** in the **Protocol** field:

Field	Description
Name	The name of the access profile.
Access Profile Type	The type of the access profile. The options are: • **EMURL**: To create a URL type access profile. • **WS**: To create a web service access profile. • **GUI**: To create a GUI access profile. • **GRCommunication**: To create a GR-aware element. • **TenantURL**: To create the tenant-related access profile. • **Other**
Protocol	The protocol for communicating the element.
Host	The name of the host on which the element is running.
Port	The port on which the element is running.
Path	The path to gain access to the access profile.
Order	The order in which you gain access to access profiles.
Description	A brief description of the access profile.

The page displays the following fields when you click **SSH** in the **Protocol** field:

Field	Description
Name	The name of the access profile.
Login Name	The login name as configured on the element.
Port	The port on which the element is running.
Use ASG Key	The option to use the ASG encryption.
Password	The password to log in to the element.
Confirm Password	The password that you retype.

The page displays the fields when you click **SNMP** in the **Protocol** field and **V3** in the **Type** field:

Field	Description
Profile Name	The name of the profile.
Description	A brief description of the profile.
Type	The SNMP protocol type.
User	The user name as defined in the element.

Table continues…

Field	Description
Authentication Type	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The possible values are: • **MD5** The default is **MD5**. • **SHA** • **None** **Authorization Type** applies only to the SNMP V3 protocol.
Authentication Password	The password to authenticate the user. The password must contain at least eight characters. **Note:** The password is mandatory.
Confirm Authentication Password	The SNMP V3 protocol authentication password that you retype for confirmation.
Privacy Type	The encryption policy for an SNMP V3 user. The possible values are: • **DES**: For SNMP-based communication. The default is **DES**. • **AES**: For SNMP-based communication. • **None**: Does not encrypt traffic for this user. Set **Privacy Type** only for an SNMP V3 user.
Privacy Password	The password used to enable the **DES** or **AES** encryption. DES passwords must contain at least eight characters.
Confirm Privacy Password	The privacy password that you retype for confirmation.
Privileges	The privileges that determine the operations that you can perform on MIBs. • **Read/Write**: To perform GET and SET operations. • **Read**: To perform only the GET operation. • **None** The default is None.
Timeout	The time in milliseconds for which the element waits for a response from the device being polled during discovery.

Table continues…

Field	Description
Retries	The number of times that the element polls a device without receiving a response before timing out.

The page displays the fields when you click **SNMP** in the **Protocol** field and **V1** in the **Type** field:

Field	Description
Profile Name	The name of the profile.
Description	A brief description of the profile.
Type	The SNMP protocol type. ✱ **Note:** To upgrade Communication Manager using SNMP protocol, you must select SNMPV1.
Read Community	The read community of the device. **Read Community** applies only to the SNMP V1 protocol.
Write Community	The write community of the device. **Write Community** applies only to the SNMP V1 protocol.
Timeout	The time in milliseconds for which the element waits for a response from the device that the element polls.
Retries	The number of times that the element polls a device and fails to receive a response. After the retries, the element times out.

Button	Description
Save	Saves the access profile details. ✱ **Note:** This button is visible only when you click **Add** and **Edit** in the **Access Profile** section.
Cancel	Cancels the operation of creating or editing an access profile and hides the fields where you enter or modify the access profile information. ✱ **Note:** This button is available only when you click **Add** and **Edit** in the **Access Profile** section.

Port

Field	Description
Name	The name of the port.
Port	The port on which the element is running.
Protocol	The protocol for the corresponding port.
Description	A brief description about the port.

Button	Description
New	Displays fields in the Port section that you can use to add a port.
Edit	Displays fields in the Port section with port information. You can change the port details in the port mode.
Delete	Deletes the selected configured port.
Commit	Saves the port details. **Note:** The section displays the **Save** button only when you click **Add** or **Edit** in the **Port** section.
Cancel	Cancels the current operation of creating or editing an access profile and hides the fields where you add or modify the port information. **Note:** The section displays the **Cancel** button only when you click **Add** or **Edit** in the **Port** section.

Attributes

Use this section to configure attributes for the selected element.

The following fields display the information about attributes defined for System Manager.

Field	Description
IP	The IP address of System Manager.
FQDN	FQDN of System Manager.
Virtual IP	The virtual IP address of System Manager.
Virtual FQDN	The virtual FQDN of System Manager.
isPrimary	The option to indicate if the element is primary or secondary.

Assign elements

Name	Description
Name	The name of the element.
Type	The type of the application to which the element belongs.
Description	A brief description about the element.

Button	Description
Assign elements	Displays the Assign elements page that you use to assign an element to another element.
Unassign elements	Removes an assigned element.

Button	Description
Commit	Creates or modifies an element by saving the information to the database. **Note:** The system displays the button only when you click **Add** or **Edit** on the Manage Elements page.
Cancel	Closes the page without saving the information and navigates back to the Manage Elements page.

For example, the following fields provide information about attributes that you can define for Messaging.

Field	Description
Login	The name in the **Trusted Server Name** field of the Trusted Servers page on the Messaging server.
Password	The password as given in the **Password** field of the Trusted Servers page on the Messaging server.
Confirm Password	The password that you retype for confirmation.
Messaging Type	The type of the Messaging server. The following types are supported: • **MM**: Modular Messaging • **CMM**: Communication Manager Messaging • **AURAMESSAGING**: Avaya Aura® Messaging
Version	The version of Messaging. Supported versions are 5.0 and later.
Secured LDAP Connection	An option to use the secure LDAP connection.

Table continues…

Field	Description
	To use the nonsecure LDAP connection, you must clear the check box.
Port	The port on which the LDAP or secure LDAP service that the element provides is running. The default port is 389 for LDAP and 636 for secure LDAP.
Location	The location of the element.

Delete Element Confirmation field descriptions

Use this page to delete an element.

Name	Description
Name	The name of the element.
Node	The node on which the element is running.
Registration	The registration status of the element. The options are: • **True**: Indicates a registered instance. • **False**: Indicates an unregistered instance.
Description	A brief description about the element.

Button	Description
Delete	Deletes the selected element.
Cancel	Closes the Delete Element Confirmation page.

Import Elements field descriptions

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

File Selection

Name	Description
Select File	The path and name of the XML file from which you must import the element data.

Button	Description
Browse	Displays the File Upload box where you can browse for the file that you must import the element data.

Configuration

Name	Description
Select Error Configuration	The options are: • **Abort on First Error**: The system stops the import of element data when the import element operation encounters the first error in the import file that contains the element data. • **Continue Processing other records**: The system imports the data of next element if the data of current element failed to import.
If a matching record already exists	The options are: • **Skip**: Skips a matching record that already exists in the system during an import operation. • **Replace**: Reimports or replaces all the data for an element. This is essentially the ability to replace an element along with the other data related to the element. • **Merge**: Imports the element data at an even greater degree of granularity. Using this option you can simultaneously perform both the add and update operation of elements data. • **Delete**: Deletes the elements along with their data from the database that match the records in the input XML file.

Schedule

Name	Description
Schedule Job	The options for configuring the schedule of the job: • **Run immediately**: Use this option if you want to run the import job immediately. • **Schedule later**: Use this option to run the job at the specified date and time.
Date	The date when you require to run the import elements job. The date format is mm: dd:yyyy. You can use the calendar icon to select a date. This field is available when you select the **Schedule later** option for scheduling a job.
Time	Time of running the import elements job. The time format is hh:mm:ss and 12 (AM or PM) or 24 hour format.

Table continues…

Name	Description
	This field is available when you select the **Schedule later** option for scheduling a job.
Time Zone	Time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Button	Description
Import	Imports or schedules the import operation based on the option you selected.

Import List

Name	Description
Select check box	Provides the option to select a job.
Start Time	The time and date of scheduling the job
Status	The current status of the job. The following are the different status of the job: 1. PENDING EXECUTION: The job is in queue. 2. RUNNING: The job execution is in progress. 3. SUCCESSFUL: The job execution is complete. 4. INTERRUPTED: The job execution is cancelled. 5. PARTIAL FAILURE: The job execution has partially failed. 6. FAILED: The job execution has failed.
Scheduled Job	Displays a link to the Scheduler user interface. You can cancel the job from the Scheduler user interface too.
% Complete	The job completion status in percentage.
Element Records	The number of user records in the input file.
Failed Records	The number of user records in the input file that failed to import.

Button	Description
View Job	Shows the details of the selected job.
Cancel Job	Cancels the import operation for the selected job. You can cancel a job that is in progress or queued for import.
Delete Job	Deletes the selected job.
Refresh	Refreshes the job information in the table.

Table continues…

Button	Description
Show	Provides an option to view all jobs on the same page. If the table displaying scheduled jobs span multiple pages, to view all jobs on a single page, select **All**.
Select: All	Selects all jobs in the table.
Select: None	Clears the check box selections.
Cancel	Returns to the **Manage Elements** page.

Import Status field descriptions

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

Status Summary

Name	Description
Start	The start date and time of the job.
End	The end date and time of the job.
File	The name of the file that is used to import the element records.
Total Records	The total number of element records in the input file.
Successful Records	The total number of element records that are successfully imported.
Failed Records	The total number of element records that failed to import.
Complete	The percentage completion of the import.

Status Details

Name	Description
Line Number	The line number in the file where the error occurred.
loginName	The login name through which job was executed.
Error Message	A brief description about the error message.

Button	Description
Done	Takes you back to the Import Elements page.

Add Communication Manager field descriptions

General Attributes

Field	Description
Name	The name of Communication Manager instance.
Hostname or IP Address	The host name or the IP address of the Communication Manager instance. For the duplicated Communication Manager, this value references the active server IP address.
Login	The login name that you use to connect to the Communication Manager instance. **Note:** craft, craft2, dadmin, inads, init, rasaccess, sroot, and tsc are the restricted logins when you configure a Communication Manager system. Do not use the login name to connect to: • The Communication Manager instance from any other application. • The Communication Manager SAT terminal by using command line interface (CLI).
Authentication Type	The authentication type. The following are the types of authentication: • **Password**: The password that authenticates the SSH or Telnet login name on the element. • **ASG Key**: The ASG key used to authenticate the ASG login.
Password	The password that authenticates the SSH or Telnet login name on the element.
Confirm Password	The password that you retype for confirmation. **Confirm Password** must match **Password**.
ASG Key	The ASG key used to authenticate the ASG login.
Confirm ASG Key	The ASG key that you retype for confirmation. **Confirm ASG Key** must match **ASG Key**.
SSH Connection	An option to use SSH for connecting to the element. By default, the system selects the check box. If you clear the check box, the system uses Telnet to connect to the element.

Table continues…

Field	Description
RSA SSH Fingerprint (Primary IP)	The RSA SSH key of the Communication Manager server. For duplex servers, the RSA SSH key is the key of the active server.
RSA SSH Fingerprint (Alternate IP)	The DSA SSH key of the standby Communication Manager server. Use the DSA SSH key only for duplex servers.
Description	A description of the Communication Manager server.
Alternate IP Address	The alternate IP address of the element. For duplex servers, the alternate IP address is the IP address of the standby server.
Enable Notifications	A real-time notification whenever an administrative change occurs in Communication Manager. For example, when you add or delete an extension from Communication Manager outside System Manager. The options are: • Selected: Enables the CM Notify sync feature for this Communication Manager instance. • Cleared: Disables the CM Notify sync feature for this Communication Manager instance. After you enable this feature, and register the System Manager IP address on Communication Manager, the system sends changes that are administered on Communication Manager to System Manager asynchronously. **Note:** Communication Manager 6.2 or later supports this feature.
Port	The port on which the service provided by the element is running. The default SSH port is 5022 if you select the **SSH Connection** check box. The default SSH port is 5023 if you do not select the **SSH Connection** check box.
Location	The location of the element.
Add to Communication Manager	An option to select the Communication Manager that you want to view in the communication manager list.

SNMPv1 Attributes

Field	Description
Version	The SNMP protocol type.
Read Community	The read community of the device.

Table continues…

Field	Description
Write Community	The write community of the device.
Retries	The number of times an application polls a device without receiving a response before timing out.
Timeout (ms)	The number of milliseconds an application polls a device without receiving a response before timing out.
Device Type	The Communication Manager application type. The options are: • **Avaya Aura(R) Communication Manager SP** for Communication Manager 6.3.100 on System Platform. • **Avaya Aura(R) Communication Manager VE** for Virtualized Environment-based Communication Manager 6.3.100 and Release 7.0.

SNMPv3 Attributes

Field	Description
Version	The SNMP protocol type.
User Name	The user name as defined in the application.
Authentication Protocol	The authentication protocol that authenticates the source of traffic from SNMP V3 protocol users. The possible values are: • **MD5 (default)** • **SHA** • **None**
Authentication Password	The SNMP authentication password.
Confirm Authentication Password	The SNMP authentication password that you retype for confirmation. **Authentication Password** and **Confirm Authentication Password** must match.
Privacy Protocol	The encryption policy for SNMP V3 users. The possible values are: • **AES**: Use the AES encryption for the SNMP-based communication. AES is the default protocol. • **DES**: Use the DES encryption for the SNMP-based communication. • **None**: Do not encrypt traffic for this user.
Privacy Password	The pass phrase used to encrypt the SNMP data.
Confirm Privacy Password	Retype the privacy password in this field for confirmation.

Table continues…

Field	Description
Retries	The number of times the application polls a device without receiving a response before timing out.
Timeout (ms)	The number of milliseconds the application waits for the response from the device being polled.
Device Type	The type of device.

Button	Description
Commit	Adds a Communication Manager instance in the inventory.
Clear	Clears all the entries.
Cancel	Cancels your action and return to the previous page.

Add IP Office field descriptions

General

Name	Description
Name	The name of the IP Office device. The name must only contain lowercase and uppercase alphabets, numbers from 0 to 9, commas, hyphens, and underscores.
Description	The description of the IP Office device.
Node	The host name or the IP address of the IP Office device.
Device Type	The type of the IP Office device. The options are IP Office and B5800.
Device Version	The version of the IP Office device.
Service Login	The login name to access the IP Office device. The default is BranchAdmin.
Service Password	The password to access the IP Office device.
Confirm Service Password	The service password that you retype for confirmation.

For IP Office releases earlier than 9.1, the default service login for IP Office is SMGRB5800Admin. After you upgrade IP Office from Release 9.0 to 9.1 or later, you can use the same login name, SMGRB5800Admin. The account remains active.

However, the system creates a new account, BranchAdmin. The configuration of the BranchAdmin account is the same as the SMGRB5800Admin account. The new account also becomes active.

In IP Office Release 9.1 or later, if you reset the security setting, the system deletes the SMGRB5800Admin account and adds the BranchAdmin account that remains disabled. You must activate the account by accessing the IP Office security setting offline.

Also, if you add the new IP Office Release 9.1 or later in System Manager by running Initial Configuration Utility (ICU) on IP Office, the default account, BranchAdmin, will be available. The account becomes active.

SNMP

Name	Description
Version	The SNMP protocol type. The options are None and V1.
Read Community	The read community of the device.
Write Community	The write community of the device.
Retries	The number of times that an application polls a device without receiving a response before timing out.
Timeout (ms)	The number of milliseconds that an application polls a device without receiving a response before timing out.

Button	Description
Commit	Adds the IP Office device to the inventory.
Clear	Clears your entries and reset the page.
Cancel	Cancels the add operation, and returns to the previous page.

Delete IP Office field descriptions

Name	Description
Name	The name of the IP Office instance you have chosen to delete.
Node	The node on which the IP Office instance you have chosen to delete is running.
Type	The type of the application instance you want to delete. In this case, **Type** is IP Office.
Version	The software version of the IP Office device you have chosen to delete.
Description	The description of the IP Office device you have chosen to delete.

Button	Description
Delete	Click to delete the IP Office device you have selected.
Cancel	Click to cancel the delete operation and go to the previous page.

Other Managed Elements capabilities available in System Manager

Managing Serviceability Agents

Serviceability Agents

The Serviceability Agent is an enhanced version of the SAL agent for forwarding logs, harvesting logs, and for alarming. The Serviceability Agent sends SNMPv2 and SNMPv3 traps and notifies the configured NMS destinations where System Manager and the SAL gateway are the two mandatory destinations.

With the Serviceability Agent user interface you can:

- Manage and configure SNMPv3 users remotely
- Manage and configure SNMP trap destinations remotely
- Create, edit, view, and delete user and target profiles. You can also attach these profiles to agents or detach these profiles from agents.

For more information on fault management using SNMP, see *Avaya Aura® System Manager Fault Management and monitoring using SNMP*.

Converting a common alarm definition file to MIB file and trapd file

Before you begin

To run the command, you require jre 1.6.0 or later installed on the system.

About this task

The MIB tool converts a Common Alarm Definition File (CADF) xml file to MIB file (`.my`) and trapd (`.conf`) file. The tool converts only CADF files with notification OIDS that are specified in the X.X.X.productID.0.n format, where n is the notification OID.

You must provide all parameters. To provide the parameters later, you must edit the generated MIB file and trapd file. The system saves the generated artifacts in the same folder as that of the CADF file. Ensure that you have required disk space and file permissions.

Procedure

1. At the prompt, type `cd $SPIRIT_HOME/scripts/utils`.
2. Type the following command:

```
generateTrapdAndMibUnix.sh [-l absolute path to cadf file] [-m
 MIB name] [-i MIB item name] [-p product ID] [-n product name][-a author]
```

Note:

- If the path to the CADF file is incorrect, the system displays JVM errors.

- If the input to the **generateTrapdAndMibUnix.sh** command is invalid, the system displays `No data or wrong data in .my and .conf files.`

Example

```
generateTrapdAndMibUnix.sh [-l /op/Avaya/SMGR_CommonAlarmDefn_Data.xml] [-m
AV-AURA-SYSTEM-MANAGER-MIB] [-i avAuraSysMgr] [-p 25] [-n Avaya Aura System Manager][-a
Avaya]
```

Related links

generateTrapdAndMibUnix on page 882

Configuration files in the MIBTOOL.jar file on page 882

Configuration files in the MIBTOOL.jar file

The `MIBTOOL.jar` file contains the following property files in the `spirit/mibtool/staticfiles` location:

File name	Description
`MIB.properties`	The file contains default values for MIB name, MIB item name, and product ID. You can change the values.
`MIBXMLTAGS.properties`	The file contains tags in CADF file that contains the information for items such as alarm name and OID. If you change the CADF file format, you must configure the tag names accordingly in the property file. Separate the values by a comma.

Note:

Do not edit the property files. If you must edit, use a program such as WinZip and open the `MIBTOOL.jar` file. Do not extract the files. To view the files, navigate to the `com/avaya/resource` directory. Open the file by with a text editor, make the changes, and save the file. When WinZip prompts, click **Choose update the zip archive with the changes**.

generateTrapdAndMibUnix

The **generateTrapdAndMibUnix** converts the Common Alarm Definition File (CADF) xml file to MIB file (`.my`) and trapd (`.conf`) file. The tool converts only CADF files with notification OIDS that are specified in the X.X.X.productID.0.n format, where n is the notification OID.

Syntax

```
generateTrapdAndMibUnix.sh [-l absolute path to cadf file] [-m
 MIB name] [-i MIB item name] [-p product ID] [-n product name][-a author]
```

Example

```
generateTrapdAndMibUnix.sh [-l /op/Avaya/SMGR_CommonAlarmDefn_Data.xml] [-m
AV-AURA-SYSTEM-MANAGER-MIB] [-i avAuraSysMgr] [-p 25] [-n Avaya Aura System Manager][-a
Avaya]
```

Considerations

You must provide all parameters. To provide the parameters later, you must edit the generated MIB file and trapd file. The system saves the generated artifacts in the same folder as that of the CADF file. Ensure that you have required disk space and file permissions.

Managing SNMPv3 user profiles

Creating an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Click **New**.
4. On the New User Profile page, complete the User Details section.
5. Click **Commit**.

Related links

SNMPv3 user profiles field descriptions on page 884

Editing an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Select the user profile you want to edit from the profile list.
4. Click **Edit**.
5. Edit the required fields in the Edit User Profile page.

   Note:

   You cannot edit an SNMPv3 user profile that is assigned to the serviceability agent of an element or that is attached to a target profile.

6. Click **Commit**.

Related links

SNMPv3 user profiles field descriptions on page 884

Viewing an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Click the user profile you want to view from the profile list.
4. Click **View**.

You can view the details, except the password, of the SNMPv3 user profile in the View User Profile page.

Related links

SNMPv3 user profiles field descriptions on page 884

Deleting an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Select the user profile or profiles you want to delete from the profile list.
4. Click **Delete**.
5. On the User Profile Delete Confirmation page, click **Delete**.

   Note:

   You cannot delete a user profile that is attached to an element or a target profile.

Filtering SNMPv3 user profiles

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Click **Filter: Enable** above the Profile List.
4. Apply the filter to one or multiple columns of the User Profile List.
5. Click **Apply**.

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

SNMPv3 user profiles field descriptions

Name	Description
User Name	The SNMPv3 user name. **Note:** The user name can contain the following characters: alphanumeric, period, underscore, white space, single quote, and hyphen. The user name cannot be blank.
Authentication Protocol	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The possible values are: • MD5

Table continues…

Name	Description
	• SHA The default is MD5.
Authentication Password	The password used to authenticate the user. **Note:** The password can contain any printable and non-whitespace characters. The password must be at least 8 characters in length and can contain up to 255 characters. The password cannot be an empty string.
Confirm Authentication Password	The authentication password that you re-enter for confirmation.
Privacy Protocol	The encryption policy for an SNMP V3 user. The possible values are: • DES: Use DES encryption for SNMP-based communication. • AES: Use AES encryption for SNMP-based communication. • None The default value is AES.
Privacy Password	The pass phrase used to encrypt the SNMP data.
Confirm Privacy Password	Retype the privacy password in this field for confirmation.
Privileges	The privileges that determines the operations that you can perform on MIBs. • Read/Write: Use to perform GET and SET operations. • Read: Use to perform only GET operation. • None The default is None.

Button	Description
Commit	Use to create a new SNMPv3 user profile. Saves the changes after an edit operation.
Back	Cancels the action and takes you to the previous page.
Delete	Use to delete the user profiles you select.
Edit	Use to edit the user profile you select.

Managing SNMP target profiles

SNMP Target profile list

Name	Description
Name	The name of the SNMP target profile. This name should be a unique value.
Domain Type	The type of transport for the flow of messages. The default value is UDP.
IP Address	The IP address of the SNMP target profile.
Port	The port of the SNMP target profile.
SNMP Version	The version of the SNMP protocol.

Button	Description
New	To go to the New Target Details page where you can add a new SNMP target profile.
View	To go to the View Target Details page where you can view an existing SNMP target profile.
Edit	To go to the Edit Target Details page where you can edit an existing SNMP target profile.
Delete	To delete the existing SNMP target profiles that you select.
Filter: Enable	To filter the SNMP target profiles list by one or multiple criteria.

Filtering target profiles

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. Click **Filter: Enable** above the Profile List.
4. Apply the filter to one or multiple columns of the Target Profile List.
5. Click **Apply**.

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

Creating an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. On the SNMP Target Profiles page, click **New**.
4. On the New Target Profiles page, complete the Target Details section.

5. **(Optional)** Click the **Attach/Detach User Profile** tab to attach a user profile.

   Perform the step only if you select the SNMPv3 protocol.

6. Click **Commit**.

Related links

SNMP target profiles field descriptions on page 888

Viewing an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. From the Target Profile list, click the profile you must view.
4. Click **View**.

   The system displays the details of the target profile in the View Target Details page.

Related links

SNMP target profiles field descriptions on page 888

Editing an SNMP target profile

About this task

Note:

Modify the target profiles that point to System Manager to reflect the changed IP address in the event of an IP address change on System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. In the Target Profile list, click the profile that you must edit.
4. Click **Edit**.
5. On the Edit Target Profiles page, modify the required fields.

   Note:

   You cannot edit a target profile that is assigned to the serviceability agent of an element. You must unassign the target profile before you edit the profile.

6. Click **Commit**.

Related links

SNMP target profiles field descriptions on page 888

Deleting an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. From the Target Profile list, click the profile or profiles you want to delete.
4. Click **Delete**.
5. On the Delete Confirmation page, click **Delete**.

   Note:

   You cannot delete a target profile that is attached to an element or an agent.

SNMP target profiles field descriptions

Name	Description
Name	The name of the SNMP target profile.
Description	The description of the SNMP target profile.
IP Address	The IP address of the target.
Port	The port number of the target.
Domain Type	The type of the message flow. The default is UDP.
Notification Type	The type of notification. The options are: • Trap • Inform
Protocol	The type of the SNMP protocol.

Button	Description
Commit	Creates the target profile in the New Target Profile page or saves the changes in the Edit Target Profile page.
Back	Cancels your action and takes you to the previous page.

Notification filtering

Notification filtering

System Manager supports alarm filtering capability. With filtering, you can select a product that System Manager supports to send filtered alarms only to specific targets.

When you send notifications to System Manager , SAL Gateway or other Network Management System (NMS), you can exclude or include notifications from elements. You can create filter profiles and assign the profiles to the target and serviceability agent pair. You can also remove the profiles from the target and serviceability agent pair. You can select alarms that you want to receive from a product on NMS. NMS can be System Manager or a third-party NMS system.

For a product, you can define the filter criteria to receive notifications on the target serviceability agent from the specific OIDs or block notifications on the target serviceability agent from the specific OIDs.

For example:

- To receive only major alarms from Session Manager, you must create a filter profile for Session Manager, select all major alarm OIDs and assign the filter profile to the target NMS for the serviceability agent of that Session Manager so that the target receives only the alarms specified in the filter profile.
- To block warning or minor alarms from Session Manager, you must create a filter profile for the product Session Manager, select exclude option and select OIDs of type warning and minor, and then assign the filter profile to the target NMS for the serviceability agent of Session Manager so that the target does not receive warnings and minor alarm notifications from that Session Manager.

Creating a notification filter profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Notification Filter Profile**.
3. On the Filter Profiles page, click **New**.
4. On the New Filter Profile page, click the **Filter Profile Details** tab and complete the fields.
5. Click **Exclude** or **Include**.

   The default is Include.

   For more information, see Create, View, Edit, or Delete Filter Profiles field descriptions.
6. Click the **Attach/Detach Notification Oids** tab, perform the following:
   a. In the **Notification Subtree** field, type a value that ends with dot star (.*) and click **Add**.

      For example, 6889.2.35.*

      System Manager excludes or includes alarms from the notification IDs that you select.

      Note:

      - If you perform Step 6a, Step 6b and Step 6c are optional.
      - If you perform Step 6b and Step 6c, Step 6a is optional.

   b. In the **Select Notifications** section, in the **Products** field, select a product.

   c. In the notification list, select one or more notification IDs.
7. Click **Commit**.

Related links

Create, View, Edit, or Delete Filter Profiles field descriptions on page 892
Filter Profiles field descriptions on page 892

Assigning filter profile to a serviceability agent on page 891
Unassigning the filter profile from a serviceability agent on page 891

Viewing the notification filter profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Notification Filter Profile**.
3. On the Filter Profiles page, select a filter profile and click **View**.
4. On the View Filter Profile page, review the fields on the following tabs:
   - **Filter Profile Details**
   - **Attach/Detach Notification Oids**
5. Click **Done**.

Related links

Create, View, Edit, or Delete Filter Profiles field descriptions on page 892
Filter Profiles field descriptions on page 892

Editing notification filter profiles

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Notification Filter Profile**.
3. On the Filter Profiles page, select a filter profile and click **Edit**.
4. On the Edit Filter Profile page, complete the following:
   a. Click the **Filter Profile Details** tab and complete the fields.

      For more information, see Create, View, Edit, or Delete Filter Profiles field descriptions.

   b. Click the **Attach/Detach Notification Oids** tab and complete the fields.
5. Click **Commit**.

Related links

Create, View, Edit, or Delete Filter Profiles field descriptions on page 892
Filter Profiles field descriptions on page 892

Deleting the notification filter profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Notification Filter Profile**.

3. On the Filter Profiles page, select a filter profile and click **Delete**.
4. On the Filter Profile Delete Confirmation page, click Delete.

Related links

Create, View, Edit, or Delete Filter Profiles field descriptions on page 892
Filter Profiles field descriptions on page 892

Assigning filter profile to a serviceability agent

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. Select a product for which you created the filter profile.
4. Click **Manage Profiles**.

   The system displays the serviceability agent in the **Selected Agents** section.
5. Click the **SNMP Target Profiles** tab, select System Manager or the third-party NMS target agent, and click **Assign**.

   The system displays the target in the list.
6. To assign the filter profile from the serviceability agent, perform the following:
   a. In the **Removable Profiles** section, select the target.

      The **Assign/Remove Filter Profile** link becomes active.
   b. Click **Assign/Remove Filter Profile**.
7. In the **Profile List** section, click the plus sign (+).

   The system displays the filter profile that you selected in the **Assigned Filter Profiles** section.

   Note:

   You can assign only one filter profile to the target agent for a serviceability agent. For example, for a Session Manager serviceability agent, if the target is System Manager, then you can add only one filter profile to the System Manager target for the same Session Manager system.
8. Click **Commit**.

   The system assigns the filter profile to the serviceability agent.

Related links

Unassigning the filter profile from a serviceability agent on page 891

Unassigning the filter profile from a serviceability agent

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.

2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. Select a product for which you created the filter profile.
4. Click **Manage Profiles**.

   The system displays the serviceability agent in the **Selected Agents** section.
5. Click the **SNMP Target Profiles** tab.
6. In the **Removable Profiles** section, select the target.

   The **Assign/Remove Filter Profile** link becomes active.
7. Click **Assign/Remove Filter Profile**.
8. In the **Assigned Filter Profiles** section, click the minus sign (-).

   The system displays the filter profile in the **Profile List** section.
9. Click **Commit**.

   The system disassociates the filter profile from the serviceability agent.

Related links

Assigning filter profile to a serviceability agent on page 891

Filter Profiles field descriptions

Name	Description
Name	The name of the notification filter profile.
Description	A description of the notification profile.

Button	Description
New	Displays the New Filter Profile page where you can create a notification filter profile.
View	Displays the View Filter Profile page where you can view a notification filter profile.
Edit	Displays the Edit Filter Profile page where you can view a notification filter profile.
Delete	Marks the notification filter profile that you select. You must confirm for the system to delete the profile.

Create, View, Edit, or Delete Filter Profiles field descriptions

Filter Profile Details

Name	Description
Name	The name of the notification filter profile.
Description	A description of the notification filter profile.

Table continues…

Name	Description
Specify Include/Exclude criteria	An option to include or exclude the notification OIDs. • **Include** • **Exclude** The default is **Include**.

Attach/Detach Notification Oids Specify Notification Subtrees

Name	Description
Notification Subtree	The notification subtree that you want to add to the subtree list. The value you enter must end with dot followed by start (.*), for example, 6889.4.*. Otherwise the system does not add notification subtree to the list.
Add	Adds the notification subtree to the list.

Specify Notifications

Name	Description
Product	The product for which you want to filter the notifications while sending notifications to System Manager, SAL Gateway or other NMS systems.

Button	Description
Commit	Saves the changes made to the page and returns to the Filter Profile page.
Back	Discards the changes and returns to the Filter Profile page.

Managing user and target profiles

Serviceability Agents list

Name	Description
Hostname	The host name of the server on which the serviceability agent runs.
IP Address	The IP address of the server on which the serviceability agent runs.
System Name	The system name of the server on which the serviceability agent runs.
System OID	The system OID of the server on which the serviceability agent runs.

Table continues…

Name	Description
Status	The enabled or disabled status of the serviceability agent. The system disables SNMPv3 and displays **Inactive** as the default status.

Automatic activation of serviceability agents

For newly installed elements that work with Release 6.3.8 serviceability agents, you do not need to manually activate the agents from the Manage Serviceability Agent page.System Manager automatically activates the agents. In the **Agents List** section, the system displays the agent as Active. You can assign the target or user profiles to the agent that is automatically activated.

✱ **Note:**

The auto activate functionality only applies to serviceability agents added in Release 6.3.5 or later. If you recover an agent by running the **`recoverAgent`** script, then the system adds the agent after receiving the next heartbeat message. The system automatically activates the recovered agent.

Repairing serviceability agents

About this task

If the alarming functionality of an element fails, you can repair the serviceability agent. The repair process triggers the SNMP configuration.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In the **Agent List** section, select one or more active agents that you want to repair.
4. Click **Repair Serviceability Agent**.

   The system starts the SNMP configuration of the serviceability agent. At the subsequent heartbeat of the agent, the system notifies System Manager about the start of the SNMP configuration. Therefore, wait for about 15 minutes, the heartbeat interval, to test alarms from the element.

   When System Manager receives the subsequent heartbeat, the system reactivates the agent. The system also assigns the target profiles and user profiles to the agent and the alarming functionality starts working.
5. **(Optional)** To make the changes immediately, log in to the server on which the serviceability agent runs and type `service spiritAgent restart`.

   You can perform this step if you do not want to wait for the next heartbeat of the agent.

Activating a serviceability agent

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.

2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In the **Agent List** section, select one or more agents that you must activate.
4. Click **Activate**.

   The system activates the SNMPv3 functionality in the remote serviceability agent that you selected. If the system does not activate the SNMPv3 functionality, refresh the Web page and repeat Step 3 and Step 4.

Related links

Managing SNMPv3 user profiles for the selected serviceability agents on page 895
Managing target profiles for the selected serviceability agents on page 895

Managing target profiles for the selected serviceability agents

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In Agent List, select the active agents that you must manage.
4. Click **Manage Profiles**.
5. Click the **SNMP Target Profiles** tab.
6. Select the target profiles you must assign from the Assignable Profiles section.
7. Click **Assign**.

   You can unassign or remove target profiles from the Removable Profiles section by clicking **Remove**.
8. Click **Commit** to assign the profiles to the selected agent.

   Note:

   You can also select more than one serviceability agents and assign the same target profiles to all the agents.

Related links

Activating a serviceability agent on page 894
Managing SNMPv3 user profiles for the selected serviceability agents on page 895

Managing SNMPv3 user profiles for the selected serviceability agents

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In the **Agent List** section, select an active agent that you must manage.
4. Click **Manage Profiles**.
5. Click the **SNMPv3 User Profile** tab.

6. In the **Assignable Profiles** section, select the user profiles that you want to assign.
7. Click **Assign**.

   To remove user profiles, in the **Removable Profiles** section, select the user profiles and click **Remove**.
8. To assign the user profiles to the selected agent, click **Commit**.

   Note:

   You can also select more than one serviceability agents and assign the same user profiles to all agents.

Related links

Activating a serviceability agent on page 894
Managing target profiles for the selected serviceability agents on page 895

Synchronization of Data

Communication Manager, Messaging data, and IP Office synchronization

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 Communication Manager, messaging data, and IP Office through this menu.

Communication System

Using System Manager, you can synchronize the System Manager data with the Communication Manager system. When you add Communication Manager to the system, System Manager automatically initiates synchronization to update the System Manager database.

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.

Important:

If there is a change in any of the following Communication Manager objects in the Communication Manager, you should perform full initialization synchronization of this Communication Manager in System Manager. You must manually initiate the full synchronization process. The Communication Manager objects are:

- system-param features
- system-param cdr
- system-param cust
- system-param spec
- system-param security

- system-param country-options
- system-param maintenance
- dialplan
- cabinet
- board

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.

Important:

In the following scenarios, even if you perform an incremental synchronization, the system initiates an initializing synchronization:

- when you upgrade System Manager. The system displays the synchronization status as *SMGR Upgraded*, and you can continue to perform the administrative tasks even after System Manager is upgraded.
- when you upgrade or downgrade Communication Manager.

IP Office system

Using System Manager, you can synchronize the System Manager data with IP Office. When you add a new IP Office device to System Manager, System Manager automatically initiates synchronization to update the System Manager database.

Synchronizing messaging data

You can also synchronize messaging data in System Manager with Messaging, 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.

Scheduled synchronization

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 an initialization synchronization or an incremental synchronization.

Related links

Initializing synchronization on page 898
Incremental Synchronization on page 899

Saving the Communication Manager translations on page 901

Synchronizing the Communication Manager data and configuring options

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Communication System**.
3. Select the Communication Manager device that you want to synchronize.
4. Select one of the following options that you want to synchronize for the selected device:
   - **Initialize data for selected devices**: To synchronize data in the System Manager database with each managed Communication Manager system.

     ✱ **Note:**

     When you add a Communication Manager instance to the system, System Manager automatically initiates an initialization task to get all the required Communication Manager data and stores the data in the System Manager database.
   - **Incremental Sync data for selected devices**: To synchronize incrementally the selected devices data in the System Manager database with each managed Communication Manager system.

     ✱ **Note:**

     This synchronization updates the data in the database in Communication Manager that is changed since last synchronization.
   - **Execute 'save trans all' for selected devices**: To save the configuration of the selected device on the same device, Communication Manager itself.
5. Perform one of the following:
   - To perform the synchronization now, click **Now**.
   - To perform the synchronization at a specified time, click **Schedule**.

   ✱ **Note:**

   To view the status of synchronization, on the System Manager web console, click **Services** > **Scheduler**.

Initializing synchronization

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Communication System**.
3. Select the Communication Manager entities you want to synchronize.
4. Select **Initialize data for selected devices**.

5. To initialize synchronization, click **Now**, or perform one of the following tasks:
   - To perform the synchronization at a specified time, click **Schedule**.
   - To cancel the synchronization, click **Cancel**.

Incremental Synchronization

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Communication System**.
3. Select the Communication Manager systems that you want to synchronize.
4. Select **Incremental Sync data for selected devices**.
5. Click **Now** to perform the incremental synchronization or do one of the following:
   - To perform the synchronization at a specified time, click **Schedule**.
   - To cancel the synchronization, click **Cancel**.

   Note:

   While scheduling incremental synchronization, set the logging levels on Communication Manager using the **change logging-levels** option. In the **Log Data Values** field, select `both`.

   When you add a Communication Manager system, the default incremental synchronization jobs will be scheduled 1 hour after the maintenance job starts on Communication Manager.

   If the incremental synchronization of the Communication Manager data fails due to the overlapping of Communication Manager synchronization and maintenance jobs, change the default scheduled job time in the Pending Jobs page.

Synchronizing the IP Office system configuration

Procedure

1. On the System Manager console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **IP Office**.
3. Select the device you want to synchronize.
4. Below the device list, select any of the following options that you want to synchronize for the selected device:
   - **System Configuration**: This option enables you to get the latest system configuration of the device and update the same in System Manager.
   - **User**: This option enables you to synchronize all the users present in System Manager from the selected device.
   - **System Configuration and Users**: This option enables you to get the latest system configuration and details of all the users from the selected device and synchronize with System Manager.

5. Click **Now** to perform the synchronization now or click **Schedule** to perform the synchronization at a specified time.

   Note:

   To view the status of synchronization, click **Services** > **Scheduler** on the System Manager console.

Synchronizing the UCM and Application Server system configuration

About this task

Use the procedure to synchronize the configuration of a UCM and Application Server device with the local machine.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **UCM and Application Server**.
3. Select the device that you want to synchronize.

   System Configuration is selected by default.
4. Do one of the following:
   - To perform the synchronization now, click **Now**.
   - To perform the synchronization at a specified time, click **Schedule**.
5. To view the status of synchronization, click **Services** > **Scheduler**.

Synchronizing the VMPro system configuration

Before you begin

To synchronize VMPro devices successfully, you must perform the following:

- Configure VMPro IP Address in IP Office System Configuration.
- Password of VMPro should be same forIP Office, UCM and Application Server and VMPro System Preferences.

  Note:

  - You can change the password for Application Sever through security setting using IP Office Manager.
  - You can change the password for VMPro System Preferences through Web Manager.
- You must give access rights to VMPro Application from security setting of IP Office and UCM and Application Server through IP Office Manager.
- You must have valid IP Office licenses for VMPro instances.

Procedure

1. On the System Manager console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **VMPro**.

3. Select the device you want to synchronize.
4. In the device list, select any of the following options that you want to synchronize for the selected device.
5. Click **Now** to perform the synchronization now or click **Schedule** to perform the synchronization at a specified time.

   Note:

   To view the status of synchronization, click **Services** > **Scheduler** on the System Manager console.

Result

If the operation of synchronizing the VMPro succeeds, you can work on the latest updated vmpro system configuration and avoid data corruption.

If the operation of synchronizing the VMPro fails, you can work only on local available system configuration in System Manager.

If the operation of synchronizing the VMPro fails and if it is first time that you attempted data synchronization, you can work only on the default configuration.

Synchronizing the messaging data

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Messaging System**.
3. Select the messaging systems that you want to synchronize.
4. Perform one of the following:
   - Click **Now** to perform the synchronization now.
   - Click **Schedule** to perform the synchronization at a specified time.

Saving the Communication Manager translations

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Communication System**.
3. From the list select a Communication Manager system.
4. Select **Execute 'save trans all' for selected devices**.
5. To save the System Manager administration changes in Communication Manager, click **Now**.

   To save the translations at a specified time, click **Schedule**.

✱ **Note:**

After running the **Save translation job**, the system may not update the last saved translation time in the Communication Manager list. This might be because the save translation operation is slow when Communication Manager has large data or translations to save. In such conditions, the system updates the last saved translation time only on the next incremental synchronization after the save translations operation is complete on Communication Manager.

About CM audit

You can perform a CM audit for those Communication Managers that are synchronized with System Manager. You can select one or more Communication Managers and perform the audit. After the audit is completed, you can view the results by clicking **View Audit Report**. This audit report comprises the audit summary or a snapshot of the changes, and the audit details or the detailed report of the changes.

Performing a Communication Manager audit

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Communication System**.
3. Select the Communication Managers that you want to audit.
4. Click **Audit**.
5. Click **Now**.

   To schedule the audit at a later time, click **Schedule**.
6. To view the audit report, click **View Audit Report**.
7. On the Audit Info page, select the job name, and click **View**.

Related links

Audit report field descriptions on page 903
CM audit field descriptions on page 902

CM audit field descriptions

Name	Description
Job Name	The name of the audit job.
Job Status	The status of the job. Specifies whether the audit job is pending, failed, or complete.
Start Time	The start time of the audit job.
End Time	The end time of the audit job.

Button	Description
View	Click to go to the audit report page.
Done	Click to complete the current action and go to the previous page.

Audit report field descriptions

Name	Description
Object Name	The name of the Communication Manager object that is audited.
Identifier	The identifier for the Communication Manager object.
CM	The **CM** field specifies all the changes in Communication Manager after the audit is complete.
System Manager	The **System Manager** field specifies all the changes in System Manager after the audit is complete.

Button	Description
Done	Click to go to the previous page.

Communication Profiles synchronization

Communication profiles synchronization

System Manager provides the account synchronization feature to synchronize profiles between CS 1000 or CallPilot communication profile and their elements. Using this feature you can synchronize profiles in User Management with the profiles in the elements. During synchronization, the account synchronization feature uses the account data in the elements as the master data. Therefore, when a profile data is not in synchronization with the element, the account data from the element is copied to System Manager.

Synchronizing the CS 1000 and CallPilot profiles

Before you begin

Register all CS 1000 and CallPilot elements on System Manager 6.2 or later.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **CS 1000 and CallPilot Synchronization**.
3. Select the element that you want to synchronize.
4. Click **Start** to start the synchronization process.

> **Note:**
>
> For the average duration of operations of the CS 1000 element, see Average duration of CS 1000 account operations.

5. **(Optional)** Do one of the following:
   - Click **Stop** to stop the synchronization process.

     The system disables all other buttons when you click **Stop**.
   - Click **Clear** to clear the synchronization information that the system displays.
   - Click **Reload** to refresh.

Related links

Adding CallPilot to the element registry on page 553
Bulk importing of users
Exporting users in bulk from web console on page 328
Synchronize communication profiles field descriptions on page 905
Average duration of CS 1000 account operations on page 907

Assigning anonymous profiles

About this task

When the synchronization process is complete, the **Summary** column displays any anonymous accounts in the element. You can assign the anonymous account to users or delete the account from the element.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **CS 1000 and CallPilot Synchronization**.
3. On the Synchronize Communication Profiles page, in the **Summary** column, click the anonymous profile that you want to assign.

   The system displays the Anonymous Communication Profiles page with the details of each anonymous account.
4. Select one of the anonymous accounts.
5. In the **Name (Last, First)** field, enter the name of the user to whom you want to assign this communication profile.
6. Click **Assign**.

   The system refreshes the Anonymous Communication Profiles page and displays the status of the assigned account.

Related links

Anonymous Communication Profiles field descriptions on page 906

Deleting anonymous profiles

About this task

You can delete the anonymous account from the element.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **CS 1000 and CallPilot Synchronization**.
3. On the Synchronize Communication Profiles page, click the anonymous profile you want to delete from the **Summary** column.

   The system displays the Anonymous Communication Profiles page with the details of each anonymous account.
4. Select the anonymous account you want to delete.
5. Click **Delete**.

   The system displays a confirmation dialog box.
6. Click **OK**.

Cleaning up communication profiles

About this task

When you delete the CS 1000 or CallPilot element from the System Manager web console, the communication profiles linked to the element still exist in User Management. You can use the CS 1000 or CallPilot communication profiles cleanup feature to permanently delete all accounts of elements that do not exist in the System Manager registry.

Before you begin

The system does not delete the communication profiles of the soft deleted users. Therefore, before you run the cleanup, restore the soft deleted users.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **CS 1000 and CallPilot Synchronization**.
3. Click **CleanUp**.
4. To confirm the operation, click **OK**.

Synchronize communication profiles field descriptions

Name	Description
Element	Name of the CS 1000 or CallPilot system.

Table continues…

Name	Description
Status	Current status of the synchronization process. The following are the possible values: • Queued - The synchronization task is queued and runs automatically once other synchronization tasks have completed. • Running - The synchronization is running. This status appears once you click the **Start** button. • Stopping- The synchronization is stops if you click the **Stop** button. • Aborted - This status appears once the synchronization stops completely. • PASS - This status indicates that the synchronization is complete. • FAIL - This status indicates that the synchronization has failed. You can look into thje log files for the information on the failure.
Date	Displays the date when the synchronization started.
Summary	Displays the number of accounts processed, the number of anonymous accounts, the number of accounts added, updated and deleted. When no accounts are processed, this field displays “O account(s) processed”.

Button	Description
Start	Starts a synchronization process.
Stop	Stops a synchronization process that is in the running state.
Clear	Clears all the synchronization results that are processed.
Reload	Refreshes the synchronization status once again.

Anonymous Communication Profiles field descriptions

Field	Description
Name (Last, First)	The name of the user to whom you must assign this communication profile.
Service Information	The service information of the CS 1000 or CallPilot system.
Target	The customer number of the system for the element.

Table continues…

Field	Description
Status	The status of the anonymous profile. The options are: • Assigned • Anonymous

Button	Description
Assign	Assigns the user to the anonymous profile that you select.
Delete	Deletes the anonymous profile that you select after confirmation.
Cancel	Cancels the assign or delete action and opens the previous page.

Related links

Average duration of CS 1000 account operations on page 907

Average duration of CS 1000 account operations

Operation	Duration in seconds
Account add	9
Account update	1
Account delete	1
Account anonymous	0.1

Configure options

The Uniform Dial Plan (UDP) 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 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 on the Synchronize CM Data and Configure Options page from **Elements** > **Communication Manager** > **System** > **Uniform Dial Plan Groups**. When you select the **Consider UDP** option, the system does not use the corresponding dial plan for the available extension range while adding an endpoint. When you do not select the **Consider UDP** option, the system uses the corresponding dial plan for the available extension range while adding an endpoint.

Chapter 16: Managing events

Managing alarms

Alarming

The Alarming service provides an interface for monitoring alarms generated by System Manager and other components. You can:

- View an alarm.
- Change the status of an alarm.
- Export alarms to a Comma Separated Values (.csv) file through the Alarming service.

System Manager generates alarms to notify users of system events. Alarms are classified by their effect on system operation. Alarms can also identify the system component that generated the alarm.

Note:

- For Release 6.1 elements with 6.1 SAL agent, and Release 6.2 elements with 6.2 serviceability agent, System Manager cannot forward traps to NMS. You can configure 6.1 elements with 6.1 SAL agent and 6.2 elements with 6.2 serviceability agent to send SNMP traps directly to a customer Network Management System (NMS).

  However, for Release 6.2.x elements, you can configure the serviceability agent from System Manager instead of configuring in each element.
- For Release 5.2 elements and Release 6.0 elements, you can configure System Manager to forward alarms to Avaya Data Center (ADC).

For information on configuring serviceability agents, see Managing Serviceability Agents.

Related links

Serviceability Agents on page 881

Viewing alarms

Procedure

1. On the System Manager web console, click **Services** > **Events**.

2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, select an alarm from the Alarm List. You can select multiple alarms.
4. Click **View**.

   The system displays the alarm details on the Alarm - View Alarm Detail page.

Changing the alarm status

The status of an alarm can be:

- **Acknowledged**: Maintenance support must manually set the alarm to this state. Indicates the alarm is under investigation.
- **Cleared**: Maintenance support must manually set the alarm to this state. Indicates the error condition has been resolved. The auto alarm clear event might result in the Cleared status.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, select an alarm and click **Change Status**.

   You can select multiple alarms.
4. Click the status that you want to apply to the selected alarms.

Exporting alarms

You can export alarms 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 Microsoft Excel.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, perform one of the following actions:
   - To export an alarm to a CSV file, select an alarm and click **More Actions** > **Export Selected**.
   - To export the filtered alarms to a CSV file, click **More Actions** > **Export All**.

     When you use **Advanced Search** or **Filter** option to filter alarms based on some criteria, **Export All** exports all the filtered data.
4. Click **Save** to save the exported file to the local disk.

Deleting alarms

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, perform one of the following steps:
   - To delete a specific alarm from the list, select the alarm that you must delete, and click **More Actions** > **Delete Selected**.
   - To delete all the alarms from the database, click **More Actions** > **Delete All**.
4. Click **OK**.

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.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, select the alarms you want to filter.
4. Click **Filter: Enable** at the top right corner of the Alarm List table.
5. 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 that contain a particular alarm code.
6. Click **Filter: Apply**.

   ✱ **Note:**

   The system displays a message if no records are found that match the specified filter criteria.

Result

The system displays the alarms that match 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 that satisfy the search conditions. You can specify multiple search conditions.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, click **Advanced Search**.
4. 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**.
5. Select or enter the search value in the third field.
6. To add another search condition, click **+** and perform the following:
   a. Select the AND or OR operator from the drop-down field.
   b. Repeat Step 4 and Step 5.

   To delete a search condition, click **-**. You can delete a search condition only if you added more than one search condition.
7. To find alarms for the given search conditions, click **Search**.

Configuring the throttling period alarm

About this task

You can configure the throttling period in minutes as threshold for all alarms or alarms specific to events at SAL Agent from Avaya Aura®. The system eliminates any redundant alarms raised within the configured period at SAL Agent.

Procedure

1. Log in to System Manager through CLI as root.
2. Open the `AlarmThrottle.properties` properties file from the `$SPIRIT_HOME/config/agent` location.
3. Type `AlarmThrottlePeriod=2` in the file.

   The system sets the throttle period in minutes and applies the configured period to all outgoing alarms.

4. To configure the throttle time for a specific event, open the `EP_BAse_Rules.xml` files which contain the events and add the following lines:

   ```
   <tns:ExtraAttribute>
   <tns:ExtraAttributeName>alarmThrottleInterval</tns:ExtraAttributeName>
   <tns:ExtraAttributeValue>2</tns:ExtraAttributeValue>
   </tns:ExtraAttribute>
   ```

   You can apply the alarmThrottleInterval as the alarm throttle period for a specific event. If you do not use the generic and the specific mechanisms, the system disables alarm throttling. The system sets the default alarm throttling period to 720 minutes or 12 hours. If you reconfigure the period, you must restart SAL Agent.

5. To disable alarm throttling, perform the following steps:

   a. In the `$SPIRIT_HOME/config/agent/AlarmThrottle.properties` file, set AlarmThrottlePeriod=-1.

   b. Restart SAL Agent.

Generating test alarms

Test alarms

You can generate a test alarm and a clear event corresponding to the generated test alarm. The severity level of the test alarm is minor. The clear event generated has no definite severity level. The clear event updates the status of the test alarms from Raised to Cleared. If Secure Access Link (SAL) Enterprise is configured to forward alarms to Avaya Data Center (ADC), the system also forwards the test alarm and the clear event for the test alarm to the ADC.

Test Alarm Event

Test Alarm property	Value
Alarm.Message	Test alarm
Alarm.Severity	Minor
Alarm.Status	Raised
Alarm.Log.ProcessName	TESTALARM
Alarm.Log.EventCode	TEST_ALARM_GEN_0001

Test Clear Event

Test Clear Event property	Value
Alarm.Message	Clear event for test alarm
Alarm. Severity	Indeterminate
Alarm.Status	Cleared
Alarm.Log.ProcessName	TESTALARM
Alarm.Log.EventCode	TEST_ALARM_CLR_0000

Related links

Generating the test alarm from the web console on page 914
Generating the test alarm from CLI on page 914

Generating the test alarm from the web console

About this task

You can generate test alarms from the System Manager web console for agents, hosts, or elements that are installed with Serviceability Agents running version 6.3.2.4-6706-SDK-1.0 or later.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In the **Agent List** section, select one or more agents for which you want to generate alarms.
4. Click **Generate Test Alarm**.

   The system generates the alarm.
5. To view the alarm, click **Events** > **Alarms**.

   To view the details of the alarm, wait until the system displays the alarms on the Alarming page.

Generating the test alarm from CLI

Procedure

1. Log in to the computer on which you installed System Manager.
2. At the command prompt, perform the following:
   a. To check the status of SAL Agent, type `service spiritAgent status` and press `Enter`.

      The system displays `SPIRIT Agent is running`.

      Note:

      If the system displays `SPIRIT Agent is not running`, then start SAL Agent.

   b. To start SAL Agent, type `service spiritAgent start` and press `Enter`.

      The `utils` directory contains SAL Agent command line utilities.
3. To navigate to the `utils` directory, at the prompt, type `cd $SPIRIT_HOME/scripts/utils/`and press `Enter`.

4. Perform one of the following:
    - To generate the test alarm for System Manager, type `sh generateTestAlarm.sh`, and press `Enter`.
    - To generate the clear alarm for System Manager, type `sh generateTestAlarm.sh -c`, and press `Enter`.
5. Perform one of the following:
    - To generate the test alarm for a different product, type `sh generateTestAlarm.sh -l LOG_LOCATION -p PRODUCT_TYPE`, and press `Enter`.
    - To generate the clear alarm for a different product, type `sh generateTestAlarm.sh -c -l LOG_LOCATION -p PRODUCT_TYPE`, and press `Enter`.

      Here, *LOG_LOCATION* is one of the log files that the SAL agent tails for this product, and `PRODUCT_TYPE` is the log product type that you configured for this product in the SAL agent.

Managing Geographic Redundancy related alarms

Forwarding the secondary System Manager alarms to the primary System Manager server

Before you begin

Log on to the System Manager web console of the primary server.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents.**

   The system displays the entries for the primary and the secondary System Manager.
3. Create a target profile of the primary System Manager server, and copy the profile to the secondary System Manager server.

   The system forwards the secondary System Manager alarm to the primary System Manager server.

Viewing the secondary System Manager alarms

About this task

You can view the alarms for the secondary System Manager that is in the standby mode.

Procedure

1. Log in to System Manager through CLI as root.
2. Type `sh $MGMT_HOME/alarmingui/scripts/DisplayAlternateDBAlarms.sh`.

3. At the prompt, type the number that matches the option that you must select from the following options:
    - (0) Exit
    - (1) Display All Alarm count
    - (2) Display alarm by notification oid (0)
    - (3) Display alarm by Status (0)
    - (4) Clear Alarm with notification oid (0)
    - (5) Display all alarms
    - (6) Display Alarms by severity (0)

    The system displays the alarms according to the option that you selected.

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
Time Stamp	The date and time when the alarm is generated.
Severity	The severity of the alarm.
Status	The current status of the alarms.
Host Name/SysName	The name of the host computer that generated the alarm.
Source IP address	The IP address of the system from that generated the alarm.
Description	The detailed description of the problem that generated the alarm.
Identifier	The unique identifier for an alarm.
Event ID	The log event ID if the alarm is generated from logs or the Event OID if the alarm is generated from the trap listener service.
NotificationOID	The SNMP OID of the alarm.
M/E Ref Number/SysOID	The unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm. For alarms that are generated from trap listener, the system displays the System OID.

Button	Description
Alarm landing Page	Changes the mode from **Auto-Refresh** to Manual refresh and displays the Alarming home page. This is a toggle button.

Alarming field descriptions

The Alarming home page contains two sections: upper and lower. The upper section contains 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
Time Stamp	The date and time when the alarm is generated.
Severity	The severity of the alarm.
Status	The current status of the alarms.
Host Name / SysName	The name of the host server that generated the alarm. In case of the trap listener service, this column displays the system name.
Source IP Address	The IP address of the system that generated the alarm.
Description	The detailed description of the problem that generated the alarm.
M/E Ref Number / SysOID	The unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm. For alarms that are generated from trap listener, the system displays the System OID.
Identifier	The unique identifier for an alarm.
Event ID	The log event ID if the alarm is generated from logs or the Event OID if the alarm is generated from the trap listener service.
NotificationOID	The SNMP OID of the alarm.

Button	Description
View	The details of the selected alarms.

Table continues…

Button	Description
Change Status	Changes the status of the selected alarm. The options are: • **Acknowledged** • **Cleared**
Auto-Refresh Mode	Changes over to the **Auto-Refresh** mode. When the Alarming page is set in this mode, it automatically updates the alarms in the table. A toggle button.
More Actions > **Export Selected**	Exports the selected alarms to a CSV file. You can view the logs using the Wordpad or Excel application.
More Actions > **Export All**	Exports all the alarms to a CSV file. You can view the logs using the Wordpad or Excel application. **Note:** When you use **Advanced Search** or **Filter** option to filter alarms based on some criteria, **Export All** exports all the filtered data.
More Actions > **Delete Selected**	Deletes the alarms that you select from the list.
More Actions > **Delete ALL**	Deletes all alarms that the system displays on the page.
Advanced Search	Displays fields that you can use to specify the search criteria for searching an alarm.
Refresh	Refreshes the log information in the table.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. A toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. A toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters alarms based on the filter criteria.
All	Selects all the alarms in the table.
None	Clears the check box selections.
Previous	The logs in the previous page. This button is not available if you are on the first page.
Next	The logs in the next page. This button is not available if you are on the last page.

Criteria section

This system displays the section when you click **Advanced Search** on the upper-right corner of page.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td><b>Criteria</b></td><td>
<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 list. Enter the search value in the text field.</p>
<p>Select following search criteria from the first drop-down list:</p>
<ul>
<li>Time Stamp: 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>Severity: Searches all the alarms that match the specified severity level.</li>
<li>Status: Searches all the alarms that match the specified status.</li>
<li>Host Name: Searches all of the alarms that are generated from the specified host.</li>
<li>M/E Ref Number: Searches all the alarms that match the specified M/E Ref Number.</li>
<li>Event ID: Searches all the alarms that match the specified Event ID.</li>
<li>Source IP address: Searches all of the alarms that are generated from the specified source IP address.</li>
<li>NotificationID: Searches all the alarms that match the specified NotificationID.</li>
<li>Identifier: Searches all the alarms that match the specified identifier.</li>
<li>Description: Searches all the alarms that match the specified description.</li>
</ul>
<p>The operators available are based on the search criterion that you select in the first drop-down field. The following table lists the operators that are available for a search criterion:</p>
<table>
<tr><th>Criterion</th><th>Operators</th></tr>
<tr><td>Time Stamp</td><td>=, >, <, >=, <=, >=, !=</td></tr>
<tr><td>Severity</td><td>Equals, Not Equals</td></tr>
<tr><td>Status</td><td>Equals, Not Equals</td></tr>
</table>
<p><i>Table continues…</i></p>
</td></tr>
</table>

Table continues…

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Criterion</th><th>Operators</th></tr>
<tr><td>Host Name</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr>
<tr><td>Identifier</td><td>=, >, <, >=, <=, >=, !=</td></tr>
<tr><td>Source IP address</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr>
<tr><td>Event ID</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr>
<tr><td>Description</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr>
<tr><td>M/E Ref Number</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr>
</table>
When you select <b>Begin Date</b> and <b>End Date</b> from the first drop-down list, you are prompted to enter the date in the third field.
</td></tr>
</table>

Button	Description
Clear	Clears the entered search criteria and sets the default search criteria.
Search	Searches the alarms based on the search conditions.
Close/Advanced Search	Hides the search fields.
+	Adds a search condition.
-	Deletes a search condition.

Managing logs

Logging service

The Logging service provides configuration capabilities and overall management of logs. The Logging service receives and stores log events and harvests file-based logs or local database logs. You can view and monitor logs and their details through the log viewer using the System Manager Web Console. The log viewer is integrated with the common console to provide consistent presentation of log messages for System Manager and the adopters.

The log viewer displays a list of logs where you can view the details of each log, perform a search for logs, and filter specific logs. The log details include information about the event that generates 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.

The following are some of the log types:

- 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.

The Logs menu in System Manager comprises of:

- Log Harvester: Through the Log Harvester menu you can harvest log files for one or more products of same or different types, running on the same computer or on different computers.
- Log Settings: This menu displays the loggers and appenders for the selected log configuration file. You can modify the logger and appender settings through this menu.
- Log Viewer: The log viewer allows you to view the logs generated by System Manager and other components and their details. You can view details of each log, perform a search for logs, and filter specific logs.

Log Types

The following are some of the log types that you might come across when viewing logs on the System Manager Web Console. You can view the station-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 are 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 those gathered for the debug types mentioned above.

Managing log harvester

Log Harvester

The Log harvesting service manages the retrieval, archival, and analysis of harvested log files stored in Serviceability Agent enabled hosts or elements. The Serviceability Agent harvests the logs and sends the harvested logs to the Logging Service through HTTPS. The logging service recognizes a successful harvest request related to a harvest profile, accepts the file segments, creates a well-defined file structure, and saves the request in the System Manager node.

You can harvest log files for one or more products of the same or different types running on the same computer or on different computers. The system displays the list of file archives and respective profiles on the log harvesting user interface and the status of each archive is available in the user interface table.

You can perform the following operations using the log harvesting service:

- 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 to a local computer.
- Search for a matching text in the harvested log files.

Accessing the Log Harvester service

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.

Result

The system displays the **Log Harvester** page.

Creating a new log harvesting profile

About this task

To create a new log harvesting profile, you must specify:

- The host name of the server on which the product is running

  Note:

  If you do not see the host name of CS 1000 when you create the profile, at the command prompt of CS 1000, run the following command:

  ```
  cd /opt/nortel/oam-logging
  ./configureSpiritAgentClient.sh <enrollment password>
  ```

  The system now enrolls CS 1000 to the log harvester of System Manager.
- The product name
- The directories or the log files
- The filter text if you select one or more directories

To harvest log files for products running on different servers, you must specify multiple filter criteria.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, click **New**.
4. On the Create New Profile page, enter the appropriate information in the **Profile Name** and **Profile Description** fields.
5. Select the host name of the server, product, and directories or files from the respective fields.
   - To select multiple directories or files from the respective list boxes, press `CTRL` and click the directories or files.
   - To clear a selection, press `CTRL` and click the item.
   - To add another log harvesting request for a different product or for another instance of the same product running on the same server or on a different server, click plus (**+**).
6. If you select one or more directories, in the **File Name Filter** field, enter a text pattern as the filter criteria.

During the harvesting operation, the system harvests only those files that match the filter criteria.

7. To save the profile and the log harvesting requests in the profile, click **Save Profile**.

Related links

Create New Profile field descriptions on page 930

Editing a log harvesting profile

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **Edit**.
4. On the Harvest Criteria Edit page, modify the information in the **Profile Name** and **Profile Description** fields.
5. Modify the hostname of the server, product, and directories or files from the respective fields.
    - To select multiple directories or files from the respective list boxes, press `CTRL` and click the directories or files.
    - To clear a selection, press the `CTRL` and click the item you select.
    - To add another log harvesting request for another product or for another instance of the same product running on the same server or on a different server, click **+**.
6. If you select one or more directories, you can enter a new filter criteria in the text box below the **Directories / Filter Text** field and click **Commit**.

    During the harvesting operation, the system harvests only those files that match the filter text.
7. Click **Save Profile** to save the changes you made to the log harvesting profile.

Related links

Harvest Criteria Edit field descriptions on page 931

Viewing the harvested log files in an archive

You can view the harvested log files of a product stored in an archive file.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. Click **Show files**.

On the Search Archives page, navigate through the folders in the archive to view the harvested log files.

Deleting a profile

About this task

You cannot 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.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **Delete**.
4. On the Profile Delete Confirmation page, click **Delete**.

   Note:

   When you delete a profile, the system deletes all requests and all archives related to the profile from the file system.

Submitting a request for harvesting log files

About this task

Use this feature to submit a log harvesting request to one or more products running on the same or different servers. 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 **Request**, the system generates a single request for all the requests contained in the profile.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. 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.
5. 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 links

Harvest Archives field descriptions on page 933

Viewing details of a log harvesting request

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. If the system does not display any requests, submit a new request.
6. Click **View**.

   The Harvest - View Harvest detail page displays the details of the selected request.

Related links

Harvest - View Harvest detail field descriptions on page 935

Searching for text in a log file

Use this feature to search for matching text in the log file of a product.

About this task

The search is based on Lucene Search. The search results are highlighted as per the Lucene highlighter. The highlight package contains classes to provide keyword in context features, typically used for highlighting search terms on the results page.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. Click **Show Files**.
6. On the Search Archives page, in the **Enter search text** field, enter the text for which you want to search.
7. In the Tree view, navigate to the log file by expanding the folders and select the log file.
8. Click **Search**.

   The system displays the search results in the Search Result Panel. The **Search Results Panel** field displays the line numbers as hyperlinks on which the searched text is found.
9. Click the hyperlink in the **Search Results Panel** field.

   The system displays the page that contains the highlighted searched text in the **Log Browser Panel** field.

Related links

Search Archives field descriptions on page 934

Viewing the contents of harvested log files

About this task

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.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. If the system does not display any requests, submit a new request.
6. Click **Show Files**.

   The system lists the log files that are harvested.
7. Select the log file and click **View**.

   The system displays the file content in the Log Browser Panel pane.

Related links

Search Archives field descriptions on page 934

Downloading the harvested log files

About this task

You can download the harvested log files of one or more products that you stored in a zip file on your local server.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. If the system does not display any requests, submit a new request.
6. Click **Show Files**.

7. On the Search Archives page, select a product name, host name of the server on which one or more products are running, or a directory.
    - If you select a product name, the system creates a zip file that contains the harvested log files for the selected product instances running on the same server or on different servers.
    - If you select a host name of a server under a product, the system creates a zip file that contains the harvested log files for the products running on the server that you selected.
    - If you select a directory, the system creates a zip file containing the harvested log files under the selected directory.
8. Click **Download**.

    The system prompts you to save the file on your local server.
9. Click **Save**.

Related links

Search Archives field descriptions on page 934

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.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, click **Filter: Enable**.

    You can find this button at the top right of the table containing log harvesting profiles.
4. Enter or select the filter criteria.

    You can filter the log harvesting profiles by the name, description and creator of the profiles.
5. Click **Filter: Apply**.

    Note:

    If no records matching the filter criteria are found, the Log Harvester page displays a message that no records matching the search criteria are found.

    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.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and 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`.
   - The zip file name that stores the harvested files.
   - The description of the log harvesting request.
   - The location of the archived file that stores the harvested files.
   - The status of the log harvesting request.
   - The 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.

   The table containing log harvesting requests displays only those log harvesting requests that match the specified filter criteria.

Viewing details of a log harvesting profile

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **View**.

   The Profile Criteria View page contains the details of the log harvesting profile you selected.

Related links

Profile Criteria View field descriptions on page 932

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
Profile Name	The name of the log harvesting profile.
Description	A brief description of the profile.
Created By	The name of the creator of the profile.
Created Time Stamp	The date and time when the profile was created.

Button	Description
View	Opens the Harvest Archives page. You can use this page to view the details of a selected log harvest profile.
New	Opens the Create New Profile page. You can use this page to create a new log harvesting profile.
Edit	Opens the Edit Profile page. You can use this page to edit a log harvesting profile.
Delete	Deletes the selected profile. You can not delete a profile if the profile is in use by the Log Harvester service.
Requests	Opens the Harvest Archives page. You can use this page to run the log harvesting requests in a selected profile.
Filter: Disable	Hides the fields displayed under the columns on which you can apply the filters without resetting the filter criteria. This is a toggle button.
Filter: Enable	The 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.
Filter: Apply	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. The files can reside on one or more servers.

Name	Description
Profile Name	The name of the log harvesting profile.
Profile Description	A brief description of the profile. This is an optional field.

Table continues…

Name	Description
Host Name	The host name of the servers on which products are installed. If you do not see the host name of CS 1000 when you create the profile, at the command prompt of CS 1000, run the following command: `cd /opt/nortel/oam-logging ./configureSpiritAgentClient.sh <enrollment password>`
Product	The products for which you can harvest logs.
Directories / Filter Text	A list of directories that contains the log files for the selected product.
Files	The log files that you can harvest for the selected product.
Filter Text	The text based on which the log files present under a selected directory are filtered for harvesting. If you select the directory `/a/b/c` and enter `com` in this field, the harvest operation for this profile harvests the log files that are in the directory `/a/b/c`. The log files contain com in the file name. The field does not support wild cards.

Button	Description
+	Specifies another log harvesting request for a product.
-	Deletes the log harvesting request for the product.
Commit	Commits the filter criteria for the selected directories.
Save Profile	Saves the new profile and settings for log harvesting requests in the database.

Harvest Criteria Edit field descriptions

Use this page to edit an existing log harvesting profile.

Name	Description
Profile Name	Displays the name of the log harvesting profile
Profile Description	Displays a brief description of the profile.
Host Name	Displays the hostname of the servers on which you installed the products.
Product	Displays the products for which you can harvest logs.
Directories / Filter Text	Lists the directories that contains the log files for the selected product.

Table continues…

Name	Description
Files	Displays the log files that you can harvest for the selected product
Filter Text	Displays the text based on which the log files present under a selected directory gets filtered for harvesting. If you select the directory `/a/b/c` and enter `com` in the **Filter Text** field, the harvest operation for this profile harvests the log files that contain *com* in the file name. The field does not support wildcards.

Button	Description
+	Allows you to specify another log harvesting request for a product.
-	Deletes the log harvesting request for the product.
Commit	Commits the filter criteria for the selected directories.
Save Profile	Saves the new profile and settings for log harvesting requests in the database.
Cancel	Ignores the changes you make to the Harvest Criteria Edit page and takes you back to the Log Harvester page.

Profile Criteria View field descriptions

Use this page to view the details of a selected log harvest profile.

Name	Description
Profile Name	Displays the name of the log harvesting profile.
Profile Description	A brief description of the profile.
Product	Displays the name of the product for which logs are harvested.
Hosts	Displays the hostname of the server on which the product resides.
Files	Displays the names of the log files for which you can harvest log messages.
Directory	Displays the directory that contains the log files.
Filter Text	The text based on which the log files present under a selected directory are filtered for harvesting. For example, if you select the directory `/a/b/c` and enter the text `com` in this field, the harvest operation for this profile harvests the log files that contain *com* in the file name. This field does not support wild characters.

Button	Description
Done	Closes this page and takes you back to the Harvest Profile List page.
Refresh	Refreshes the records in the table.

Harvest Archives field descriptions

Use this page to create an archive for the log harvesting request. The archive created for a successful harvesting request contains the requested log files in a zip file.

Name	Description
Archive Name	The name of the archive file that you want to create for storing the harvested log files.
Archive Description	A brief description of the archive. This field is optional.

Name	Description
Request Id	The unique identification number assigned to a log harvesting request.
Archive Name	The name of the archive file that you create for storing the harvested log files.
Request Time Stamp	The date and time when the log harvesting request is submitted.
Request Description	A brief description of the log harvesting request.
Status	The status of the log harvesting request. The options are: • SUCCESS: The status is SUCCESS if System Manager successfully harvests the log messages. • FAILURE: The status is FAILURE if System Manager failed to harvest the log messages for the product. • PARTIAL SUCCESS: The status is PARTIAL SUCCESS if System Manager partially harvests the log messages.
Status Time Stamp	The date and time when the execution status of the log harvesting request is generated.
Status Description	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.
Location	The location where the harvested log messages are archived.

Button	Description
Run Profile	Runs the log harvesting requests for the selected profile.
View	Opens the View Harvest detail page. You can use this page to view the details of a selected log harvesting request.
Show Files	Opens the Search Archives page. You can use this page to search for text contained in the harvested log files, download log files of one or more products running on a same or different servers, view the contents of a log file.
Filter: Disable	Hides the fields displayed under the column filter fields without resetting the filter criteria. A toggle button.
Filter: Enable	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.
Filter: Apply	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 the harvested log files.
- Search a text in the harvested log files.
- Download the harvested log files on your local server.

Name	Description
Enter search text	The text that you want search for in the harvested log files.
List box	Displays the hierarchy of the harvested log files in an archive. The files are organized in a tree view.
Log Browser Panel	Displays the contents of the selected log files.
Search Results Panel	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 **Log Browser Panel** field.

Button	Description
Previous	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.
Next	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.
Search	Searches for the occurrences of the text specified in the **Enter search text** field in the selected log files.
View	Displays the contents of the selected log files in the **Log Browser Panel** field.
Download	Downloads the selected log files present in the archive to your local server.

Harvest - View Harvest detail field descriptions

Use this page to view the details of a selected log harvest request.

View Parent

Name	Description
Request Id	Displays the unique identification number assigned to a log harvesting request.
Archive Name	Displays the name of the archive file that stores the harvested log files containing the log messages.
Status	Displays the status of log harvesting requests. The options are: • SUCCESS: The status is SUCCESS if System Manager successfully harvests the log messages. • FAILURE: The status is FAILURE if System Manager fails to harvest the log messages for the product.
Request Description	A brief description of the log harvesting request.

Child Request Details

Name	Description
Product	Displays the unique identification number assigned to a log harvesting request.
Status	Displays the status of the log harvesting request. The options are: • **SUCCESS**: The status is SUCCESS if System Manager successfully harvests the log messages.

Table continues…

Name	Description
	• **FAILURE**: The status is FAILURE if System Manager fails to harvest the log messages for the product.
Host Name	Displays the hostname of the server on which the product resides.
Status Description	A brief description about the execution status of the request.
Status Time Stamp	Displays the date and time when the system generates the status of the log harvesting request.

Button	Description
Done	Closes this page and takes you back to the Harvest Archives page.
Refresh	Refreshes the records in the table.
Filter: Enable	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. A toggle button.
Filter: Apply	Filters the log harvesting requests based on the filter criteria.
Filter: Disable	Hides the fields displayed under the columns on which you can apply the filters without resetting the filter criteria. A toggle button.

Managing log settings

Log Settings

Log Settings displays the loggers and appenders for any log configuration file that you select. You can also modify the logger and appender settings through this menu. The Logger List displays the name and level of the log along with the appender details.

Accessing the Log Settings service

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.

Result

The system displays the **Log Settings** page.

Viewing loggers for a log file

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.

Related links

Logging Settings field descriptions on page 937

Logging Settings field descriptions

Use this page to view and edit loggers defined in a log file.

Log Settings

Name	Description
Select Log File	The field lists the log files that you can configure.

Logger List

Name	Description
Logger	The loggers in the selected log files.
Log level	The log level indicating the level of logging set for the corresponding logger.
Attached Appenders > Name	The name of the appender.
Attached Appenders > File Path	The path of the file to which the appender logs the information.
Attached Appenders >Facility	The process running on the machine that created the log message.
Attached Appenders > host	The name of the syslog host where the log output is stored.
Show All	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 links

Viewing loggers for a log file on page 937

Editing a logger in a log file

About this task

You can set log levels for loggers which defines the level of logging the logger logs.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.
4. In the **Logger List** section, select a logger and click **Edit**.
5. On the Edit logger page, in the **Log Level** field select a log level.
6. To view the logs for successful events, in the **Log Level** of the specified log, click **Info**.

   For example, as a user of System Manager Communication Manager capabilities, if you set the **Log Level** to **Info** in `com.avaya.iptcm.eps.logging.audit` and `com.avaya.iptcm.eps.logging.operation`, the system captures the successful events in the audit log and the operational log present at `/var/log/Avaya/mgmt/iptcm/audit.log` and `/var/log/Avaya/mgmt/iptcm/operation.log` respectively.

   Note:

   If you perform an application upgrade, the system does not retain the modified log level configuration. After an application upgrade, you must configure the log level settings again to view the logs for successful events.

7. Click **Commit**.

   The log level is set for the selected logger.

Related links

Edit Logger field descriptions on page 939

Assigning an appender to a logger

About this task

The appender where a logger logs the log messages.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.
4. In the **Logger List** section, select a logger and click **Edit**.
5. On the Edit logger page, click **Attach** in the Attached Appenders section.
6. On the Attach Appender page, select 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 links

[Attach Appender field descriptions](#) on page 941

Modifying an appender

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.
4. In the **Logger List** section, select a logger and click **Edit**.
5. On the Edit logger page, select an appender in the **Attached Appenders** section.
6. Click **Edit**.
7. On the Edit Appender page, modify the appender information.

   You can modify information in the **Threshold Log Level**, **Max File Size**, **File Path**, and **Number Of Backup Files** fields
8. Click **Commit**.

Related links

[Edit Appender field descriptions](#) on page 940

Removing an appender from a logger

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.
4. In the **Logger List** section, select a logger and click **Edit**.
5. On the Edit logger page, select an appender in the **Attached Appenders** 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
Logger	The name of the logger.
Log level	The level of logging for which the logger logs the information.

Attached Appender

Name	Description
Appender	The name of the appender.
Threshold Log Level	The threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level.
File Path	The path of the file where the appender logs the information.
Max File Size	The maximum size in KB, MB, and GB reserved for the appender file.
# Backup Files	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.
Facility	The process running on the machine for which log messages are created.
Host	The name of the syslog host that stores the log output.
Header	The header part of the syslog packet. The header part contains timestamp and host name information.
Facility Printing	The printed message includes the facility name of the application.

Button	Description
Edit	Opens the Edit Appender page. Use this page to modify the appender information.
Attach	Opens the Attach Appender page. Use this page to add an appender to the logger.
Detach	Removes the selected appender from the logger.
Commit	Saves the changes in the logger information to the database.
Cancel	Closes the Edit Logger page and takes you back to the Logging Configuration page.

Edit Appender field descriptions

Use this page to edit the information of an appender.

Name	Description
Logger	The name of the logger.

Table continues…

Name	Description
	Note: You can only view this information.
Appender	The name of the appender. **Note:** You can only view this information.
Threshold Log Level	The threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level .
File Path	The path of the file where the appender logs the information.
Max File Size	The maximum KB, MB, and GB reserved for the appender file.
# Backup Files	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
Commit	Saves the changes to the database.
Cancel	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
Logger	The name of the logger.
Log Level	The level of logging for which the logger logs the information.
Select Appender	The list of appenders that you can assign to the logger.

Button	Description
Commit	Assigns the appender to the logger.
Cancel	Closes the **Attach Appender** page and takes you back to the Edit Logger page.

Managing log viewer

Log Viewer

Log Viewer displays all the logs generated by System Manager and the applications. The Log List displays a list of all the logs. You can view the details of each log, perform a search for logs, and filter specific logs. Log details include 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.

Viewing log details

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
3. On the Logging page, select a log.
4. Click **View**.

Exporting logs

You can export logs 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 Microsoft Excel.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
3. On the Logging page, perform one of the following actions:
   - To export a log to a CSV file, select a log from the list and click **More Actions** > **Export Selected**.
   - To export the filtered logs to a CSV file, click **More Actions** > **Export All**.

     When you use **Advanced Search** or **Filter** option to filter logs based on a specific criteria, **Export All** exports all the filtered data
4. Click **Save** to save the exported log file to the local disk.

Filtering logs

You can filter and view logs that meet the specified filter criteria. To apply the filters, you need 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.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
3. On the Logging page, click **Filter: Enable** at the top right corner of the log table.
4. Enter or select the filter criteria.
5. Click **Filter: Apply**.

   The page displays the logs that match the specified filter criteria.

   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.

Searching for logs

You can specify conditions for finding logs. The system displays logs that satisfy the search conditions. You can specify multiple search conditions.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
3. On the Logging page, click **Advanced Search**.
4. In the **Criteria** section, from the first and second drop-down fields, select the search criterion and the operator.
5. Select or enter the search value in the third field.
6. 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.
7. 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.
8. 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.
9. Click **Search** to find the logs for the given search conditions.

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
Select check box	The option to select a log.
Log ID	The unique identification number that identifies the log.
Time Stamp	The date and time of the log generation.
Host Name	The name of the system from which the log is generated.
Product Type	The code that uniquely identifies the component which generated the log. For example, product, device, application, and service. An example of the log product type is GW600, which is a product type code identifier.
Severity	The severity level of the log. The following are the type of severities: • **Emergency**: System is unusable. • **Alert**: Action must be taken immediately. • **Critical**: Critical conditions. • **Error**: Error conditions. • **Warning**: Warning conditions. • **Notice**: Normal but significant condition. • **Informational**: Informational messages. • **Debug**: Debug-level messages. ✱ **Note:** The colors of severities do not indicate logging severities
Event ID	The unique identification number assigned to the event that generated the log.
Message	A 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.
Process Name	The process on the device that has generated the message, usually the process name and process ID.
Facility	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

Table continues…

Name	Description
	of the message. The following are the types of supported facilities: • User-Level Messages • Security/authorization • Log Audit

Button	Description
View	Opens the Log - View Log Detail page. Use this page to view the details of the selected log.
Auto-Refresh Mode	Switches to the Auto-Refresh mode. When the Logging page is set in this mode, it automatically updates the logs in the table. A toggle button.
More Actions > **Export Selected**	Exports the selected logs to a CSV file. You can view the logs using the Wordpad or Excel application.
More Actions > **Export All**	Exports all the logs to a CSV file. You can view the logs using the Wordpad or Excel application. **Note:** When you use **Advanced Search** or **Filter** option to filter logs based on some criteria, **Export All** exports all the filtered data.
Advanced Search	The fields that you can use to specify the search criteria for searching a log.
Refresh	Refreshes the log information in the table.
Filter: Enable	The fields under select columns that you can use to set filter criteria. A toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. A toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters logs based on the filter criteria.
Select: All	Selects all the logs in the table.
Select: None	Clears the selections.
Previous	The logs in the previous page. This button is not available if you are on the first page.
Next	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 top right corner.

Name	Description
Criteria	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 list. Enter the search value in the text field. Select following search criteria from the first drop-down list: • Log ID: The unique identification number assigned to the log. • Host Name: Name of the system for which log is generated. • Product type: A code which uniquely identifies the component which generated the log. For example, product, device, application, service, and so on. • Severity: Severity level of the log. • Message: Brief description about the log. • Event ID: Unique identification number assigned to the event. • Process Name: Process on the device that has generated the message • Time Stamp: Date and time of the log generation. • 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. The second drop-down list 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 list. The following are the list of operators: • Equals • Not Equals • Starts With • Ends With • Contains The operators for Time Stamp are: =, >, <, >=, <=, and !=. When you select Time Stamp from the first drop-down list, the page provides date and time fields for entering the date and time in the respective fields.

Name	Description
	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 formats: • 24Hr • AM • PM

Button	Description
Clear	Clears the search criterion and sets the criterion to the default search criteria.
Search	Searches the logs based on the search conditions.
Close/Advanced Search	Hides the search fields.
+	Adds a search condition.
-	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
Log ID	The unique identification number that identifies the log.
Time Stamp	The date and time of the log generation.
Host Name	The name of the system from which the log is generated.
Product Type	The 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.
Severity	The severity level of the log. The following are the type of severities: • **Emergency**: System is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant condition • **Informational**: Informational messages

Table continues…

Name	Description
	• **Debug**: Debug-level messages **Note:** The colors of severities do not indicate logging severities.
Event ID	The unique identification number assigned to the event that has generated the log.
Message	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.
Process Name	The process on the device that has generated the message. This is usually the process name and process ID.
Facility	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: • User-Level Messages • Security/authorization • Log Audit

Button	Description
Logging Landing Page	Switches the mode from Auto-Refresh to manual refresh and displays the Logging Home page. This is a toggle button.

TrapListener service

The TrapListener service receives traps and informs that come from different applications and displays on the System Manager Alarming page.

- TrapListener receives V2c and V3 traps and informs that are defined in the common alarm definition file.
- TrapListener processes the Common Alarm Definition file for applications where all trap definitions are present.

You can configure the TrapListener service from **Services** > **Configurations** on the System Manager web console. For information on configuring the TrapListener service, see Configuring the TrapListener service.

If you change the Trap Listener settings as an administrator, you must create a new SNMP target profile for the System Manager IP address and a new SNMPv3 user profile for System Manager. The values in the new profiles must match the values in the Trap Listener settings. Also, attach the System Manager SNMPv3 user profile to the System Manager target profile, and then attach the new SNMP target profile to all serviceability agents. For information on creating SNMP user profiles and target profiles and attaching the target profiles to serviceability agents, see Managing Serviceability Agents in *Administering Avaya Aura® System Manager*.

Related links

Configuring the TrapListener service on page 824

TrapListener service field descriptions on page 824

Serviceability Agents on page 881

Chapter 17: Managing licenses

WebLM overview

Avaya provides a Web-based License Manager (WebLM) to manage licenses of one or more Avaya software products for your organization. WebLM is a Web-based license manager that 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) Web site at https://plds.avaya.com.

The license file of a software product is in an XML format. The license file contains information regarding the product, the major release, the licensed features of the product, and the licensed capacities of each feature that you purchase. After you purchase a licensed Avaya software product, you must activate the license file for the product in PLDS and install the license file on the WebLM server.

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 is displayed on the Server Properties page of the WebLM server.

Obtaining the license file

About this task

For each licensed Avaya product that you are managing from the WebLM server, you can obtain a license file from PLDS, and install it on the corresponding WebLM server. For additional information on using PLDS, see *Getting Started with Avaya PLDS - Avaya Partners and Customers* at https://plds.avaya.com.

In Geographic Redundancy, you must generate the license file by using the host ID of primary System Manager.

⚠ **Caution:**

> Do not modify the license file that you receive from Avaya. WebLM does not accept a modified license file.

You require the host ID of the WebLM server to obtain the license file from PLDS. For client node locking, while generating the license file, you must provide the WebLM server host ID and client host ID.

Procedure

1. Log on to the System Manager web console.
2. On the System Manager Web Console, click **Services** > **Licenses**.
3. In the left navigation pane, click **Server properties**.
4. Note the **Primary Host ID**.
5. Using the host ID, generate the license from PLDS.

Related links

Install license field descriptions on page 955

Accessing WebLM

Before you begin

You require permissions to access the WebLM application.

Procedure

1. Log on to the System Manager web console.
2. On the System Manager Web Console, click **Services** > **Licenses**.

Installing a license file

About this task

You can install a license file on the WebLM server. To reinstall a license file on a WebLM server on which the license file that Remote Feature Activation (RFA) generated is installed, remove the license file that RFA generated from the WebLM server before you install the new license file. Use the Uninstall functionality to remove the license file from the WebLM server.

Before you begin

- Get the license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.
- Log on to the WebLM server.

If you experience problems while installing the license file, see “License file installation errors” in *Administering standalone Avaya WebLM*.

Procedure

1. In the left navigation pane, click **Install license**.
2. On the Install license page, enter the license file path or click **Browse**, and select the license file.

3. Read the terms and conditions, and click **Accept the License Terms & Conditions**.
4. Click **Install**.

   WebLM displays a message on successful installation of the license file. The installation of the license file might fail for reasons, such as:

   - The digital signature on the license file is invalid. If you get such an error, request PLDS to redeliver the license file.
   - The current capacity use exceeds the capacity in the installed license.

Related links

Install license field descriptions on page 955

Client node locking

WebLM supports client node locking of licenses where licenses are tied to specific application instances. You cannot move licenses across application instances. The feature is provided to support some Avaya data products that require licenses to be node-locked to an application instance or the client. For example, VPFM/COM. To use this feature, you must include the host IDs of the application instance and the WebLM server in the license file.

With the client node-locking feature:

- WebLM allows multiple licenses for a client node-locked product to be installed on the server at the same time. Each client node-locked license contains a unique host ID of the client.
- When a client node-locked license is installed on WebLM, WebLM automatically associates the license file with the client or application host ID that is included in the license file.
- The license request from the element would include the client/element host ID. WebLM serves licenses only if the client host ID in the request matches with any of the installed client node locked license files.
- WebLM enforces mutual TLS authentication for client node-locked licenses.
- The license over-install checks are based on the client host ID. While over-installing a license file with a new file for a client instance whose client host ID changed due to rehost, license file includes the old and new client host IDs. In this case, over-install check will be based on the old client host ID.

Viewing the license capacity and utilization of the product features

Before you begin

- Log on to the WebLM server.
- Install the license file on the WebLM server for the licensed product.

About this task

Use this procedure to view the license capacity and license utilization of a product for which you installed a license file.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **View license capacity**.
    - If centralized licensing is disabled, the system displays the license capacity and the actual license usage of the product.
    - If centralized licensing is enabled, the system displays the **Installed License Files** table. Click the **Host ID - Centralized Licensing ID** hyperlink to view the license capacity of the license file for the selected host ID. If the license file is assigned to an element then the system displays the element display name, element ID, license owner, license host, and license file host IDs for the element.

Related links

View license capacity field descriptions on page 955

Viewing peak usage for a licensed product

Before you begin

- Log on to the WebLM server.
- Install the license file on the WebLM server for the licensed product.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **View peak usage**.
    - If centralized licensing is disabled, the system displays the peak usage of the licensed features of the product.
    - If centralized licensing is enabled, the system displays the **Installed License Files** table. Click the **Host ID** hyperlink to view the peak usage of the license file for the selected host ID. If the license file is assigned to an element then the system displays the element display name and element ID for the element.

Related links

View peak usage field descriptions on page 956

Uninstalling a license file

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. In the left navigation pane, click **Uninstall license**.
3. On the Uninstall License page, select the license file that you want to uninstall.
4. Click **Uninstall**.
5. On the Uninstall License Confirmation page, click **Uninstall**.

   If the license file you selected cannot be uninstalled, the system displays only the **Cancel** button.

Related links

Uninstall license field descriptions on page 962

Viewing the server properties

Before you begin

Log on to the WebLM server.

Procedure

In the left navigation pane, click **Server properties**.

Note:

The host ID specified in PLDS is embedded in the license file. You can install the license file only if the host ID of the server that hosts WebLM matches the host ID in the license file. Therefore, when you request for a license file, specify the correct host ID of the server that hosts WebLM .

Related links

Server Properties field descriptions on page 963

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
Product Name	The name of the product for which the license file is installed.
Product Version	The version of the product for which the license file is installed.
Type of License	The type of license file installed for the product.
Date of Installation	Date and time of installation of license file.

Install license field descriptions

Name	Description
Enter license path	The complete path where the license file is saved.
Browse	The option to browse and select the license file.
Avaya Global License Terms & Conditions	Avaya license terms and conditions that the user must agree to continue the license file installation.

Button	Description
Install	Installs the product license file.

View license capacity field descriptions

Licensed Features

Use the View license capacity page to view the total number of feature licenses in the license file and the current usage of those licenses.

Field	Description
Feature (License Keyword)	The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.
Expiration Date	The date on which the feature license expires.

Table continues…

Field	Description
Licensed capacity	The number of licenses for each licensed feature. The system fetches the number of feature licenses information from the license file.
Currently Used	The number of feature licenses that are currently in use by the licensed application. For features of type Uncounted, the column displays *Not counted*.

Acquired Licenses

The Acquired licenses table displays information about the licenses acquired by the licensed application. You can view the information in the table only if the licensed product has acquired feature licenses.

Field	Description
Feature	The feature keyword for each licensed feature that is currently acquired by a licensed application.
Acquired by	The name of the licensed application that has acquired the license.
Count	The number of feature licenses that are currently acquired by the licensed application.

View peak usage field descriptions

Use this page to view the usage information of feature licenses of a licensed application at different time intervals.

Field	Description
Feature (License Keyword)	The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.
Currently Allocated	The number of feature licenses purchased by the organization.
Usage: qty/%	The number of feature licenses for each licensed feature that a licensed application currently uses. The column also displays the percentage of usage. For example, if 50 feature licenses are available and five feature licenses are used by applications, the column displays 5/10%.
Peak Usage (Last 7 days): qty/%	The highest number of feature licenses for each licensed feature that has been used in the last seven days.

Table continues…

Field	Description
	For example, if the peak usage for a feature license in the past seven days was 25, and the number of available licenses during these seven days was 50, then the column displays 25/50%.
Peak Usage (Last 30 days): qty/%	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 was 50, and the number of available licenses during these 30 days was 50, then the column displays 50/100%.
Time of Query	The date and time when the last usage query for WebLM was executed.
Status	The success or failure of the last usage query executed for the WebLM server.

Centralized licensing

About centralized licensing

Some Avaya products do not share licenses from a single license file as each element instance requires a separate license file. You require a dedicated WebLM server to host the relevant license file of the associated element instance. In this licensing model, you require the same number of WebLM servers as the number of products that you install and configure. In the virtualized environment, this model requires additional virtual machines for each element instance, thus increasing the VMware licensing cost. Thus, you cannot centrally manage the licenses for a product and must log in to each WebLM server and manage licenses for each element instance.

WebLM now supports centralized management of products that cannot share a license file across element instances. You can install multiple license files for a product on a single WebLM server and associate specific license files to specific element instances.

After you enable centralized licensing from the WebLM interface, you can install multiple license files for the same product. You can add multiple element instances, and associate each license file to an element instance. The WebLM server provides licenses to the element instances based on the association you define.

Note:

For Communication Manager, centralized licensing is supported from Communication Manager Release 6.3.4 and later.

Enabling centralized licensing

Before you begin

Install a Communication Manager license file that supports centralized licensing. Centralized licenses contain the FEAT_WLM_CENTRALIZED feature in the Communication Manager license file.

About this task

By default, centralized licensing is disabled for Communication Manager. You must enable centralized licensing to use this feature.

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. In the left navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. Click **Enable Centralized Licensing**.

   ⚠ **Warning:**

   After enabling the Centralized Licensing feature for Communication Manager, you must link the license file to the associated Communication Manager server instance. If you do not link the license file to a Communication Manager server instance, the Communication Manager server instance cannot acquire the license file from the WebLM server.

Configure centralized licensing field descriptions

Elements and License File Assignments

Name	Description
Element Display Name	The display name that you enter for the Communication Manager main server.
Element ID	The element identifier for the Communication Manager server is the IP address of the main server. The element ID must match the name used by the Communication Manager server to acquire licenses from WebLM.
Host ID - Centralized Licensing ID	The host ID of the license file. The first 12 characters are the WebLM server host ID, and the last 5 characters are the centralized licensing ID. The centralized licensing ID is a unique number across multiple license files for the same product.
License Host Name	The host name of the license as defined in the license file.

Table continues…

Name	Description
Date of Installation	The date of installation of the license file.

Installed License Files

Name	Description
Host ID - Centralized Licensing ID	The host ID of the license file. The first 12 characters are the WebLM server host ID, and the last 5 characters are the centralized licensing ID. The centralized licensing ID is a unique number across multiple license files for the same product.
License Host Name	The host name of the license as defined in the license file.
Assigned To Element	The field that indicates whether a license file is associated with the Communication Manager server. The possible values are: • **Yes**: The license file is associated with a Communication Manager server. • **No**: The license file is not associated with a Communication Manager server.
Date of Installation	The date of installation of the license files.

Button	Description
New	Adds a Communication Manager server instance and the mapping of an element to a license file.
Edit	Edits the properties of a Communication Manager server instance.
Delete	Deletes a Communication Manager server instance.

Adding an element instance and assigning the element instance to a license file

Before you begin

Enable the Centralized Licensing feature.

Install the license files that you want to assign to an element instance.

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. In the left navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. In the Elements and License File Assignments section, click **New**.

   The system displays the Add License Mapping page.

4. In the **Element Display Name** field, enter the display name of the instance.
5. In the **Element IP Address** field, enter the element IP address of the instance.

   The element ID is a unique ID. For Communication Manager, enter the IP address of the Communication Manager server.
6. In the **Select License File** table, select the license file that you want to assign to the element instance.

   Note:

   In a duplex pair, add each of the Communication Manager server as a separate element and assign the same license file to both the servers.

   Warning:

   You must assign a Communication Manager license file to only one Communication Manager main server (simplex or duplex pair). If you will assign the same license file to multiple Communication Manager servers (other than the duplex pairs), Communication Manager will enter in License Error Mode with the 30-day grace period.
7. Click **Save**.

Related links

Element instance field descriptions on page 961

Editing an element instance and license file assignment

Before you begin

- Enable the centralized licensing feature.
- Install the license file that you want to assign to the element instance.
- Add an element instance.

About this task

Use this procedure to edit the properties of an element instance.

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. In the left navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. On the Configure Centralized Licensing page, select the element instance.
4. Click **Edit**.
5. On the Edit Element Instance page, modify the display name and element IP address of the element instance.
6. In the **Select License File** table, you can select a new license file for the element instance.
7. Click **Save**.

Related links

[Element instance field descriptions](#) on page 961

Deleting an element instance

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. In the left navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. On the Configure Centralized Licensing page, select the element instance that you want to delete.
4. Click **Delete**.

   The system displays the Delete Element Confirmation page.
5. Click **Delete**.

   The system deletes the element instance and its assignment with the license file.

Element instance field descriptions

Name	Description
Element Display Name	The display name that you enter for the element instance.
Element IP Address	The element identifier for the Communication Manager server is the IP address of the main server. The element ID must match the name used by an element instance to acquire licenses from WebLM.

Select License File

Name	Description
Host ID - Centralized Licensing ID	The host ID of the license file. The first 12 characters are the WebLM server host ID, and the last 5 characters are the centralized licensing ID. The centralized licensing ID is a unique number across multiple license files for the same product. For centralized licensing scenarios with just one license file, the host ID has 12 characters. Click the **Host ID** hyperlink to view the license capacity of the license file having the host ID.
License Host Name	The host name of the license as defined in the license file.

Table continues…

Name	Description
Assigned To Element	The field that indicates whether a license file is associated with an element instance. The possible values are: • **Yes**: The license file is associated with an element instance. • **No**: The license file is not associated with an element instance.
Date of Installation	The date of installation of the license file.

Button	Description
Save	Adds or edits the element instance.
Cancel	Cancels the add or delete element instance operation.

Disabling centralized licensing

Before you begin

Ensure that:

- You have not added an element instance for the product. If you have added the element instances, delete the element instances.
- You have installed only a single license file for the product. If you have installed multiple license files, uninstall all the files except any one license file.

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. In the left navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. Click **Disable Centralized Licensing**.

Uninstall license field descriptions

Use this page to remove a license file from the WebLM server for a licensed product. The **Allocation Table License Files** table displays the ALF files. You cannot uninstall the ALF files.

Field	Description
License Host Name	The WebLM server where the license files are installed.
Host ID	The host ID of the license file.

Table continues…

Field	Description
Products	The products for which licenses are installed on the WebLM server.
SID	The System ID of the license file.
Select Check box	Use to select the license files that you require to remove from the WebLM server. You cannot uninstall the ALF license files.

Button	Description
Uninstall	Removes the selected license files from the WebLM server.

Server Properties field descriptions

Use this page to view the MAC address of the server.

Server Host ID

Field	Description
Primary Host ID	The MAC address of the server. For non-VMware deployments, the primary host ID is the MAC address of the server. For VMWare deployments, the primary host ID is a 12 character combination of the IP address and the UUID of the system. You must use the host ID to generate licenses which you later install on the current instance of the WebLM server.

Enterprise licensing

Configuring enterprise licensing

Before you begin

- Log on to WebLM Home.
- Install the enterprise license file on the WebLM server for the product.

To verify the license file for a product, in the left navigation pane, click **Licensed products** and select the product. The content pane displays the product name, System Identification number (SID), and the license file type installed for the product at the top of the page.

✱ **Note:**

System Manager WebLM is always configured as the master WebLM server. You cannot configure System Manager WebLM as local WebLM to an external WebLM.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. In the left navigation pane, click **Enterprise configuration**.
3. On the Enterprise Configuration page, enter the appropriate information in the fields.

   For more information, see Enterprise Usage field descriptions.

   To successfully set up and configure the master WebLM server, enter valid information in the mandatory fields that are marked with a red asterisk.
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 name of the SMTP server.
7. In the **E-mail notification settings for periodic operation** section, perform the following:
   a. Set the **E-mail notification** to `On`.
   b. In the **E-mail address** field, enter an email address.
   c. To add the email address to the list of recipients for the WebLM server to send email notifications, click **Add To List**.
8. In the **Default Periodic License Allocation Schedule** section, select the day and time for periodic license allocations.

   The values you enter in this section remain as 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 the query for periodic usage.

   The values you enter in this section remain as the default setting for periodic usage for all local WebLM servers in the enterprise.

   ✱ **Note:**

   For any periodic operations, you must perform the manual allocation at least one time.
10. Click **Submit**.

    The system validates the information. The system displays the host ID in the **Host ID** field. The host ID is the host ID of the computer where you installed the WebLM server.

Related links

Enterprise Configuration field descriptions on page 972

Enterprise Usage field descriptions on page 980

Adding a local WebLM server

Before you begin

- Log on to the WebLM server.
- Install the enterprise license file.
- Identify the WebLM servers that you must add as the local WebLM server.
- Configure the security certificate before you add a local WebLM server.
- On the Add Trusted Certificate page, select **Import using TLS** , and enter the appropriate information in the **IP Address** and the **Port** fields of the local WebLM server.

  For more information, see Adding a Trusted Certificate in the Avaya Aura® System Manager help.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Local WebLM Configuration** > **Add local WebLM**.
3. On the Local WebLM Configuration: Add local WebLM page, enter the appropriate information.

   To successfully set up and configure the local WebLM server, fields that are marked with a red asterisk (*) are mandatory.

   For detailed descriptions of the fields, see Add local WebLM field descriptions on page 975.
4. In the **Local WebLM Configuration** section, enter the name, description, IP address, and port of the local WebLM server.
5. Select a protocol for the master WebLM server to communicate with the local WebLM server.
6. In the **Periodic license allocation schedule** section, select the day and time for periodic license allocations.
7. In the **Periodic usage query schedule** section, select the day and time of the query for periodic usage.
8. 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 **Host ID** field.

Related links

Add local WebLM field descriptions on page 975

Modifying a local WebLM server configuration

Before you begin

- Log on to the WebLM server.
- Install the enterprise license file.
- Add at least one local WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Local WebLM Configuration** > **Modify local WebLM**.
3. On the Local WebLM Configuration: Modify local WebLM page, select the local WebLM server that you require to configure.
4. Click **Modify**.

   The system displays another Local WebLM Configuration: Modify local WebLM page with a different set of WebLM configuration fields.
5. Modify the information in the following fields:
   - In the **Local WebLM configuration** section, **Name**, **Description**, **Protocol**, and **Port**
   - In the **Periodic License Allocation schedule** section, **Day** and **Time**
   - In the **Periodic Usage Query schedule** section, **Day** and **Time**
6. Click **Modify**.

   The system saves your changes.

Related links

Modify local WebLM field descriptions on page 976

Removing a local WebLM server

Before you begin

- Log on to the WebLM server.
- Install the enterprise license file.
- Add at least one local WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Local WebLM Configuration** > **Delete local WebLM**.
3. On the Local WebLM Configuration: Delete local WebLM page, select the local WebLM server that you require 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 links

Delete local WebLM field descriptions on page 978

Viewing the license capacity of the licensed features of a product

Before you begin

Log on to the WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **View by feature**.

Related links

View by feature field descriptions on page 971

Viewing the connectivity status of the local WebLM servers

Before you begin

Log on to the WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **View by local WebLM**.

   The page displays the connectivity status of the local WebLM servers.

Related links

View by local WebLM field descriptions on page 972

Validating connectivity to local WebLM servers for a product

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Local WebLM Configuration**.

3. On the Local WebLM Configuration: View local WebLM page, select the local WebLM servers that you want to validate for connectivity.
4. To query the selected local WebLM servers, click **Validate Connectivity**.

Result

The **status** column on the Local WebLM Configuration: View local WebLM page of the selected WebLM servers displays if the connection request made to the local WebLM server is successful.

Related links

View Local WebLMs field descriptions on page 974

Viewing usage by WebLM

Before you begin

Log on to the WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Usages** > **Usage by WebLM**.

   The system displays the Usages: Usage by WebLM page.
3. In the **Select WebLM** field, select the master or local WebLM server.
4. Click **Query System**.

Related links

Usage by WebLM field descriptions on page 979

Viewing enterprise usage of a license feature

Before you begin

Log on to the WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Usages** > **Enterprise Usage**.

   The system displays the Usages: Enterprise Usage page.
3. In the **Select Feature (License Keyword)** field, select the licensed feature.

   The page displays the usage of the licensed feature for the master WebLM server and the local WebLM servers.

Related links

Enterprise Usage field descriptions on page 980

Viewing the periodic status of the master and local WebLM servers

Before you begin

Log on to the WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Periodic status**.

   The system displays the Periodic Status page.

Related links

Periodic Status field descriptions on page 985

Querying usage of feature licenses for master and local WebLM servers

Before you begin

Log on to the WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Usages** > **Query Usage**.

   The system displays the Usages: Query Usage page.
3. To view the usage details by feature licenses of a server, select the master or local WebLM server.
4. Click **Query Usage**.

   If you select all WebLM severs or click **Check All** and click **Query usage**, the system displays the progress of the query request.

Result

If you select one local WebLM server, the Usages: Usage by WebLM page displays the details of the local WebLM server you selected.

Related links

Query Usage field descriptions on page 981

Changing allocations of licensed features for a local WebLM server

Use this functionality to change the license allocations of a feature that resides on a local WebLM server for the product.

Procedure

1. Log in to the master WebLM server.
2. In the left navigation pane, click **Licensed products** and select the product name.
3. Click **Allocations** > **Change allocations**.

   The system displays the Allocations: Change Allocations page.
4. In the **New Allocation** column, enter the number of licenses you require to allocate for the feature that resides on a local WebLM server.
5. Click **Submit Allocations**.

Related links

Change Allocations field descriptions on page 984

Viewing allocations by features

Before you begin

Log on to the WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Allocations** > **View by feature**.

   The system displays the Allocations: View by Feature page.

Related links

Allocations by Features field descriptions on page 982

Viewing allocations by the local WebLM server

Before you begin

Log on to the WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Allocations** > **View by local WebLM**.

The system displays the Allocations: View by Local WebLM page.

3. In the **Select Local WebLM** field, select the local WebLM server.

Result

The page displays the allocation details for the local WebLM server you select.

Related links

Allocations by Local WebLM field descriptions on page 983

Viewing usage summary

Before you begin

Log on to the WebLM server.

Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Usages**.

   The system displays the Usage Summary page.

Related links

Usage Summary field descriptions on page 979

View by feature field descriptions

Use this page to view the license capacity for each feature license of a product.

Name	Description
Feature (License Keyword)	The display name and the keyword for the licensed features of the product.
License Capacity	The total number of feature licenses that the organization purchases for each feature.
Currently available	The number of floating licenses of each feature that is currently available with the master WebLM server. The feature licenses that are not allocated to any local WebLM server are known as floating licenses. ✱ **Note:** For uncounted features, this column displays “Not counted”.

View by local WebLM field descriptions

Use this page to view the information related to local WebLM servers of a product.

Name	Description
Local WebLM name	Specifies the name of the local WebLM server.
IP address	Specifies the IP address of the local WebLM server.
Last contacted	Specifies the date and time when the local WebLM server was last contacted.
Status	Lists the success or failure of the last connection request to each local WebLM server.

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 applies to the entire enterprise unless you override the setting while you add a local WebLM.

The master WebLM server uses the settings of the periodic operations to query itself and generate the usage report for licenses.

Master WebLM Configuration

Name	Description
Name	Specifies the name of the WebLM server.
Description	Provides a brief description of the server.
IP address	Specifies the IP address of the WebLM server.
Host ID	Specifies the host ID of the computer where you installed the WebLM server. You cannot edit the **Host ID** field.

Default periodic operation settings

Name	Description
Retry count	Specifies the number of times a master WebLM server must try to connect to a local WebLM server for a periodic operation after a connection failure. For example, set the count to 2. The master WebLM server makes an initial unsuccessful attempt to connect to a local WebLM server. The master WebLM server makes two more attempts to connect to the local WebLM server.

Table continues…

Name	Description
Retry interval	Specifies the duration in minutes, within which the retry count specified in the **Retry count** field must be carried out. For example, suppose the **Retry count** is 2 and the Retry interval is 10 minutes. If the attempt to connect to the server fails, the master WebLM server makes two attempts in 10 minutes to connect to the local WebLM server.

SMTP Server Settings

Name	Description
Server name	Specifies the name of the SMTP server.

E-mail notification settings for periodic operation

Name	Description
E-mail notification	Specifies the e-mail notification. The notification options are: • On: Sends an e-mail notification to the administrator if the periodic operations fail. • Off: Does not send an e-mail notification to the administrator if the periodic operations fail.
E-mail address	Specifies the e-mail address to which the WebLM application sends the e-mail notification if the periodic operations fail to execute. **Note:** Click **Add To List** to add the e-mail address in the list of recipients who must receive the e-mail notification of the periodic operation status.
E-mail addresses	Provides the list of e-mail addresses to which the WebLM application sends the e-mail notifications.
Add To List	Adds the e-mail address that you enter in the **E-mail address** field to the list of recipients who must receive the e-mail notification of the periodic operation status.
Remove Selected	Removes the selected e-mail address from the **E-mail addresses** field.

Default Periodic License Allocation Schedule

Name	Description
Day	The day of the week on which the master WebLM server must send the ALF (Allocation license file) again to the local WebLM server.
Time	The time of the day specified in the **Day** field when master WebLM must send the ALF again to the local WebLM server.

Default Periodic Usage Query Schedule

Name	Description
Day	The day of the week on which the master WebLM server must query local WebLM servers for usage reports.
Time	The time of the day you specify in the **Day** field when the master WebLM server must query local WebLM servers for usage reports.

Button	Description
Submit	Saves the enterprise configuration.
Reset	Resets the values in the fields to the values you previously saved.

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
Local WebLM Name	The name of the local WebLM server.
IP Address	IP address of the local WebLM server.
Last Contacted	Date and time when the local WebLM server was last contacted.
Status	Lists the success or failure of the last connection request to each local WebLM server.

Button	Description
Validate Connectivity	Validates the connectivity of the selected WebLM server.
Check All	Selects all the local WebLM server.
Clear All	Clears the selections of local WebLM servers.

Add local WebLM field descriptions

Local WebLM configuration

Field	Description
Name	The name of the server.
Description	A brief description of the server.
IP Address	A unique IP address of the server. If you enter an IP address that is already configured for a local WebLM server, the system displays the message: `IP Address is being duplicated`.
Protocol	The protocol scheme over which the master WebLM server communicates with the local WebLM server. **Note:** If the local WebLM server that you add is a standalone WebLM server in Virtualized Environment, use HTTPS. You cannot use HTTP for communication with the standalone WebLM server in Virtualized Environment.
Port	The port number on which the master WebLM server communicates with the local WebLM server in the specified protocol scheme.
Host ID	The host ID of the computer on which you installed the server. You cannot edit the **Host ID** field.

Periodic License Allocation schedule

Field	Description
Day	The day of the week on which the master WebLM server must send the ALFs again to the local WebLM server. By default, the system displays the settings specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However,

Table continues…

Field	Description
	the change in the schedule is only applicable to this local WebLM server.
Time	The time of the day specified in the **Day** field when the master WebLM server must send the ALFs again to the local WebLM server. By default, the system displays the settings you specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.

Periodic Usage Query schedule

Field	Description
Day	The day of the week on which the master WebLM server must query local WebLM servers for usage reports. By default, the system displays the settings you specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.
Time	The time of the day specified in the **Day** field when the master WebLM server must query local WebLM servers for usage reports. By default, the system displays the settings you specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.

Button	Description
Configure and validate	Configures the local WebLM server and validates the creation of the local WebLM server.
Back	Returns to the View local WebLMs page.

Modify local WebLM field descriptions

Use this page to modify the information of a local WebLM server.

Local WebLM configuration

Name	Description
Name	Specifies the name of the server.
Description	Displays a brief description of the server.
IP Address	Specifies the IP address of the server. **Note:** You cannot modify the information in the **IP address** field.
Protocol	Specifies the protocol scheme over which the master WebLM server listens to the local WebLM server. **Note:** If the local WebLM server that you add is a standalone WebLM server in Virtualized Environment, use HTTPS. You cannot use HTTP for communication with the standalone WebLM server in Virtualized Environment.
Port	Specifies the port number on which the master WebLM server listens to the local WebLM server in the specified protocol scheme.
Host ID	Specifies the host ID of the computer where you installed the server. **Note:** You cannot modify the information in the **Host ID** field.

Periodic License Allocation schedule

Name	Description
Day	Specifies the day of the week on which the master WebLM server must send the ALFs again to the local WebLM server.
Time	Specifies the time of the day you entered in the **Day** field when the master WebLM server must send the ALFs again to the local WebLM server.

Periodic Usage Query schedule

Name	Description
Day	Specifies the day of the week on which the master WebLM server must query the local WebLM servers for usage reports.

Table continues…

Name	Description
Time	Specifies the time of the day you entered in the **Day** field when the master WebLM server must query the local WebLM servers for usage reports.

Button	Description
Modify	Navigates to the Modify Local WebLM page for the local WebLM server you select.
Back	Discards the configuration changes and takes you back to the Modify local WebLM page.

Delete local WebLM field descriptions

Use this page to delete a local WebLM server.

Name	Description
Local WebLM name	The name of the local WebLM server.
IP address	The IP Address of the local WebLM server.
check box	Use to select the local WebLM servers that you require to delete.

Button	Description
Delete	Removes the local WebLM server you selected.
Reset	Clears the selection of the local WebLM servers.

Deletion of the local WebLM server

Use the Delete Local WebLM option to delete the instance of a local WebLM server from the master WebLM server. When you delete a local WebLM server using the Delete Local WebLM option, the system does not remove the server physically. The master WebLM server sends a delete request to the local WebLM server. On receiving a delete request, the local WebLM server deletes the ALF of the product that is installed on the local WebLM server. The system deletes the instance of the local WebLM server from the master WebLM server, irrespective of the success or failure of the ALF deletion process on the local WebLM server.

If the master WebLM server is unable to send the delete request to the local WebLM server, the system deletes the instance of the local WebLM server from the master WebLM server. The ALF installed on the local WebLM server automatically expires after 30 days.

Related links

Delete local WebLM field descriptions on page 978

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
WebLM Name	Displays the names of the master WebLM server and local WebLM servers of the product.
IP address	Specifies the IP address of the master WebLM server and local WebLM servers of the product.
Time of Query	Specifies the date and time when the system executed the last usage query for the WebLM server. If the status of the last usage query is `Failed`, this column also displays the date and time of the usage query that was last successful.
Status	Specifies the success or failure status of the last usage query that the system executed for each WebLM server. The **Status** column of a WebLM server remains blank if the server is not queried even once for feature license usage. The usage query can be a periodic usage query or a nonperiodic usage query.

Usage by WebLM field descriptions

Use this page to query the feature license usage by the master and local WebLM servers.

Name	Description
Select WebLM	The master and local WebLM servers for which you can view the usage.
Feature (License Keyword)	The name and keyword of the counted features of the product.
Currently Allocated	The number of feature licenses for each feature that the system currently allocates to the selected WebLM server. For the master WebLM server of the product, this column lists the floating licenses available with the server.
Usage: qty/%	The number of feature licenses for each feature that the licensed applications currently use from the allocated feature licenses. The column also displays the percentage of usage.

Table continues…

Name	Description
	For example, if 50 feature licenses are allocated and applications use five feature licenses, this column displays 5/10%.
Peak Usage (last 7 days): qty/%	The highest number of feature licenses for each feature that the applications use 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 was 25 and 50 feature licenses were available during the peak usage calculation, the column displays 25/50%.
Peak Usage (last 30 days): qty/%	The highest number of feature licenses for each feature that the applications use 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 was 50 and 50 feature licenses were available during the peak usage calculation, the column displays 50/100%.
Time of Query	The date and time when the system executed the usage query for the WebLM server you select.
Status	The success or failure of the last usage query process executed for each WebLM server. The **Status** column remains blank if the server is queried even once for feature license usage. The usage query can be a periodic usage query or a nonperiodic usage query.

Button	Description
Query System	Queries the selected WebLM server for the feature license usage.

Enterprise Usage field descriptions

Use this page to view the feature license usage of all WebLM servers for the selected feature.

Name	Description
Select Feature (License Keyword)	Specifies the license features for which you can view the license usage.
License capacity	Specifies the total number of feature licenses the organization purchases for each feature.

Table continues…

Name	Description
Available	Lists the number of licenses currently available with the master WebLM server.
WebLM Name	Specifies the names of the WebLM servers of the product.
Currently Allocated	Specifies the number of feature licenses that the system currently allocates to the WebLM servers for the selected feature.
Usage qty/%	Specifies the number of feature licenses that the licensed applications currently use, from the allocated feature licenses for the selected 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 displays 5/10%.
Peak Usage (last 7 days): qty/%	Specifies the highest number of feature licenses that applications use 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 is 50, the column displays 25/50%.
Peak Usage (last 30 days): qty/%	Specifies the highest number of feature licenses that applications use 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 is 50, the column displays 50/100%.
Time of Query	Specifies the date and time when the system executes the usage query for the selected feature.
Status	Specifies the status of the last usage query process that the system executes for each WebLM server. The status can be *Success* or *Failure*.

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 the feature license usage report.

Name	Description
WebLM Name	The names of the master and the local WebLM servers of the product as links. To view the feature

Table continues…

Name	Description
	license usage of a server, select the name of the required server in the **WebLM Name** column. **Note:** If the specified WebLM server is not queried even once for feature license usage, the table on the Usage by WebLM page remains blank.
IP address	The IP address of the master WebLM server and the local WebLM servers of the product.
Time of Query	The date and time when the system executes the last usage query for the WebLM server. If the status of the last usage query is `Failed`, the **Time of Query** column displays the date and time of the usage query that was last successful. **Note:** If the server does not receive a query request even once for feature license usage, the **Time of Query** column of a WebLM server remains blank.
Status	The success or failure of the last usage query that the system executes for each WebLM server. If the server does not receive a query request even once for feature license usage, the **Status** column of a WebLM server remains blank. The usage query can be a periodic usage query or a nonperiodic usage query.
Select Check box	Use to select the WebLM server for which you require to determine the usage query.

Button	Description
Check All	Selects all the WebLM servers.
Clear All	Clears the selections for all the WebLM servers.
Query Usage	Queries the WebLM servers of the product you select for their feature license usage report.

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
Feature (License Keyword)	Specifies the name and license keyword of the counted features of the product.
Local WebLM Name	Specifies the name of the local WebLM servers of the product. By default, this column is blank. The system displays the names of the local WebLM servers only when you select the arrow head in the **Feature (License Keyword)** column. If a local WebLM server does not exist for the product, the **Local WebLM Name** column remains blank for all the licensed features.
IP address	Specifies the IP addresses of the local WebLM servers of the product. By default, this column is blank. The system displays the IP address of the local WebLM servers only when you select the arrow-head in the **Feature (License Keyword)** column. If a local WebLM server does not exist for the product, the **IP address** column remains blank for all the licensed features.
License Capacity	Specifies the total number of feature licenses purchased by the organization for the respective feature.
Currently Allocated	Specifies the total number of feature licenses of the respective feature that the system 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` in the **Currently Allocated** column for the licensed feature.
Available	Lists the number of floating licenses of the respective feature that is currently available with the master WebLM server.

Note:

To view the information about the number of feature licenses of a feature that the system allocates to each local WebLM server, click the arrow-head beside the name of the required feature. The system displays new rows below the feature row with the feature license allocation information for each local WebLM server to which the feature is allocated.

Allocations by Local WebLM field descriptions

Use this page to view the feature license allocation information by local WebLM.

Name	Description
Select Local WebLM	Specifies the local WebLM servers for which you can view the feature license allocation information.
Last Allocation	Specifies the date and time when feature licenses were last allocated to the local WebLM server you select.
Status	Specifies the success or failure status of the last license allocation process that the system executes for the local WebLM server you select. The allocation process can be a periodic allocation process or a nonperiodic allocation process. If the status of the last license allocation process is `Failed`, and if the status of a previous license allocation process for the server is `Success`, the system displays the date and time of the last license allocation process that was successful in the **Last Allocation** field.
Feature (License Keyword)	Specifies the name and license keyword of the counted features that the system allocates to the local WebLM server you select.
License Capacity	Specifies the total number of feature licenses the organization purchases for each feature.
Currently Allocated	Specifies the total number of feature licenses of each feature that the system allocates to the local WebLM server you select.
Available	Lists the number of licenses currently available on the master WebLM server for allocation to local WebLM servers.

Change Allocations field descriptions

Use this page to change current feature license allocation information for each local WebLM server of a product.

Name	Description
Feature (License Keyword)	The name and license keyword of the counted features that the system allocates to the local WebLM server you select.
Local WebLM Name	The name of the local WebLM server.
IP address	The IP addresses of the local WebLM servers of the product.
License Capacity	The total number of feature licenses that the organization purchases for each feature.

Table continues…

Name	Description
Currently Allocated	The total number of feature licenses of each feature that the system allocates to the local WebLM server you select.
Currently Used	The total number of feature licenses of each feature that the product uses.
Available	The number of floating licenses of each feature that is currently available with the local WebLM server.
New Allocation	The number of new licenses that the system allocates to a local WebLM server.

Button	Description
Submit Allocations	Allocates the number of feature licenses that you specify in the **New Allocation** field to the corresponding local WebLM servers.
Reset	Resets the values that you specify in the **New Allocation** field to the previously saved value.

Periodic Status field descriptions

Use the Periodic Status option to view the status of periodic operations such as the periodic allocation of the feature licenses to the local WebLM server and querying of the local WebLM server for usage report.

Periodic Allocation

Name	Description
Local WebLM Name	Specifies the name of the local WebLM server of a product.
IP Address	Specifies the IP addresses of all the local WebLM servers of the product.
Last Allocation	Displays the date and time when the system executed the last periodic license allocation process for each local WebLM server. If the status of the last periodic license allocation process is `Failed`, the **Last Allocation** column displays the date and time of the periodic license allocation process that was last successful.
Status	Displays the success or failure status of the last periodic license allocation process that the system executed for each local WebLM server.

Periodic Usage

Name	Description
WebLM Name	Displays the name of the master WebLM server and local WebLM servers of a product.
IP Address	Displays the IP addresses of the master and local WebLM servers of a product.
Last Usage Query	Displays the date and time when the system executed the last periodic usage query for each WebLM server. If the status of the last periodic usage query is `Failed`, the **Last Usage Query** column also displays the date and time of the periodic usage query that was last successful.
Status	Displays the success or failure status of the last periodic usage query that the system executed for each WebLM server. If the server is not queried even once for feature license usage, the **Status** column of a WebLM server remains blank.

Chapter 18: Data Replication Service

Data Replication Service

Data Replication Service (DRS) replicates data stored on the System Manager server to other element nodes or the slave nodes. DRS uses and extends SymmetricDS as the underlying mechanism for data replication.

SymmetricDS is an asynchronous data replication software that supports multiple subscribers and bi-directional synchronization. SymmetricDS uses Web and database technologies to replicate tables between relational databases in near real time. The system provides several filters while recording the data, extracting the data that has to be replicated to a slave node, and loading the data on the slave node.

Databases provide unique transaction IDs to rows that are committed as a single transaction. SymmetricDS stores the transaction ID along with the data that changed, so that it can play back the transaction at the destination node exactly the way it happened. This means that the target database maintains the same integrity as the source.

DRS provides a mechanism wherein elements can specify their data requirements in an XML document. On the basis of the XML document, DRS creates database triggers on the specified application tables and captures the database events for delivery to other element nodes. The client nodes then fetch these database events.

Data replication happens in two distinct phases:

- Full-sync. This is the initial replication phase, wherein whatever data the replica node requests is replicated to the client node.
- Regular-sync. This is the phase after full-sync, wherein subsequent change events are replicated to the replica node.

DRS supports the following modes of replication:

- Replication in Repair mode. In the repair mode, DRS 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 DRS.
- 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. DRS 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. DRS creates replication batches whenever the data in the master database is added, modified, and deleted.

Using DRS, you can:

- View replica nodes in a replica group.
- Repair the replica nodes that are not synchronized. The repair action replicates the required data from System Manager.

Synchronization in a Geographic Redundancy scenario

- DRS clients work with virtual IP or FQDN for a seamless switchover to the active System Manager when failover, failback, or split network occurs.
- DRS clients provide an audit mechanism to determine if the active System Manager contains the required data to resume synchronization. After a state change, the audit mechanism validates the last batch of data that is replicated to the element with the last batch of the data in the active System Manager. The state change includes failover, failback, and split network.
- During the audit, if the element contains more recent data than the data available on the active System Manager, the system marks the element for repair. Otherwise the system marks the element as in-sync with System Manager.

DRS client audit

You can configure Data Replication Service (DRS) client elements in the Geographic Redundancy (GR) mode or GR-unaware mode.

A GR-aware DRS client must conform to the norms for a GR-aware element. A GR-aware element must work with the virtual FQDN configuration.

When you activate the secondary System Manager or when you enable GR after the system restores the primary System Manager, DRS marks all client nodes that are GR-aware for audit. The system displays the nodes marked for audit as *Pending Audit*. When you activate the secondary System Manager, DRS configures all GR-unaware DRS client nodes to deny recording any database change events. The system displays the state of DRS client nodes that are GR-unaware as *Not Managed*.

During the restoration of the primary System Manager, if you select the database of:

- The primary System Manager, the system marks all configured GR-aware client nodes for audit.
- The secondary System Manager, the system marks all DRS client nodes that are GR-aware for audit. Also, the system marks all DRS client nodes that are GR-unaware for repair.

When the system marks a node for audit, the system denies any further requests from the node until the audit is complete for that node. DRS service on System Manager sends a request to the DRS client element for audit data. DRS performs the audit for the DRS client and determines whether the client node requires a full synchronization. If the audit reveals that the client has more recent data than the data on System Manager, DRS schedules a full-synchronization for the element. This phase marks the completion of audit and the system configures DRS to accept requests from the element.

Using DRS, the system initiates the client audit under following situations:

- Manual: When an administrator activates the secondary System Manager, DRS flags all configured clients for audit. This action ensures that none of the configured client elements have more data than the secondary System Manager. DRS flags similar client audit when the primary System Manager is recovered.
- Automated: During situations such as split network, when an administrator activates the secondary System Manager server, a node changes to the secondary System Manager server. However, in split network scenario, you cannot predict the network condition and the node can change back to the primary System Manager server.

Viewing replica groups

Procedure

On the System Manager web console, click **Services** > **Replication**.

Result

The system displays the Replica Groups page with the groups in a table.

Related links

Replica Groups field descriptions on page 991

Viewing replica nodes in a replica group

You can view the replica nodes in a group.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, 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 links

Replica Nodes field descriptions on page 992

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 Data Replication Service.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, perform one of the following:
   - Select a replica group for which you want repair the replica nodes from the table displaying replica groups and click **View Replica Nodes**.
   - Click the name of the replica node under 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 links

Replica Nodes field descriptions on page 992

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.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, 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.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, 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 links

Replication Node Details field descriptions on page 995

Removing a replica node

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, select the replica group from which you must remove a node and click **View Replica Nodes**.
3. On the Replica Node page, click **Remove**.

Removing a replica node from the queue

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, select the replica group for which you must remove the node and click **View Replica Nodes**.
3. On the Replica Node page, click **Remove from Queue**.

Replica Groups field descriptions

The replica groups are logical groupings of the replica nodes. You can use the replica groups field descriptions page to:

- View all the replica groups in the enterprise.
- View the replication status of the replica groups.

The page displays the following fields when you select `All` from the **Replica Group** field.

Name	Description
Select check box	An option to select a replica group.
Replica Group	The name of the replica group. Each replica group in the list is a hyperlink. When you click a group, the system displays the replica nodes for that group on the Replica Nodes page.
Synchronization Status	For each replica group, displays the combined synchronization status of all replica nodes under the group
Group Description	A brief description of the replica group.

Button	Description
View Replica Nodes	Displays the Replica Nodes page. Use this page to view replica nodes for a group that you select.
Repair	Initiates full-sync for the selected groups and effectively for all the replica nodes that belong to the selected groups.
Filter: Enable	Displays fields under **Replica Group** and **Synchronization Status** columns where you can set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Apply	Filters replica nodes based on the filter criteria.

Replica Nodes field descriptions

You can use this page to:

- View the replica nodes in a selected replica group when you request data replication from the master database of System Manager.
- View the replication status of the replica nodes in a group.

Name	Description
Select check box	Provides the option to select a replica node.
Replica Node Host Name	Displays the full hostname of the replica node. If you need to administer Session Manager, the Replica Nodes Web page displays the fully qualified domain name. For example, ab-ct10-defg-bsm.mydata.com.
Product	Displays the name of the product.

Table continues…

Name	Description
Synchronization Status	Displays the synchronization status of the replica node. When you install a node, the node goes from a **Ready for Repair** state to the **Queued for Repair** to **Repairing**, and finally to the **Synchronized** state. During this phase, the replica node receives a full-sync, wherein configured data is replicated to the replica node. Once the replica node is prepared with a full-sync, thereafter the node receives the subsequent changes in the form of regular-sync. A replica node can be in any one of the following states during the lifecycle: • **Ready for Repair**. The database of the replica node is not synchronized with the master database. • **Queued for Repair**. The replication request of the replica server is in queue with other data replication requests. The color code of the status is yellow. • **Repairing**. The data replication process is in progress. The color code of the status is yellow. • **Synchronized**. The system has successfully replicated the data that the replica node requested from the master database to the database of the replica node. The color code of the status is green. **Note:** If you encounter the following, contact the administrator who can manually intervene to resolve the problem: • `Not Reachable`. System Manager is unable to connect to the replica node. This indicates that the replica node is switched off for maintenance, a network connectivity failure, or any other issue that affects general connectivity between System Manager and the replica node. • `Synchronization Failure`. Data replication is broken between System Manager and the replica node. This status generally indicates a catastrophic failure.

Table continues…

Name	Description
	During the automatic replication of data from the master to the replica node, the system displays the following status: • **Synchronizing**. The data replication is in progress for the replica node. The color code of the status is yellow. • **Synchronized**. The system successfully replicated the data that the replica node requested from the master database to the database of the replica node. The color code of the status is green. • **Pending Audit**. The replica node is marked for audit. In this state, DRS dishonors any request from the node until audit is successfully conducted for the node. On completion of audit activity, the node displays any of the other states as applicable. The color code of the status is yellow.
Last Synchronization Time	Displays the last time when the system performed the data synchronization or replication for the replica node.
GR Enabled	Displays whether the replica node is GR-enabled or not.
Last Replication Request Time	Displays the time when a pre-7.0 replica node last requested System Manager for data or the time when System Manager last tried to send data to a replica node on Release 7.0 or later.

Button	Description
View Details	Opens the Data Replication page. Use this page to view the synchronization details for a replica node.
Repair	Replicates or resynchronizes data from the master node to a selected replica node.
Remove	Removes the nodes you select from the replica group.
Remove From Queue	Removes the replica node you select from the queue.
Show All Replica Groups	Takes you back to the Replica Groups page.

Replication Node Details field descriptions

You can use this page to view the following details:

- The batch-related information such as total number of batches received, processed, and skipped for a replica node.
- The last time when the replication server performed the synchronization or replication.
- Synchronization or replication error details.

General

Name	Description
Replica Node Group	Displays the name of the group that the replica node belongs to. A node-group is a logical grouping of similar nodes.
Replica Node Host Name	Displays the full hostname of the replica node. If you need to administer Session Manager, the Replica Nodes Web page displays the fully qualified domain name. For example, ab-ct10-defg-bsm.mydata.com.
Last Down Time	Displays the last time and date when the replica node could not be reached. System Manager periodically checks whether a replica node is reachable.
Last Repair Start Time	Displays the last time and date when a full-sync was started for the node.
Last Repair End Time	Displays the last time and date when a full-sync was completed for the node.
Last Pull Time	Displays the time when a pre-7.0 replica node last requested System Manager for data or the time when System Manager last tried to send data to a replica node on Release 7.0 or later.
Build Version	Displays the version of the element configuration.
GR Enabled	Displays whether the replica node is GR-enabled or not.

Synchronization Statistics

Name	Description
Pending Batches	Lists the batches that are yet to be replicated to the replica node. During the data replication process, System Manager records the changes for a particular replica node in the form of events. When a replica node

Table continues…

Name	Description
	requests System Manager for change events, the change events are made into batches. These batches are then replicated to the replica node.
Pending Unbatched Events	Lists the change events that are yet to be formed into batches. The recorded change events are formed into batches and only a predefined number of batches are replicated to a replica node in a request. The remaining events wait for the subsequent request from the replica and are called unbatched events pending batching and subsequent replication.
Synchronization Status	Displays the synchronization status of the replica node. For details, see Replica Nodes field descriptions.
Last Synchronization Time	Displays the last time when the system performed the data synchronization or replication for the replica node.
Last Batch Acknowledged	Displays the last batch that an element acknowledged as successfully processed on the element side. During an audit, Data Replication Service (DRS) compares the last successfully committed batch on the node with the data in the last batch acknowledged batch. If the node has a more recent batch, then DRS schedules a full-sync for the node.
Marked For Audit	Marks all replica nodes that are GR-enabled for audit: The status can be: • ✓: Indicates that the node is marked for audit. • ✗: Indicates that the node is not marked for audit. When the node is marked for audit, the replica status changes to **Pending Audit**, and the color changes to yellow. • When you activate the secondary System Manager or when you enable GR after the primary System Manager restores • When the primary System Manager restores and you choose the database of the primary System Manager

Table continues…

Name	Description
	• When the primary System Manager restores and you choose the database of the secondary System Manager DRS denies any request from the replica node that is marked for audit until the audit is complete for the replica node.
Last Audit Time	Displays the last time and date when DRS performed the audit of data from the node that is marked for audit.

Last Error Details

Name	Description
Cause of Error	Describes why the system failed to replicate or synchronize data.
Time of Error	Displays the time when the error occurred.

Chapter 19: Managing reports

Reports

Avaya Aura® System Manager supports the Reports feature for communication objects. System Manager Release 7.0added about 350 predefined List and Display Communication Manager configuration reports.

Use Reports to:

- Generate Communication Manager object reports in various formats such as CSV, PDF, and HTML.
- Create and manage reports.
- Edit report parameters.
- Rerun reports.
- Customize the contents of a report.
- Save reports in the System Manager server.
- View and delete reports that are stored in System Manager.
- Save reports to a local computer.
- Email reports to one or more addresses. You can configure an email server to send reports.

You can assign permissions for reports and generate reports for specific custom user.

Reports Definition List field descriptions

Name	Description
Report Name	The name of the report.
Host Names	The Communication Manager instance from which the report is generated.
Creation Date	The date when the report was generated.
Created By	The user who created the report.
Format	The format in which the report is generated.

Table continues…

Name	Description
Object	The Communication Manager object used for generating the report.
Used Space	A maximum space of 1 GB allocated for storing the generated reports. If the report files exceed the maximum file size, the system generates an alarm. You must manually delete some files before generating the new report. You can configure the **Reports Output Directory Properties**, by clicking **Services** > **Configurations**. In the left navigation page, click **Settings** > **Reports** > **Configurations**. For more information, see View Profile:Configuration field descriptions.

Related links

View Profile:Configuration field descriptions on page 804

Generating a detailed report

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the left navigation pane, click **Generation**.
3. On the Reports Definition List page, click **New**.
4. On the New Report page, in the **Application** field, click **Communication Manager**.
5. In the Communication Manager table, select one or more Communication Manager instances.
6. Click **Next**.
7. Select **Detailed (Database)** to generate the report for Communication Manager objects in the database.
8. Click **Next**.
9. On the Reports Generation page, in **All Fields**, select the fields that you want to include in your report.
10. Select the report type from **Report Type**.
11. Click the right arrow icon. ›

    The **Selected Field** table displays the selected fields. By default, some fields are already available in the **Selected Fields** table.
12. Click **Next**.

13. On the Report Parameters page, complete the report parameters, and click **Generate Report**.

    You can download and view the report from **Services** > **Reports** > **History**.

    Note:

    You can only generate a **Detailed (Database)** report if the Initializing synchronization for the specific Communication Manager instances is successful, else report generation fails.

Related links

New report field descriptions on page 1001

Generating a basic report

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the left navigation pane, click **Generation**.
3. On the Reports Definition List page, click **New**.
4. On the New Report page, in the **Application** field, select **Communication Manager**.
5. From the Communication Manager table, select one or more Communication Manager instances.
6. Click **Next**.
7. Click **Basic (List and Display)** to generate a report directly from Communication Manager.
8. On the Basic Report page, select **Report Type**. You can generate either a **List** report or a **Display** report.
9. In the **Communication Manager Object** field, select Communication Manager object for which you want to generate a report.
10. In the **Qualifier** field, type the qualifier for the Communication Manager object.
11. Click **Next**.
12. On the Report Parameters page, complete the report parameters, and click **Generate Report**.

    You can download and view the report that you generated from **Services** > **Reports** > **History**.

    Note:

    You can only generate a **Basic** report if the Initializing synchronization for the specific Communication Manager instances is successful, else report generation fails.

Related links

New report field descriptions on page 1001

New report field descriptions

New Report page

Name	Description
Application	The application type for which you want to generate the report.
Name	The name of the element instance that you choose for generating the report.
Host	The Communication Manager system that you select for generating the report.

Basic Report generation page

Name	Description
Report Type	The report type. You can either generate a **List** report or a **Display** report for the particular Communication Manager object that you select.
Communication Manager Object	The Communication Manager object for which you want to generate the report.
Name	The name of the element instance that you choose for generating the report.
Host	The Communication Manager system that you select for generating the report.
Qualifier	The qualifier for the Communication Manager object that you select for generating the report.

Detailed reports generation page

Name	Description
Report Type	The Communication Manager object for which you want to generate the report.
All Fields	The fields that you want to generate as part of the report. The fields vary according to the Communication Manager object you choose.
Selected Fields	The fields that you select from **All Fields**. The report that you generate displays only the fields in **Selected Fields**.

Table continues…

Name	Description
Reset	Resets your selection. The system displays the default fields when you click **Reset**.
Move Up button	Moves up the field you selected by one position in the **Selected Fields** table.
Move Down button	Moves down the field you selected by one position in the **Selected Fields** table.

Report Parameters page

Name	Description
Report Name	The name of the report. Type a name of your choice in the **Report Name** field.
Select file format	The format in which you want to generate the report. The possible values are: • **CSV** • **PDF** • **HTML**
Select demiliter	The delimiter that you want to apply while generating the report. The possible values are: • **comma** • **semicolon** • **space** • **tab**
Select destination location	The location where you want to save the report generated. The possible values are: • **Local**: The option to save the generated report to your local computer. • **Remote Server**: The option to save the generated report to a **Remote server**, perform one of the following actions: - Select the **Remote Server** from the drop-down field to store your reports. - Select the one of the following fields that you want to store the reports: • **Name** • **IP** • **Type** • **Remote Server From** • **Default Server**

Table continues…

Name	Description
	• **Email**: The option to enter one or more email addresses that you want to send the report. You can enter multiple email addresses that are separated by a semicolon.
Customize Report	The option to customize your report. Select one of the following: • **Customize Report Header**: The option to choose a title of your choice for your report. • **Export Column Titles on First Row**: Select this option to export the column titles of your report. If you select this option, the first page displays only the column headers that you select. Other pages display the default report headers.
Schedule Job	The scheduler options to schedule the report generation job. • Select **Now** to generate the report immediately. • Select **Later** to generate the report at the scheduled time.

Button	Description
Next	Displays the next page.
Back	Displays the previous page.
Generate Report	Generates the report.
Cancel	Cancels your action.

Editing report parameters

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the left navigation pane, click **Generation**.
3. Select the report whose parameters you want to edit.
4. Click **Edit** .
5. On the Edit Report Definition page, edit the required parameters.
6. Click **Generate Report** to generate a report.

Rerunning reports

About this task

use rerun reports to generate a new report after Communication Manager synchronization is complete. Rerunning reports displays the latest available data after synchronization.

Using rerun feature, you can run the reports according to the previous configuration of the report.

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the left navigation pane, click **Generation**.
3. On the Reports Generation page, select the report that you want to rerun.
4. Click **Run Now**.

   The system displays a status message that the report generation is scheduled.

   After the system generates the report, the Report Generation page displays the date of creating the report.

Customizing reports

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the left navigation pane, click **Generation**.
3. On the Report Generation page, perform one of the following actions:
   - Click **New**.
   - Select a report, and click **Edit**.

   The system directs you to the New Report page.
4. On the New Report page, select one or more Communication Manager instances.
5. Click **Next**.

   The system directs you to **Basic Report**.
6. In the **Basic Report** section, select one or more Communication Manager instances and perform one of the following actions:
   - Select **Basic (list and display)**, and perform the following actions:
     a. Select the report type from **Report Type**.
     b. Select **Communication Manager Objects** that you want the report to display.
     c. Select one or more Communication Manager instances.

- Select **Detailed (Database)**, and perform the following actions:
    a. Select the report type from **Report Type** .
    b. Select one or more instances from the **Available Fields** column .
    c. Click the right arrow to add one or more instances from the **Available Fields** column to the **Selected Fields** column.

       The **Selected Fields** table displays the selected columns. By default, some columns are available in the **Selected Fields** table.

7. Click **Next**.

   The system displays the Report Parameters page.
8. Select **Customize Report** to add a name of your choice to the report.

   The system displays the **Customize Report Header** field.
9. Click **Customize Report Header** to add a name of your choice to the report.
10. Select **Export Column Titles on First Row** to export the column titles that the system displays on the report output.
11. On the Report Parameters page, complete the report parameters, and click **Generate Report**.

    You can download and view the report from **Services** > **Reports** > **History**.

Downloading reports

Before you begin

You must generate a report by clicking **Reports** > **Generation**.

If you select multiple reports and download them, the files are archived and downloaded as a zip file.

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the left navigation pane, click **History**.
3. Perform one of the following actions:
    - From the **Report History** table, select the report you want to download and click **Download Report**.
    - In the **Report History** table, click the hyperlink in the **File Name** column.

   The report is downloaded to your local computer.

Related links

Reports history field descriptions on page 1006

Reports history field descriptions

Field	Description
File Name	The name of the report that you type while generating a report.
Report Format	The format in which the report is generated.
Creation Date	The report generation date.
Created By	The name of the user who generated the report.
File Size	The size of the report file.
Object/CM Command Used	The Communication Manager command that you used to create this report. • For Basic Reports, the column shows Communication Manager command used. • For Detailed Reports, the column shows **Object** command used.
File Size (in KB)	The size of the report output file in KB.

Related links

Downloading reports on page 1005

Configuring email properties for reports

About this task

You must set up the email configuration before you email reports to recipients.

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Settings** > **SMGR**.
3. On the View Profile:SMGR page, click **Edit**.
4. On the Edit Profile:SMGR page, in the Email Configuration Properties section, type the values in the **From Email Address**, **From Email Password**, **Email**, and **Email Host Port** fields.
5. Click **Commit**.

Sending reports through email

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the left navigation pane, click **History**.
3. Select the report or reports that you want to send through email.
4. Click **Email Report**.
5. In the **Enter email addresses** field, enter the email addresses to which you want to send the report.

   You can enter multiple email addresses separated by a semicolon.
6. Click **Email Report**.

   To go to the previous page, click **Back**.

   To clear the email addresses you have entered, click **Clear**.

Deleting reports

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the left navigation pane, click **History**.
3. From the **Report History** table, select the report that you want to delete.
4. Click **Delete**.
5. On the Report History Delete Confirmation page, click **Delete**.

Configuring report properties

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Settings** > **Reports** > **Configurations**.
3. Click **Edit** .
4. On the Edit profile: Configuration page, configure the following properties:
   - output directory
   - alarm properties
   - cleanup properties

5. Click **Done**.

Related links

View Profile:Configuration field descriptions on page 804

Remote server configuration

Adding a remote server

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the left navigation pane, click **Reports** > **Remote Server Configuration**.
3. On the Remote Server Configuration page, click **New**.
4. On the Add Server page, complete the details of the remote server.
5. Click **Commit**.

Viewing the details of a remote server

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the left navigation pane, click **Reports** > **Remote Server Configuration**.
3. On the Remote Server Configuration page, select the server whose details you want to view.
4. Click **View**.

   You can view the details of the remote server on the View Server page.

Editing the details of a remote server

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the left navigation pane, click **Reports** > **Remote Server Configuration**.
3. On the Remote Server Configuration page, select the server whose details you want to edit.
4. Click **Edit**.
5. On the Edit Server page, edit the details of the remote server.

6. Click **Commit**.

Deleting a remote server

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the left navigation pane, click **Reports** > **Remote Server Configuration**.
3. On the Server Configuration page, select the server or servers that you want to delete.
4. Click **Delete**.
5. On the Confirmation page, click **Delete**.

Remote Server configuration field descriptions

Field	Description
Name	The name of the remote server.
IP Address	The IP address of the remote server.
Server Path	The remote server path where the reports are saved.
Type	The type of remote server: • SCP • SFTP
Default Library	The option to use the default library to store the reports.
User Name	The user name of the remote server.
Password	The password of the remote server.
Confirm Password	The remote server password that you retype.

Button	Description
Commit	Adds or edits the changes to the remote server.
Clear	Cancels all changes that you perform.
Cancel	Cancels your current action.
Edit	Edits the remote server configuration details.
Done	Saves the remote server configuration changes.

Chapter 20: Managing scheduled jobs

Scheduler

The Scheduler service provides a generic job scheduling service for System Manager and Avaya Aura® applications. The Scheduler service provides an interface to run a job on demand or on a periodic basis. You can schedule a job to generate an output immediately or set the frequency of the task execution to run on a periodic basis. You can modify the frequency for a periodic job schedule any time. After you define a task or a job, System Manager creates instances of the task, monitors the execution of the task, and updates the status of the task.

Scheduled jobs can be of three types:

- System scheduled: The job that the system executes on a periodic basis for the system to operate normally. The system adds these jobs at start-up and supports all frequencies other than one time. Scheduled jobs run asynchronously in the background. As an administrator, you cannot add or delete system-scheduled jobs. You can only disable or enable the jobs to stop temporarily.
- Admin scheduled: The job that the administrator schedules for administering the application. The administrator can use various navigation paths to schedule jobs such as bulk import and directory synchronization. The system lists the jobs in the scheduler as admin scheduled jobs.
- On-demand: The administrator can schedule on-demand jobs from the list of existing jobs.

You can perform the following operations using the Scheduler page on System Manager Web Console:

- View the pending and completed scheduled jobs.
- Modify a job scheduled by an administrator or an on-demand job.
- Delete a scheduled job.
- Schedule an on-demand job.
- Stop a running job.
- Enable or disable a job.
- Search a scheduled job.

Accessing scheduler

Procedure

On the System Manager web console, click **Services** > **Scheduler**.

Assigning permissions to access Scheduler

About this task

System Manager provides access permissions to **Scheduler** through Role Based Access Control (RBAC). System Manager defines flexible access privileges for add, delete, modify, view, schedule on-demand, enable, disable and stop so that the users with administrator credentials can create their own roles.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and perform one of the following steps:
   - Click **New**.
   - Right-click and select **New**.

   The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.
4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. In **Group Name**, select the group of templates to which you want to apply this permission.

   You can leave **Group Name** blank if you do not want to select a group.
7. In the **Element or Resource Type** field, select **scheduleroperation**.
8. In **Element or Resource Instance**, select **adminSched**, **onDemand**, **sysSched**, or **All**.
9. Click **Next**.
10. Select **all operations**, and click **Commit**.

    You can now gain access to the **Scheduler** links.

Viewing pending jobs

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. In the left navigation pane, click **Pending Jobs**.
3. To view the details of the job, 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.

Related links

Pending Jobs field descriptions on page 1017

Viewing completed jobs

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Click **Completed Jobs** in the left navigation pane.

   The Completed Jobs page displays completed jobs.
3. To view the details of the jobs, 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.

Related links

Completed Jobs field descriptions on page 1019

Viewing logs for a job

About this task

Use this functionality to view logs for a pending and completed job.

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Perform the following:
   - To view logs for a pending job, perform the following steps:
     a. Click **Pending Jobs** in the left navigation pane.

   b. On the Pending Jobs page, select a pending job and click **More Actions** > **View Log**.

- To view logs for a competed job, perform the following steps:

   a. Click **Completed Jobs** in the left navigation pane.

   b. On the Completed Jobs page, select a completed job and click **More Actions** > **View Log**.

The log viewer displays the details for the selected job.

Filtering jobs

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Perform one of the following:
   - To filter pending jobs:

     a. In the left navigation pane, click **Scheduler** > **Pending Jobs**.

     b. On the Pending Jobs page, click **Filter: Enable**.
   - To filter completed jobs:

     a. In the left navigation pane, click **Scheduler** > **Completed Jobs**.

     b. On the Completed Jobs page, click **Filter: Enable**.

   The system displays the **Filter: Enable** option at the upper-right corner of the page.
3. Complete the fields to filter a job using the following criteria:
   - **Job Type**. The type of the job.
   - **Job Name**. Name of the job.
   - **Job Status**. Status of the job.
   - **State**. State of the job.
   - **Frequency**. Frequency at which the job must be executed.
   - **Scheduled By**. The user who scheduled the job
4. Click **Apply**.

   The system displays jobs that match the filter criteria.

Editing a job

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Perform one of the following steps:
   - To edit a pending job, perform the following steps:
     a. Click **Pending Jobs** in the left navigation pane.
     b. On the Pending Jobs page, select a pending job and click **Edit** or click **View** > **Edit**.
   - To edit a competed job, perform the following steps:
     a. Click **Completed Jobs** in the left navigation pane.
     b. On the Completed Jobs page, select a completed job and click **Edit** or click **View** > **Edit**.
3. On the Job Scheduling-Edit Job page, modify the appropriate information and click **Commit** to save the changes.

   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

Before you begin

You have logged in as an administrator to delete an administrator scheduled job.

About this task

Use this functionality to delete an obsolete job. You can delete an on-demand and an administrator scheduled job.

Note:

You can remove only **Schedule On Demand** type of jobs.

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Perform one of the following steps:
   - To remove a pending job, perform the following steps:
     a. Click **Pending Jobs** in the left navigation pane.
     b. On the Pending Jobs page, select a pending job.

        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. See Disabling a job on page 1015 on how to disable a job.

c. Click **Delete**.

- To remove a competed job, perform the following steps:

a. Click **Completed Jobs** in the left navigation pane.

b. 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.

c. Click **Delete**.

3. On the Delete Confirmation page, click **OK**.

System Manager deletes the job you select from the database.

Disabling a job

About this task

Use this functionality to make a job inactive.

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Perform one of the following steps:
   - To disable a pending job, perform the following steps:
     a. Click **Pending Jobs** in the left navigation pane.
     b. On the Pending Jobs page, select a pending job and click **More Actions** > **Disable**.
   - To disable a competed job, perform the following steps:
     a. Click **Completed Jobs** in the left navigation pane.
     b. On the Completed Jobs page, select a completed job and click **More Actions** > **Disable**.
3. On the Disable Confirmation page, click **Continue**.

   The **State** of the job you selected changes to **Disabled**.

Enabling a job

About this task

Use this functionality to make a job active.

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Perform one of the following steps:
   - To enable a pending job, perform the following steps:
     a. Click **Pending Jobs** in the left navigation pane.
     b. On the Pending Jobs page, select a pending job and click **More Actions** > **Enable**.
   - To enable a competed job, perform the following steps:
     a. Click **Completed Jobs** in the left navigation pane.
     b. On the Completed Jobs page, select a completed job and click **More Actions** > **Enable**.

     Note:

     When you enable a job, the system does not restart the job that completed all executions. To restart a job that completed all executions, reconfigure the job parameters from Job Scheduling-Edit Job page.

   The system displays `Enabled` in the **State** column of the selected job.

Stopping a job

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. In the left navigation pane, click **Pending Jobs**.
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

Name	Description
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. ⚙ System scheduled job. 2. 🕒 Admin scheduled job. 3. 🕒 On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The types of status are: 1. Pending Execution 2. Running
State	The state of a job whether the job is active or inactive. The types of state are: • Enabled: An active job. • Disabled: An inactive job.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The person who scheduled the job.

Button	Description
View	Displays the Job Scheduling-View Job page that displays the details of the selected pending job.
Edit	Displays the Job Scheduling-Edit Job page that you can use to modify the information of a selected pending job.
Delete	Displays the Delete Confirmation page that prompts you to confirm the deletion of the selected jobs.
More Actions > **View Log**	Displays the Logging page that displays the logs for the selected pending jobs.
More Actions > **Stop**	Stops the selected job that is currently running.
More Actions > **Enable**	Changes the state of the selected pending job from inactive to active.
More Actions > **Disable**	Displays the Disable Confirmation page that prompts you to confirm the disabling of the selected pending job.

Table continues…

Button	Description
More Actions > **Schedule On Demand Job**	Displays the Job Scheduling-On Demand Job page that you can use to schedule the selected pending job of type On Demand.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a pending job.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. **Filter: Enable** is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Apply	Filters pending jobs based on the filter criteria.
Select: All	Selects all the pending jobs in the table displayed in the **Job List** section.
Select: None	Clears the selection for the pending jobs that you have selected.
Refresh	Refreshes the pending job information.

Criteria section

To view this section, click **Advanced Search**. You can find the **Advanced Search** link at the at the upper-right corner of the page.

Name	Description
Criteria	The following three fields: • Field 1– The list of criteria that you can use to search the pending jobs. • Field 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you selected in the first field. • Field 3 – The value corresponding to the search criteria.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the pending jobs based on the specified search conditions and displays the search results in the **Groups** section.
Close	Cancels the search operation and hides the **Criteria** section.

Related links

[Viewing pending jobs](#) on page 1012
[Scheduler](#) on page 1010

Completed Jobs field descriptions

Name	Description
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. ⚙ System scheduled job. 2. 🕒 Admin scheduled job. 3. 🕒 On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The types of status are: 1. Status Unknown 2. Interrupted 3. Failed 4. Successful 5. Not Authorized
Last Run	The date and time when the job was last run.
State	The state of a job, whether the job is active or inactive. The types of state are: • Enabled: An active job. • Disabled: An inactive job.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The person who scheduled the job.

Button	Description
View	Displays the Job Scheduling-View Job page that displays the details and of the selected completed job.
Edit	Displays the Job Scheduling-Edit Job page that you can use to modify the information of a selected completed job.

Table continues…

Button	Description
Delete	Displays the Delete Confirmation page that prompts you to confirm the deletion of the selected Jobs.
More Actions > **View Log**	Displays the Logging page that displays the logs for the selected completed jobs.
More Actions > **Enable**	Changes the state of the selected completed job from inactive to active.
More Actions > **Disable**	Displays the Disable Confirmation page that prompts you to confirm the disabling of the selected completed job.
More Actions > **Schedule On Demand Job**	Displays the Job Scheduling-On Demand Job page that you can use to schedule an On Demand job.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a completed job.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters pending jobs based on the filter criteria.
Select: All	Selects all the completed jobs in the table displayed in the Job List section.
Select: None	Clears the selection for the completed jobs that you have selected.
Refresh	Refreshes the completed job information.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page.

Name	Description
Criteria	Displays the following three fields: • Field 1 - The list of criteria that you can use to search the completed jobs. • Field 2 – The operators for evaluating the expression. The operators that system displays depends on the type of criterion that you selected in the first field. • Field 3 – The value corresponding to the search criteria.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the completed jobs based on the specified search conditions and displays the search results in the **Groups** section.
Close	Cancels the search operation and hides the **Criteria** section.

Related links

Viewing completed jobs on page 1012
Scheduler on page 1010

Job Scheduling-View Job field descriptions

Use this page to view the details and frequency of a job.

Job Details

Name	Description
Job Name	The name of the job.
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. ⚙ System scheduled job. 2. 🕒 Admin scheduled job. 3. 🕒 On-demand job.
Job Status	The current status of the job. The types of status are: 1. Running 2. Pending 3. Status Unknown 4. Interrupted 5. Failed 6. Successful 7. Not Authorized
Job State	The state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	The settings that 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.
Range	The number of recurrences or a date after which the job stops to recur.

Button	Description
View Log	Opens the Logging page that you can use to view the logs for the selected job.
Edit	Opens the Job Scheduling-Edit Job page that you can use to edit the pending job information.
Cancel	Closes the Job Scheduling-View Job page and returns to the Pending Jobs or Completed Jobs page.

Related links

Scheduler on page 1010

Job Scheduling-Edit Job field descriptions

Job Details

Name	Description
Job Name	The name of the job.
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. ⚙ System scheduled job. 2. 🕒 Admin scheduled job. 3. 🕒 On-demand job. **Note:** You can only view the information in this field.
Job Status	The current status of the job. The types of status are: 1. Running 2. Pending

Table continues…

Name	Description
	3. Status Unknown 4. Interrupted 5. Failed 6. Successful 7. Not Authorized **Note:** You can only view the information in this field.
Job State	The state of a job whether the job is active or inactive. The types of state are: • Enabled: An active job. • Disabled: An inactive job.
Scheduled By	The scheduler of the job. **Note:** You can only view the information in this field.

Job Frequency

Name	Description
Task Time	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.
Recurrence	The settings that 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.
Range	The number of recurrences or the date after which the job stops to recur.

Button	Description
Commit	Saves the changes to the database.
Cancel	Closes the Job Scheduling-View Job page and returns to the Pending Jobs or Completed Jobs page.

Related links

Scheduler on page 1010

Job Scheduling-On Demand Job field descriptions

Use this page to schedule an on-demand job.

Job Details

Name	Description
Job Name	The name of the job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	The settings that 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: • Execute task one time only. • Task are repeated: - Minutes - Hourly - Daily - Weekly - Yearly
Range	The settings that define the number of recurrences or date after which the job stops recurring. The options are: • No End Date • End After occurrences • End By Date

Button	Description
Commit	Schedules an On-Demand job.
Cancel	Cancels the scheduling of an On Demand job operation and takes you back to the Pending Jobs or Completed Jobs page.

Disable Confirmation field descriptions

Use this page to disable selected jobs.

Name	Description
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. ⚙ System scheduled job. 2. 🕒 Admin scheduled job. 3. 🕒 On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The types of status are: 1. Running 2. Pending 3. Status Unknown 4. Interrupted 5. Failed 6. Successful 7. Not Authorized
State	The state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job.
Last Run	The date and time when the job was last run successfully. **Note:** The last run is applicable only for completed jobs.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The scheduler of the job.

Button	Description
Continue	Disables the job and cancels the next executions that are scheduled for the job.
Cancel	Cancels the operation of disabling a job and takes you back to the Pending or completed Jobs page.

Related links

Scheduler on page 1010

Stop Confirmation field descriptions

Use this page to stop a running job.

Name	Description
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. ⚙ System scheduled job. 2. 🕓 Admin scheduled job. 3. 🕓 On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The jobs on this page have status Running.
State	The state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job. All the jobs on this page are in the **Enabled** state.
Last Run	The date and time when the job was last run successfully. **Note:** The last run is applicable only for completed jobs.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The scheduler of the job.

Button	Description
Continue	Stops the job.
Cancel	Cancels the operation of stopping a job and takes you back to the Pending Jobs page.

Related links

Scheduler on page 1010

Delete Confirmation field descriptions

Name	Description
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. ⚙ System scheduled job. 2. 🕑 Admin scheduled job. 3. 🕑 On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the job.
State	The state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job. The jobs on this page are in the **Disabled** state.
Last Run	The date and time when the job was last run. **Note:** The last run is applicable only for completed jobs.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The scheduler of the job.

Button	Description
Continue	Deletes the selected job.
Cancel	Cancels the operation of deleting a job and takes you back to the Pending or completed Jobs page.

Related links

Scheduler on page 1010

Chapter 21: 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. With System Manager, you can create, store, and use templates to simplify tasks like adding, editing, and viewing endpoints or subscribers. In System Manager, you can use default templates or you can create your own templates as well.

Templates are available 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 or custom templates any time.

You can create a custom alias endpoint template by duplicating a default alias template. The Alias template is populated in **Custom templates** after synchronization. You can view, edit, upgrade and delete these alias custom templates in **Templates** > **CM Endpoint** > **Custom templates**.

Template versioning

Template versioning

You can version endpoint templates with Communication Manager 5.0 and later. You can associate a template with a specific version of 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: Aura Messaging 6.3, Aura Messaging 6.2, Aura Messaging 6.1, Aura Messaging 6.0, MM 5.0, MM 5.1, MM 5.2, CMM 5.2, CMM 6.0, CMM 6.2, CMM 6.3 and CMM 7.0.

Filtering templates

Procedure

1. On the System Manager web console, click **Services** > **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.

Upgrading a template

Use this feature to upgrade an existing Communication Manager template to a later Communication Manager release. You can upgrade only custom templates. This feature supports upgrading a Communication Manager agent or endpoint template from an earlier Communication Manager release to a subsequent Communication Manager release. You can also upgrade templates across multiple releases.

This feature does not support downgrading of template versions.

When you perform the upgrade operation, note that:

- System migrates the existing template settings to the new template version.
- System sets the new parameters in the new template version to default values.
- System deletes the deleted parameters in the new template version as compared to the older template version.
- System makes the new keywords available for editing within the new template, but the upgraded template retains the previous keyword setting, if available. If the previous keyword is not available, then the default is used in the upgraded template.

After you commit a template upgrade task, the system upgrades the template and enlists the newly upgraded template on the Template List.

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. Click **CM Endpoint** in the left navigation pane.
3. Select the Communication Manager system whose custom template you want to upgrade from the list under **Supported Feature Server Versions**.

You can upgrade only custom templates.

4. Click **Show List**.
5. Select the custom template that you want to upgrade from **Template List**.
6. Click **Upgrade**.
7. On the Upgrade Endpoint Template page, select the Communication Manager version for template upgrade from the list in **Supported CM Version**.
8. In the **Template Name** text box, enter the new name for the template.
9. Click **Upgrade**. The system updates **Template List** with the newly upgrade template.

Adding CM Agent template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Agent**.
3. Click **New**.
4. Enter a name in the **Template Name** field.
5. Complete the mandatory fields under the **General Options** and **Agents Skills** tabs.
6. Click **Commit**.

Related links

Add Agent Template field descriptions on page 1041

Editing CM Agent template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Agent**.
3. Select the template you want to edit from the Templates List.

   Note:

   You cannot edit default templates.

4. Click **Edit** or click **View** > **Edit**.
5. Complete the **Edit Agent Template** page.
6. Click **Commit** to save the changes.

Related links

Add Agent Template field descriptions on page 1041

Viewing CM Agent template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Agent**.
3. Select the template you want to view from the Templates List.
4. Click **View**.

   You can view the **General Options** and **Agent Skills** sections on the View Agent Template page.

Related links

Add Agent Template field descriptions on page 1041

Deleting CM Agent template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Agent**.
3. Select the template you want to delete from the Templates List.

   Note:

   You cannot delete default templates.
4. Click **Delete**.

Duplicating CM Agent template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Agent**.
3. Select the template you want to copy from the Templates List.
4. Click **Duplicate**.

5. Complete the **Duplicate Agent Template** page.
6. Click **Commit**.

Related links

Add Agent Template field descriptions on page 1041

Adding CM Endpoint templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Endpoint**.
3. Click the **Custom Templates List** tab.
4. Click **New**.
5. Select the **Set type**.
6. Enter a name in the **Template Name** field.
7. Complete the mandatory fields under the **General Options**, **Feature Options**, **Site Data**, **Abbreviated Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections.
8. Click **Commit**.

Related links

Endpoint / Template field descriptions on page 644

Editing CM Endpoint templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Endpoint**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click the **Custom templates** tab.

   Note:

   You cannot edit default templates.
6. Select the template you want to edit from the template list.
7. Click **Edit** or click **View** > **Edit**.

8. Complete the **Edit Endpoint Template** page.
9. Click **Commit** to save the changes.

Related links

Endpoint / Template field descriptions on page 644

Viewing CM Endpoint templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Endpoint**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click the **Custom template** or **Default template** tab.
6. Select the template you want to view.
7. Click **View**.

   You can view the **General Options**, **Feature Options**, **Site Data**, **Abbreviated Call Dialing**, **Enhanced Call Fwd**, and **Button Assignment** sections on the View Endpoint Template page.

Related links

Endpoint / Template field descriptions on page 644

Deleting CM Endpoint templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Endpoint**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click the **Custom templates** tab.

   Note:

   You cannot delete default templates.
6. Select the endpoint templates you want to delete from the endpoint template list.
7. Click **Delete**.

Duplicating CM Endpoint templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **CM Endpoint**.
3. Select a Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click the **Custom templates** tab or the **Default templates** tab.
6. Select the template you want to copy from the endpoint template list.
7. Click **Duplicate**.
8. Enter the name of the new template in the **New Template Name** field.
9. Choose the appropriate set type from the **Set Type** field.
10. Complete the **Duplicate Endpoint Template** page and click **Commit**.

Related links

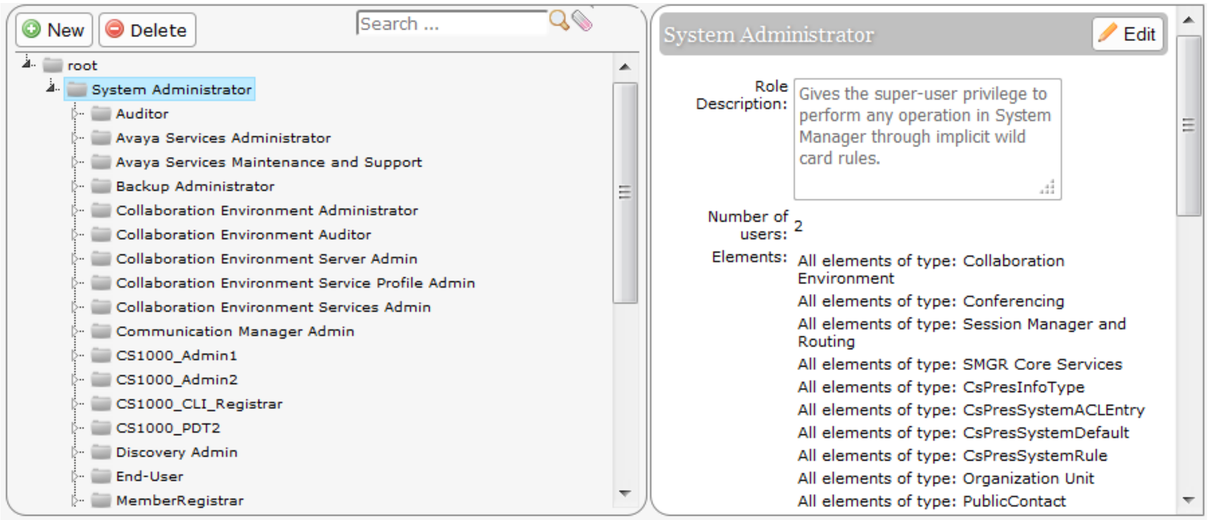
Endpoint / Template field descriptions on page 644

Assigning permissions for CM templates

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and perform one of the following steps:
   - Click **New**
   - Right-click and select **New**.

   The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



- root
  - System Administrator
    - Auditor
    - Avaya Services Administrator
    - Avaya Services Maintenance and Support
    - Backup Administrator
    - Collaboration Environment Administrator
    - Collaboration Environment Auditor
    - Collaboration Environment Server Admin
    - Collaboration Environment Service Profile Admin
    - Collaboration Environment Services Admin
    - Communication Manager Admin
    - CS1000_Admin1
    - CS1000_Admin2
    - CS1000_CLI_Registrar
    - CS1000_PDT2
    - Discovery Admin
    - End-User
    - MemberRegistrar

System Administrator

Role Description: Gives the super-user privilege to perform any operation in System Manager through implicit wild card rules.

Number of users: 2

Elements: All elements of type: Collaboration Environment
All elements of type: Conferencing
All elements of type: Session Manager and Routing
All elements of type: SMGR Core Services
All elements of type: CsPresInfoType
All elements of type: CsPresSystemACLEntry
All elements of type: CsPresSystemDefault
All elements of type: CsPresSystemRule
All elements of type: Organization Unit
All elements of type: PublicContact

4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping**.
7. In **Group Name**, select the group of templates to which you want to apply this permission.

   You can leave **Group Name** blank if you do not want to select a group.
8. In the **Element or Resource Type** field, click **Communication Manager Templates**.
9. In the **Element or Resource Instance** field, click the Communication Manager templates to which you want to apply this permission.

   The system displays only the templates you select in the **Element or Resource Instance** field in the Agent or Endpoints Templates List page.
10. Click **Next**.
11. On the Permission Mapping page, apply the required permission. For example, click **select view**.
12. Click **Commit**.

    Users with the view permission can only view the CM Endpoint templates within the specified group. You must select **All** and then select view.

Adding subscriber templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **Messaging**.
3. Select a messaging version from the list of supported messaging versions.

4. Click **Show List**.
5. Click **New**.
6. Complete the **Basic Information**, **Subscriber Directory**, **Mailbox Features**, **Secondary Extensions** and **Miscellaneous** sections in the Add Subscriber Template page.
7. Click **Commit**.

   Subscriber templates have different versions based on the software version. The subscriber templates you create have to correspond to the Messaging, 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 links

Subscriber MM Templates field descriptions on page 1053
Subscriber CMM Templates field descriptions on page 1051
Subscriber Messaging Templates field descriptions on page 1048

Editing subscriber templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **Messaging**.
3. From the supported messaging version list, select a messaging version.
4. Click **Show List**.
5. Select a subscriber template from the Subscriber Template list.
6. Click **Edit** or **View** > **Edit**.
7. Edit the required fields on the **Edit Subscriber Template** page.
8. Click **Commit** to save the changes.

   Note:

   You cannot edit any of the default subscriber templates.

Related links

Subscriber MM Templates field descriptions on page 1053
Subscriber CMM Templates field descriptions on page 1051
Subscriber Messaging Templates field descriptions on page 1048

Viewing subscriber templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **Messaging**.
3. From the supported messaging versions list, select one of the messaging versions.
4. Click **Show List**.
5. Select a subscriber template from the Subscriber Template list.
6. 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 links

Subscriber MM Templates field descriptions on page 1053
Subscriber CMM Templates field descriptions on page 1051
Subscriber Messaging Templates field descriptions on page 1048

Deleting subscriber templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **Messaging**.
3. From the list of supported messaging versions, select a supported messaging version.
4. Click **Show List**.
5. From the Subscriber Template list, select the templates you want to delete.
6. Click **Delete**.

   Note:

   You cannot delete any default subscriber template.

Duplicating subscriber templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **Messaging**.

3. From the list of supported messaging versions, select a messaging version.
4. Click **Show List**.
5. From the Subscriber Template list, select the subscriber template you want to copy.
6. Click **Duplicate**.
7. Complete the Duplicate Subscriber Template page and click **Commit**.

Related links

Subscriber MM Templates field descriptions on page 1053
Subscriber CMM Templates field descriptions on page 1051
Subscriber Messaging Templates field descriptions on page 1048

Viewing associated subscribers

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **Messaging**.
3. From the list of supported messaging versions, select a messaging version.
4. Click **Show List**.
5. From the Subscriber Template list, select a subscriber template for which you want to view the associated subscribers.
6. 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.

Templates List

You can view Templates List when you click **Template** under **Services** on the System Manager console.

You can apply filters and sort each of the columns in the Template List. When you click **Refresh**, you can view the updated information available after the last synchronization operation.

IP Office Endpoint Templates

Name	Description
Name	Name of the template.

Table continues…

Name	Description
System Type	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.
Version	The change version of the template.
Set Type	The set type of the branch gateway endpoint template.
Last Modified Time	The time and date when the template was last modified.

Name	Description
Name	The name of the template.
Owner	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.
Version	The change version of the template.
Default	Specifies whether the template is default or user-defined.
Last Modified	The time and date when the endpoint or messaging template was last modified.
Set type (for endpoint templates)	The set type of the endpoint template.
Type (for messaging templates)	Specifies whether the messaging type is Messaging, MM, or CMM.
Software Version	The software version of the element for the template.

IP Office System Configuration template

Name	Description
Name	Name of the template.
System Type	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.
Version	The change version of the template.
Last Modified Time	The time and date when the template was last modified.

CM Agent template

Name	Description
Name	Name of the template.
Owner	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.
Version	The change version of the template.
Default	Specifies whether the template is default or user-defined.
Software Version	The software version of the element for the template.
Last Modified	The time and date when the template was last modified.

CM Endpoint template

Name	Description
Name	Name of the template.
Owner	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.
Version	The change version of the template.
Default	Specifies whether the template is default or user-defined.
Software Version	The software version of the element for the template.
Last Modified	The time and date when the template was last modified.

Messaging template

Name	Description
Name	Name of the template.
Owner	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.
Version	The change version of the template.
Default	Specifies whether the template is default or user-defined.

Table continues…

Name	Description
Type	The type of the messaging template.
Software Version	The software version of the element for the template.
Last Modified	The time and date when the template was last modified.

Add Agent Template field descriptions

Field	Description
System Type	The Communication Manager that the agent is assigned to.
Template Name	The name of the agent template. You can enter the name of your choice in this field.
Software Version	The Communication Manager version of the agent template.

Field	Description
AAS	The option to use this extension as a port for an Auto Available Split/Skill. By default, this check box is clear. This option is intended for communication server adjunct equipment ports only, not human agents. ❗ **Important:** When you enter `y` in the AAS field, it clears the password and requires execution of the **`remove agent-loginid`** command. To set AAS to `n`, remove this logical agent, and add it again.
ACW Agent Considered Idle	The option to count After Call Work (ACW) as idle time. The valid entries are **System**, **Yes**, and **No**. Select **Yes** to have agents who are in ACW included in the Most-Idle Agent queue. Select **No** to exclude ACW agents from the queue.
AUDIX	The option to use this extension as a port for AUDIX. By default, this check box is clear. ✱ **Note:** The AAS and AUDIX fields cannot both be `y`.
AUDIX Name for Messaging	You have the following options: • Enter the name of the messaging system used for LWC Reception

Table continues…

Field	Description
	• Enter the name of the messaging system that provides coverage for this Agent LoginID • Leave the field blank. This is the default setting.
Auto Answer	When using EAS, the auto answer setting of the agent applies to the station where the agent logs in. If the auto answer setting for that station is different, the agent setting overrides the station setting. The valid entries are: • **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. You can use the ringer-off button to prevent the ring when the feature-related system parameter, **Allow Ringer-off with Auto-Answer** is set to `y`. • **acd**: Only ACD split /skill calls and direct agent calls go to auto answer. If this field is acd, non-ACD calls terminated to the agent ring audibly. • **none**: All calls terminated to this agent receive an audible ringing. This is the default setting. • **station**: Auto answer for the agent is controlled by the auto answer field on the Station screen.
Aux Work Reason Code Type	Determines how agents enter reason codes when entering AUX work. The valid entries are: • **system**: Settings assigned on the Feature Related System Parameters screen apply. This is the default setting. • **none**: You do not want an agent to enter a reason code when entering AUX work. • **requested**: You want an agent to enter a reason code when entering AUX mode but do not want to force the agent to do so. To enter this value, the reason codes and EAS on the System-Parameters Customer-Options screen must be set to`y`. • **forced**: You want to force an agent to enter a reason code when entering AUX mode. To enter this value, the Reason Codes and EAS on the System-Parameters Customer-Options screen must be set to `y`.
Call Handling Preference	Determines which call an agent receives next when calls are in queue. When calls are in queue and an

Table continues…

Field	Description
	agent becomes available, the following entries are valid: • **skill-level**: Delivers the oldest, highest priority calls waiting for the highest-level agent skill. • **greatest-need**: Delivers the oldest, highest priority calls waiting for any agent skill. • **percent-allocation**: Delivers a call from the skill that will otherwise deviate most from its administered allocation. Percent-allocation is available only with Avaya Business Advocate software. For more information, see *Avaya Business Advocate User Guide*.
COR	The Class Of Restriction for the agent. Valid entries range from **0** to **995**. The default entry is **1**.
Coverage Path	The coverage path number used by calls to the LoginID. Valid entries are a path number from **1** to **999**, time of day table **t1** to **t999**, or blank (default). This is used when the agent is logged out, busy, or does not answer calls.
Direct Agent Calls First (not shown)	The option to direct agent calls to override the percent-allocation call selection method and be delivered before other ACD calls. Clear the check box if you want to treat direct agent calls as other ACD calls. This field replaces the Service Objective field when percent-allocation is entered in the Call Handling Preference field. For more information, see *Avaya Business Advocate User Guide*.
Direct Agent Skill	The number of the skill used to handle Direct Agent calls. Valid entries range from **1** to **2000**, or blank. The default setting is blank.
Forced Agent Logout Time	Enables the Forced Agent Logout by Clock Time feature by administering a time of day to automatically log out agents using an hour and minute field. Valid entries for the hour field range from **01** to **23**. Valid entries for the minute field are **00**, **15**, **30**, and **45**. The default is blank (not administered). Examples are: 15:00, 18:15, 20:30, 23:45.
Local Call Preference	The option to administer Local Preference Distribution to handle agent-surplus conditions, call-surplus conditions, or both. Use this field to administer call-surplus conditions. To set up an algorithm for agent-surplus conditions, set the Local

Table continues…

Field	Description
	Agent Preference field on the Hunt Group screen. You can select this check box only if the Call Center Release field is set to 3.0 or later and the Multiple Locations customer option is active.
LoginID for ISDN/SIP Display	The option to include the Agent LoginID CPN and Name field in ISDN and SIP messaging over network facilities. By default, the check box is clear, indicating that the physical station extension CPN and Name is sent. Send Name on the ISDN Trunk Group screen prevents sending the calling party name and number if set to n and may prevent sending it if set to `r` (restricted).
Logout Reason Code Type	Determines how agents enter reason codes. The valid entries are: • **System**: Settings assigned on the Feature Related System Parameters screen apply. This is the default entry. • **Requested**: You want an agent to enter a reason code when logging out but do not want to force the agent to do this. To enter this value, the reason codes and EAS on the System-Parameters Customer-Options screen must be set to `y`. • **Forced**: You want to force an agent to enter a reason code when logging out. To enter this value, the Reason Codes and EAS on the System-Parameters Customer-Options screen must be set to `y`. • **None**: You do not want an agent to enter a reason code when logging out.
LWC Reception	Indicates whether the terminal can receive Leave Word Calling (LWC) messages. The valid entries are: • **audix** • **msa-spe**. This is the default entry. • **none**
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.

Table continues…

Field	Description
Maximum time agent in ACW before logout (Sec)	Sets the maximum time the agent can be in ACW on a per agent basis. The valid entries are: • **system**: This is the default entry. Settings assigned on the Feature Related System Parameters screen apply. • **none**: ACW timeout does not apply to this agent. • **30-9999 sec**: Indicates a specific timeout period. This setting will take precedence over the system setting for maximum time in ACW.
MIA Across Skills	The valid entries are: • **System**: The system-wide values apply. This is the default value. • **Yes**: Removes 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. • **No**: Excludes ACW agents for the queue.
Localized Display Name	The name associated with the agent login ID
Attribute	The attribute associated with the agent login ID.
Percent Allocation	The percentage for each of the agent's skills if the call handling preference is percent-allocation. Valid entry is a number from **1** to **100** for each skill. Entries for all the agent skills together must add up to 100%. Do not use target allocations for reserve skills. Percent Allocation is available as part of the Avaya Business Advocate software.
Password	The password the agent must enter upon login. Displayed only if both the AAS and AUDIX check boxes are clear. Valid entries are digits from **0** through **9**. Enter the minimum number of digits in this field specified by the Minimum Agent-LoginID Password Length field on the Feature-Related System Parameters screen. By default, this field is blank.
Confirm Password	Confirms the password the Agent entered in the Password field during login. Displayed only if both the AAS and the AUDIX check boxes are clear. By default, this field is blank. **Note:** Values entered in this field are not echoed to the screen.

Table continues…

Field	Description
Port Extension	The assigned extension for the AAS or AUDIX port. The values are displayed only if either the AAS or AUDIX check box is selected. This extension cannot be a VDN or an Agent LoginID. By default, this field is blank
Reserve Level	The reserve level to be assigned to the agent for the skill with the Business Advocate Service Level Supervisor feature or the type of interruption with the Interruptible AUX Work feature. You can assign a reserve level of `1` or `2` or an interruptible level of `a`, `m`, `n`, or blank for no reserve or interruptible level, where, • `a`: auto-in-interrupt • `m`: manual-in-interrupt • `n`: notify-interrupt Changes to this field take effect the next time the agent logs in. Values of 1 and 2 are allowed only if Business Advocate is enabled. A skill level cannot be assigned with a reserve level setting. Reserve level set to `1` or `2` defines the EWT threshold level for the agent to be added to the assigned skill as a reserve agent. When the EWT for this skill reaches the corresponding threshold set on the Hunt Group screen, agents automatically get this skill added to their logged in skills. Agents are delivered calls from this skill until the skill's EWT drops below the assigned overload threshold for that level. The Interruptible Aux feature is a way to help meet service level targets by requesting agents who are on break to become available when the service level target is not being met. For more information on Service Level Supervisor, see *Avaya Business Advocate User Guide*.
Service Objective	The option to administer Service Objective. Service Objective is administered on the Hunt Group screen and the agent LoginID screen. This field is displayed only when Call Handling Preference is set to greatest-need or skill-level. The communication 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 part of the Avaya Business Advocate software.

Table continues…

Field	Description
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.
Skill Number	The Skill Hunt Groups that an agent handles. The same skill may not be entered twice. You have the following options: • If EAS-PHD is not optioned, enter up to four skills. • If EAS-PHD is optioned, enter up to 20 or 60 skills depending on the platform. **Important:** Assigning a large number of skills to agents can potentially impact system performance. Review system designs with the ATAC when a significant number of agents have greater than 20 skills per agent.
Skill Level	A skill level for each of an agent's assigned skills. If you specify the EAS-PHD option, 16 priority levels are available. If you do not specify this option, two priority levels are available.
Tenant Number	The tenant partition number. Valid entries range from **1** to **100**. The default is entry is **1**. **Note:** Values entered in this field are not echoed to the screen.

Button	Description
Commit	Completes the action you initiate.
Clear	Clears all entries.
Done	Completes your current action and takes you to the subsequent page.
Cancel	Cancels your current action and takes you to the previous page.

Subscriber Messaging Templates field descriptions

Field	Description
Template name	The template of this subscriber template.
Type	The messaging type of the subscriber template.
Software Version	The software version of the element for the template.

Basic Information

Field	Description
Last Name	The last name of the subscriber.
First Name	The first name of the subscriber.
PBX Extension	A number whose length can range from three digits to 10 digits, that the subscriber will use to log on to the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local computer.
Password	The default password that users must use to log on to their mailbox. The password must be from 3 to 15 digits and adhere to system policies that you set on the Avaya Aura® Messaging server.
Class Of Service Name	The Class Of Service (CoS) name for this subscriber. CoS controls subscriber access to many features and provides general settings, such as mailbox size. The value that you select must be available in the messaging system.
Community ID	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.

Subscriber Directory

Field	Description
Telephone Number	The name that the system displays before the computer name and domain in the subscriber's email address.

Table continues…

Field	Description
Common Name	The display name of the subscriber.
ASCII version of name	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
Personal Operator Mailbox	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.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	The order in which the subscriber hears the voice messages. The options are: • **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.
Intercom Paging	The intercom paging settings for a subscriber. The options are: • **paging is off**: To disable intercom paging for this subscriber. • **paging is manual**: If the subscriber can modify, with Subscriber Options or the TUI, callers can page the subscriber. • **paging is automatic**: If the TUI automatically allows callers to page the subscriber.

Table continues…

Field	Description
VoiceMail Enabled	Specifies whether a subscriber can receive messages, email messages, and call-answer messages from other subscribers. The options are: • **yes**: use this 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.

Secondary Extensions

Field	Description
Secondary extension	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
Miscellaneous1	Gives additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous2	Gives additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous3	Gives additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.
Miscellaneous4	Gives additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber template.
Reset or **Clear**	Undoes all the changes.
Edit	Allows you to edit the fields.
Done	Completes your action and takes you to the previous page.
Cancel	Takes you to the previous page.
Schedule	Performs the action at the chosen time.

Subscriber CMM Templates field descriptions

Field	Description
Template name	The template of this subscriber template.
New Template Name	The name of the duplicate template. You can enter the name of your choice.
Type	The messaging type of the subscriber template.
Software Version	The software version of the element for the template.

Basic Information

Field	Description
Last Name	The last name of the subscriber.
First Name	The first name of the subscriber.
Extension	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: • Be within the range of Extension Numbers assigned to your system. • Not be assigned to another local subscriber. • Be a valid length on the local computer.
Password	The default password that a user has to use to login to his or her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank
Class Of Service ID	The class of service (CoS) ID for this subscriber. CoS controls subscriber access to many features and provides general settings, such as mailbox size. The value that you select must be available in the messaging system.
Community ID	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.
MWI Enabled	The option to set the message waiting indicator (MWI) for the subscriber. The options are: • **No**: If the system must not send MWI for the subscriber or if the subscriber does not have a phone or switch on the network. • **Yes**: If the system must send MWI for the subscriber.

Table continues…

Field	Description
Account Code	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
Email Handle	The name that the system displays before the computer name and domain in the subscriber's email address.
Common Name	The display name of the subscriber.

Mailbox Features

Field	Description
Covering Extension	The number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits depending on the length of the system extension, or leave this field blank.

Secondary Extensions

Field	Description
Secondary extension	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
Misc 1	Additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the Messaging system.
Misc 2	Additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the Messaging system.
Misc 3	Additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the Messaging system.
Misc 4	Additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the Messaging system.

Button	Description
Commit	Adds the subscriber template.
Reset or **Clear**	Undoes all changes.
Edit	Allows you to edit the fields.
Done	Completes the action and takes you to the previous page.
Cancel	Returns to the previous page.

Subscriber MM Templates field descriptions

Field	Description
Type	The messaging type of the subscriber template.
New Template Name	The name of the duplicate template. You can enter the name of your choice.
Template name	The messaging template of a subscriber template.
Software Version	The software version of the element for the template.

Basic Information

Field	Description
Last Name	The last name of the subscriber.
First Name	The first name of the subscriber.
Numeric Address	A unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.
PBX Extension	The primary telephone extension of the subscriber.
Class Of Service ID	The class of service (CoS) ID for this subscriber. CoS controls subscriber access to many features and provides general settings, such as mailbox size. The value that you select must be available in the messaging system.
Community ID	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.
Password	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
Email Handle	The name that the system displays before the computer name and domain in the subscriber's e-mail address. The computer name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.
Telephone Number	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 (]).
Common Name	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.
ASCII Version of Name	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
Backup Operator Mailbox	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.
Personal Operator Schedule	Specifies when to route calls to the backup operator mailbox. The default value for this field is **Always Active**.
TUI Message Order	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

Table continues…

Field	Description
	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.
Intercom Paging	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, callers can page the subscriber. • **paging is automatic**: if the TUI automatically allows callers to page the subscriber.
Voicemail Enabled	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**: use this 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.

Secondary Extensions

Field	Description
Secondary extension	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
Misc 1	Gives additional, useful information about a subscriber template. Entries in this field are for

Table continues…

Field	Description
	convenience and are not used by the messaging system.
Misc 2	Gives additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 3	Gives additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.
Misc 4	Gives additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system.

Button	Description
Commit	Adds the subscriber template.
Reset	Undoes all the changes.
Edit	Allows you to edit the fields.
Done	Completes your action and takes you to the previous page.
Cancel	Takes you to the previous page.

Managing IP Office Endpoint template

Adding an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office Endpoint**.
3. Click **New**.
4. Enter the required information in the **Name**, **System Type**, **Set Type**, and **Version** fields.
5. Click **Details**.

   The system launches the IP Office Manager application.
6. On the IP Office Manager window, in the right pane, specify the required details, such as voice mail, telephony, and button programming in the respective tabs.

7. Click **File** > **Save Template and Exit** to save the template configuration and exit the IP Office application.

   The system directs you to the landing page of **IP Office Endpoint**.

   You can view the newly created template in the list of templates under IP Office endpoint templates.

   When you upgrade System Manager, Default Centralized ATA Template, Default Centralized SIP Template are now available to create centralized users.

Related links

IP Office endpoint template field descriptions on page 1059

Viewing an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office Endpoint**.
3. Select a type of system from the list of IP Office supported templates.
4. Click **Show List**.
5. Under **IP Office Endpoint Templates**, select the template you want to view from the list of templates.
6. Click **View**.

   This action launches the IP Office Manager application.
7. On the IP Office Manager window, click the tabs on the right pane to view the template details.
8. Click **File** > **Exit** to exit the IP Office Manager application.

   The system displays the **IP Office Endpoint** landing page.

Related links

IP Office endpoint template field descriptions on page 1059

Editing an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office Endpoint**.
3. Select a type of system from the list of IP Office supported templates.
4. Click **Show List**.

5. From the list of **IP Office Endpoint Templates**, select the template you want to edit.
6. Click **Edit**.

   This system launches the IP Office application.
7. On the IP Office Manager window, in the right pane, edit the required details.
8. Click **File** > **Save Template and Exit** to save the modifications to the template and exit the IP Office Manager application.

   The system displays the IP Office Endpoint landing page.

Related links

IP Office endpoint template field descriptions on page 1059

Duplicating an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office Endpoint**.
3. Select a system type from the list of IP Office supported templates.
4. Click **Show List**.
5. From the list of IP Office endpoint templates, select the template you want to duplicate.
6. Click **Duplicate**.
7. Type a template name in the **New Template Name** field.
8. Click **Commit**.

   If you want to make changes to the new endpoint template, click **Details**.

Related links

IP Office endpoint template field descriptions on page 1059

Deleting an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office Endpoint**.
3. Select a type of system from the list of IP Office supported templates.
4. Click **Show List**.
5. From the **IP Office Endpoint Templates** list, select the template you want to delete.
6. Click **Delete**.

The system displays the template instance you selected for deletion.

7. Perform one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation and return to the **IP Office Endpoint** landing page.

Upgrading IP Office endpoint templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office Endpoint**.
3. Select the IP Office device type.
4. Click **Show List**.
5. Select the template you want to upgrade.
6. Click **Upgrade**.
7. In the **Supported IP Office Versions** field, enter the target version for upgrade.
8. In **Template Name**, type the name of the template.

   Template name must be a unique name.
9. Click **Upgrade**.

   System Manager upgrades the selected template, and the IP Office Manager starts with the upgraded template. The original template you selected is retained.
10. After the IP Office Manager starts, the new, upgraded template, save and exit.

    The system displays the upgraded template in the IP Office Endpoint List page.

IP Office endpoint template field descriptions

Name	Description
Name	The name of the IP Office endpoint template.
System Type	The type of system associated with the IP Office device. The valid options are: • **IP Office**: for IP Office core unit • **B5800**: for B5800 core unit
Version	The version of the IP Office endpoint template.

Table continues…

Name	Description
Set Type	The set type associated with the IP Office endpoint template. This is a drop-down field listing the following set types: • **ANALOG** • **SIP** • **IPDECT** • **DIGITAL** • **H323** • **SIP DECT** Only IP Office devices support the **SIP DECT** set type.
Last Modified Time	The date and time when you last modified the template.

Button	Description
Details	Click to open the IP Office application to add or edit the template details.

Managing IP Office System Configuration template

Adding an IP Office System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office System Configuration**.
3. Click **New**.
4. Complete the **Name**, **System Type**, and **Version** fields.
5. Click **Details**.

   The system launches the IP Office application.
6. On the Offline Configuration Creation window, click **OK**.
7. In the right pane, complete the system configuration template by filling the required fields, and click **OK**.
8. Click **File** > **Save Template and Exit** to save the template specifications and exit theIP Office application.

The system directs you to the IP Office System Configuration landing page where you can view the newly created system template in the IP Office System Configuration list.

Viewing an IP Office System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office System Configuration**.
3. On the IP Office Branch Gateway Template page, from the IP Office supported templates list, select an IP Office system type.
4. Click **Show List**.
5. Select the system configuration template you want to view from the IP Office System Configuration list.
6. Click **View**.

   The system launches the IP Office Manager application.
7. On the IP Office Manager window, in the right pane, you can view the system configuration template details. All the fields are read-only.
8. Click **File** > **Exit** to exit IP Office Manager.

   The system directs you to the IP Office System Configuration landing page.

Editing an IP Office system configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office System Configuration**.
3. On the IP Office System Configuration Templates page, select an IP Office system type.
4. Click **Show List**.
5. Select the system configuration template you want to edit from the IP Office System Configuration list.
6. Click **Edit**.

   The system launches the IP Office Manager application.
7. On the IP Office Manager window, edit the required configuration parameters, and click **OK**.
8. Click **File** > **Save Template and Exit** to save the modifications to the system configuration template and exit theIP Office Manager application.

   The system displays the IP Office System Configuration landing page.

Deleting an IP Office system configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office System Configuration**.
3. On the IP Office Template page, select a IP Office system type.
4. Click **Show List**.
5. Select the system configuration template you want to delete from the IP Office System Configuration list.
6. Click **Delete**.

   The system displays the system template instance you selected for deletion.
7. Do one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation, and return to the IP Office System Configuration landing page.

Applying an IP Office system configuration template on an IP Office device

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office System Configuration**.
3. On the IP Office Template page, select an IP Office system type.
4. Click **Show List**.
5. From the IP Office System Configuration List, select the system template you want to apply to an IP Office device.
6. Click **Apply**.

   You will be directed to a new page where you can select a device to apply the template.
7. From the list of IP Office devices, select the IP Office device on which you want to apply the selected IP Office system configuration template.

   Important:

   When you apply a template on a device, the data of the template that you wish to apply may override the existing system configuration data on the device.

8. Do one of the following:
    - Click **Now** to perform apply the template immediately.
    - Click **Schedule** to apply the template at a specified time in **Scheduler**.
    - Click **Cancel** to cancel this task and return to the IP Office System Configuration landing page.

IP Office System Configuration template field descriptions

Name	Description
Name	The name of the IP Office System Configuration template.
System Type	The type of system associated with the template. The options are: • **IP Office**: for IP Office core unit • **B5800**: for B5800 core unit
Version	The version number of the template.
Last Modified Time	The date and time when the IP Office System Configuration template was last modified.

Button	Description
Details	Displays the IP Office application where you can add or edit the template details.

Manage audio files

Audio files in .WAV and .C11 formats are used in auto attendant configuration in the Auto Attendant feature in IP Office. In System Manager, you can manage .WAV and .C11 audio files from the Manage Audio page in IP Office System Configuration in Template Management. The .C11 audio file is for use in IP Office IP500V2 or the B5800 Core Unit.

To push an auto attendant file to a IP Office System Configuration template through System Manager, you must first upload the .WAV audio files using the **Upload** button in the Manage Audio page. When you upload the .WAV audio files, the corresponding .C11 audio files are automatically created. If you need to convert any .WAV audio file which does not have a corresponding .C11 audio file, or if the corresponding .C11 audio file is deleted, click the **Convert** button in the Manage Audio page.

Use the **Manage Audio** page in **IP Office System Configuration** to:

- Upload .WAV and .C11 audio files.
- Convert .WAV to .C11 audio file format.

- Delete .WAV and .C11 audio files.

Uploading an audio file

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office System Configuration**.
3. Click **More Options** > **Manage Audio**.
4. On the Manage Audio page, enter the complete path of the audio file in the **Select an Audio File** text box. You can also click **Browse** to locate and select the audio file you want to upload.

   The system displays the audio file you selected for uploading in a table.
5. If you want to remove the audio file from your selection, click the **Remove** link in the **Action** column.
6. Click **Upload**.

   You can view the newly uploaded audio files listed in the **List of Audio Files** table.

Converting an .WAV audio file to a .C11 audio file

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office System Configuration**.
3. Click **More Options** > **Manage Audio**.
4. On the Manage Audio page, select the .WAV audio file from the **List of Audio Files** that you want to convert to .C11 format.
5. On the Convert Audio page, the system lists the file you selected for conversion.
6. If you want to change the recording label of the .WAV file, edit the label text in the corresponding text box under the **Recording Label** column.
7. Click **Commit** to confirm the convert action.

   The system displays the newly converted audio file under the corresponding audio name column in the **List of Audio Files** table.

Deleting an audio file

About this task

Use the **Delete** button to delete audio files from the list of audio files. You can choose to either delete the .WAV audio format, or the .C11 audio file format, or delete both the audio file formats in a single step.

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **IP Office System Configuration**.
3. Click **More Options** > **Manage Audio**.
4. On the Manage Audio page, select the audio file you want to delete from the list of audio files.
5. Click **Delete**.
6. On the Delete Audio File Confirmation page, you can view the audio files you selected in Step 4 for deletion. From the **Select the type of deletion** field perform one of the following:

   - Select the type of audio file extension you want to delete.
   - Select **Both** if you want to delete both the file extension types.

   Sample scenario: Suppose you have ABC.wav and ABC.c11 audio files in the **List of Audio Files**. If you want to delete only the ABC.wav audio file, then select **Wave** from **Select the type of deletion**. If you want to delete both the audio files in a single step, then select **Both** from the **Select the type of deletion** field.
7. Click **Delete**.
8. Click **Done** to return to the IP Office System Configuration landing page.

Manage Audio field descriptions

Name	Description
wav Audio File Name	The file name of the .WAV type of audio file.
Last uploaded time of wav	The time when you last uploaded the .WAV audio file in the system.
Recording Label	The recording label of the .wav file.
C11 Audio File Name	The file name of the .C11 type of audio file.
Last converted time of wav to C11	The time when you last converted a .wav file to a .C11 audio file.
Select an Audio File	Displays the complete path of the audio file.

Table continues…

Name	Description
Select the type of deletion on the Delete Audio File Confirmation page	Provides the option to select the type of deletion of audio files. The valid options are: • **Wave**: Select to delete only the .WAV type of file for the selected audio file. • **C11**: Select to delete only the .C11 type of file for the selected audio file. • **Both**: Select to delete both, .WAV and .C11, types of files for the selected audio file.

Button	Description
Delete	Click to delete the selected audio file.
Convert	Click to convert an audio file of type .WAV to .C11.
Done	Click to exits the **Manage Audio** page and return to the IP Office Template List page.
Browse	Click to locate and select an audio file.
Upload	Click to upload an audio file to System Manager.
Delete on the Delete Audio File Confirmation page	Click to confirm the delete action for the selected audio file.
Cancel on the Delete Audio File Confirmation page	Click to cancel the delete operation and return to the **Manage Audio** page.

Managing UCM and Application Server system configuration templates

Adding a UCM and Application Server Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, in the **Templates List** section, click **New**.
4. Complete the **Name**, **System Type**, and **Version** fields.
5. Click **Details**.

   The system launches the IP Office Manager application.
6. On the Offline Configuration Creation window, click **OK**.

7. In the right pane, complete the system configuration template by filling the required fields, and click **OK**.
8. Click **File** > **Save Template and Exit** to save the template specifications and exit the IP Office Manager application.

   The system directs you to the UCM and Application Server Templates landing page where you can view the newly created system template in the **UCM and Application Server Templates** list.

Related links

UCM and Application Server Templates field descriptions on page 1070

Viewing a UCM and Application Server Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, in the **Supported System Types** section, select one of the following system types:
   - IP Office Application Server
   - Unified Communications Module
4. Click **Show List**.
5. Select the system configuration template you want to view from the **UCM and Application Server Templates** list.
6. Click **View**.

   On the IP Office Manager window, in the right pane, you can view the system configuration template details. All the fields are read-only.

   The system starts the IP Office Manager application.
7. Click **File** > **Exit** to exit IP Office Manager.

   The system displays the UCM and Application Server Templates page where you can select a device to apply the template.

Related links

UCM and Application Server Templates field descriptions on page 1070

Editing a UCM and Application Server Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.

2. In the left navigation page, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, In the **Supported System Types** section, select an one of the following system types:
   - IP Office Application Server
   - Unified Communications Module
4. Click **Show List**.
5. Select the system configuration template you want to edit from the UCM and Application Server Templates list.
6. Click **Edit**.

   The system launches the IP Office Manager application.
7. On the IP Office Manager window, edit the required configuration parameters, and click **OK**.
8. Click **File** > **Save Template and Exit** to save the modifications to the system configuration template and exit the IP Office Manager application.

   The system displays the UCM and Application Server Templates landing page.

Related links

UCM and Application Server Templates field descriptions on page 1070

Deleting a UCM and Application Server Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, In the **Supported System Types** section, select one of the following system types:
   - IP Office Application Server
   - Unified Communications Module
4. Click **Show List**.
5. Select the system configuration template you want to delete from the UCM and Application Server Templates list.
6. Click **Delete**.

   The system displays the system template instance you selected for deletion.
7. Do one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation, and return to the UCM and Application Server Templates landing page.

Related links

UCM and Application Server Templates field descriptions on page 1070

Applying a UCM and Application Server Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, In the **Supported System Types** section, select one of the following system types:
    - IP Office Application Server
    - Unified Communications Module
4. Click **Show List**.
5. From the UCM and Application Server Configuration List, select the system template you want to apply to a device.
6. Click **Apply**.

    You will be directed to a new page where you can select a device to apply the template.
7. From the list of IP Office devices, select the IP Office device on which you want to apply the selected UCM and Application Server Configuration template.

    > **Important:**
    >
    > When you apply a template on a device, the data of the template that you wish to apply may override the existing system configuration data on the device.
8. Do one of the following:
    - Click **Now** to perform apply the template immediately.
    - Click **Schedule** to apply the template at a specified time in **Scheduler**.
    - Click **Cancel** to cancel this task and return to the UCM and Application Server Templates landing page.

Related links

UCM and Application Server Templates field descriptions on page 1070

UCM and Application Server Templates field descriptions

Name	Description
Name	The name of the system configuration template of UCM and Application Server.
System Type	The type of system associated with the template. The options are: • **Unified Communications Module**: For UCM core unit • **Application Server**: For Application Server core unit
Version	The version number of the template.
Last Modified Time	The date and time when the UCM and Application Server System Configuration template was last modified.

Button	Description
Details	Displays the application where you can add or edit the template details.

Managing VMPro system configuration templates

Adding a VMPro System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.
3. Click **New**.
4. Complete the **Name** and **Version** fields.
5. Click **Details**.

   The system launches the **VMPro** application.
6. In the right pane, complete the system configuration template by filling the required fields, and click **Update**.
7. Click **Save and Exit** to save the template specifications and exit the **VMPro** application.

The system displays the VMPro System Configuration page where you can view the newly created system configuration template.

Related links

VMPro System Configuration Templates field descriptions on page 1074

Viewing a VMPro System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.
3. On the VMPro Template page, from the **VMPro** supported templates list, select an **VMPro** system type.
4. Click **Show List**.
5. Select the system configuration template you want to view from the **VMPro** System Configuration list.
6. Click **View**.

   The system launches the **VMPro** application.
7. On the VMPro window, in the right pane, you can view the system configuration template details. All the fields are read-only.

Related links

VMPro System Configuration Templates field descriptions on page 1074

Editing a VMPro System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.
3. On the VMPro System Configuration Templates page, select a VoicemailPro system type.
4. Click **Show List**.
5. Select the system configuration template you want to edit from the VMPro System Configuration list.
6. Click **Edit**.

   The system launches the VMPro application.
7. To edit the configuration parameters on the Voicemail Pro-System Preferences window, click **Update** .

8. Click **OK**.
9. Click **File** > **Save and Exit** to save the modifications to the system configuration template and exit the VMPro application.

   The system displays the VMPro System Configuration Template page.

Related links

VMPro System Configuration Templates field descriptions on page 1074

Deleting a VMPro System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.
3. On the VMPro System Configuration Templates page, select a **VMPro** system type.
4. Click **Show List**.
5. Select the system configuration template you want to delete from the VMPro System Configuration Template list.
6. Click **Delete**.

   The system displays the system template instance you selected for deletion.
7. Do one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation, and return to the VMPro System Configuration Template landing page.

Related links

VMPro System Configuration Templates field descriptions on page 1074

Applying a VMPro System Configuration template on a device

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Templates**.
3. On the VMPro System Configuration Template page, select a Voicemail Pro system type.
4. Click **Show List**.
5. From the VMPro System Configuration Templates List, select the system template you want to apply to a VMPro device.
6. Click **Apply**.

The system displays the VMPro System Configuration page where you can select a device to apply the template.

7. From the list of VMPro devices, select the VMPro device on which you want to apply the VMPro system configuration template.

   Important:

   When you apply a template on a device, the data of the template that you apply might override the existing system configuration data on the device.

8. Do one of the following:
   - Click **Now** to perform apply the template immediately.
   - Click **Schedule** to apply the template at a specified time in **Scheduler**.
   - Click **Cancel** to cancel this task and return to the VMPro System Configuration Template landing page.

Related links

VMPro System Configuration Templates field descriptions on page 1074

Duplicating a VMPro System Configuration template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.
3. On the VMPro System Configuration Templates page, select a VoicemailPro system type.
4. Click **Show List**.
5. From the VMPro System Configuration list, select the system configuration template that you want to duplicate .
6. Click **Duplicate**.

   The system launches the VMPro application.
7. In the **New Template Name** field, type the name of the new template.
8. Click **Commit**.

   The system displays the new template on the VMPro System Configuration Templates page.

Related links

VMPro System Configuration Templates field descriptions on page 1074

VMPro System Configuration Templates field descriptions

Name	Description
Name	The name of the Voicemail Pro template.
Version	The version number of the template.
Last Modified Time	The date and time when the IP Office Voicemail Pro template was last modified.

Button	Description
Details	Displays the IP Office Voicemail Pro application where you can add or edit the template details.

Managing VMPro call flow templates

Adding a VMPro Call Flow template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. Click **New**.
4. Complete the **Name** and **Version** fields.
5. Click **Details**.

   The system launches the **VMPro** application.
6. In the right pane, complete the call flow template by filling the required fields, and click **Update**.
7. Click **Save and Exit** to save the template specifications and exit the **VMPro** application.

Result

The system displays the VMPro Call Flow page where you can view the newly created call flow template.

Related links

VMPro Call Flow Templates field descriptions on page 1077

Viewing a VMPro Call Flow template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. On the VMPro Template page, from the **VMPro** supported templates list, select the **VMPro** system type.
4. Click **Show List**.
5. Select the system configuration template you want to view from the **VMPro** call flow list.
6. Click **View**.

Result

The system launches the **VMPro** application. On the VMPro window, in the right pane, you can view the call flow template details. All the fields are read-only.

Related links

VMPro Call Flow Templates field descriptions on page 1077

Editing a VMPro Call Flow template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. On the VMPro Call Flow Templates page, select a VoicemailPro system type.
4. Click **Show List**.
5. Select the call flow template you want to edit from the VMPro Call Flow list.
6. Click **Edit**.

   The system launches the VMPro application.
7. To edit the call flow parameters on the Voicemail Pro-System Preferences window, click **Update** .
8. Click **OK**.
9. Click **File** > **Save and Exit** to save the modifications to the call flow template and exit the VMPro application.

Result

The system displays the VMPro Call Flow Templates page.

Related links

VMPro Call Flow Templates field descriptions on page 1077

Deleting a VMPro Call Flow template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. On the VMPro Call Flow Templates page, select a **VMPro** system type.
4. Click **Show List**.
5. Select the call flow template you want to delete from the VMPro Call Flow Templates list.
6. Click **Delete**.

   The system displays the VMPro call flow template that you selected for deletion.
7. Do one of the following:
   - Click **Delete** to delete the template.
   - Click **Cancel** to cancel the delete operation, and return to the VMPro Call Flow Templates page.

Related links

VMPro Call Flow Templates field descriptions on page 1077

Applying a VMPro Call Flow template on a device

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro Call Flow Templates**.
3. On the VMPro Call Flow Templates page, select the Voicemail Pro system type.
4. Click **Show List**.
5. From the VMPro Call Flow Templates List, select the system template you want to apply to a VMPro device.
6. Click **Apply**.

   The system displays the VMPro Call Flow page where you can select a device to apply the template.
7. From the list of VMPro devices, select the VMPro device on which you want to apply the VMPro call flow template.

Important:

When you apply a template on a device, the data of the template that you apply might override the call flow data on the device.

8. Do one of the following:
   - Click **Now** to apply the template immediately.
   - Click **Schedule** to apply the template at a specified time in **Scheduler**.
   - Click **Cancel** to cancel the task and return to the VMPro Call Flow Templates page.

Related links

VMPro Call Flow Templates field descriptions on page 1077

Duplicating a VMPro Call Flow template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. On the VMPro Call Flow Templates page, select a VoicemailPro system type.
4. Click **Show List**.
5. From the VMPro Call Flow list, select the call flow template that you want to duplicate.
6. Click **Duplicate**.

   The system launches the VMPro application.
7. In the **New Template Name** field, type the name of the new template.
8. Click **Commit**.

Result

The system displays the new template on the VMPro Call Flow Templates page.

Related links

VMPro Call Flow Templates field descriptions on page 1077

VMPro Call Flow Templates field descriptions

Name	Description
Name	The name of the Voicemail Pro template.
Version	The version number of the template.
Last modified time	The last time that the IP Office Voicemail Pro template was modified.

Button	Description
Details	Displays the template details of the IP Office Voicemail Pro application.

Chapter 22: Security

Managing certificates

Trust Management

System Manager uses Trust Management to provision and manage certificates of various applications, servers, and devices for a secure, interelement communication. Trust Management provides Identity (Server) and Trusted (Root/CA) certificates that applications can use to establish mutually authenticated Transport Layer Security (TLS) sessions.

System Manager uses a third-party open source application, Enterprise Java Beans Certificate Authority (EJBCA), as a Certificate Authority for certificate management.

From Manage Elements, you can manage certificates for System Manager and the elements that System Manager supports.

Related links

Certificate Authorities on page 1093

Certificate generation and certificate management capabilities in System Manager

The table provides the major certificate generation and certificate management capabilities that System Manager offers. System Manager manages certificates for System Manager and elements that System Manager manages.

All communications between the client and the servers in the Avaya Aura® environment are secured using the Transport Layer Security (TLS) protocol. In TLS, servers are configured with an identity certificate issued by a certificate authority. When clients connect to servers, the server presents its identity certificate for the client to validate. The client checks whether the server identity certificate was issued by a certificate authority that the client trusts. If the validation succeeds, a secure connection is established.

#	Use case	Example	With System Manager CA as Root CA Default mode	With System Manager CA as SubCA	With third-party CA signed identity certificates
1	New certificate generation by using the System Manager Trust Management page	Request from a product that is integrated with System Manager for certificates during installation. For example, Session Manager.	✓	✓	Not applicable
2	New certificate generation by using the SCEP client	Request for certificates during the installation or registration of devices or endpoints that hosts an SCEP client. For example, B5800.	✓	✓	Not applicable
3	New certificate generation by System Manager	Generating certificates manually to install the certificates on remote instances of various products or endpoints.	✓	✓	Not applicable
4	New certificate generation by System Manager web console by using a standard Certificate Signing Request (CSR)	Generating certificates manually to install the certificates on remote instances of products that want to generate the keys on product and require System Manager CA to sign the certificates.	✓	✓	Not applicable
5	Installing a new identity certificate issued by a third-party CA	Configuring the System Manager web interface to use a certificate issued by a well-known CA, for	✓	✓	✓

Table continues…

#	Use case	Example	With System Manager CA as Root CA Default mode	With System Manager CA as SubCA	With third-party CA signed identity certificates
		example, VeriSign, instead of a certificate issued by own CA.			
6	Replacing an identity certificate issued by the System Manager CA with a new certificate issued by System Manager CA	Installing a new certificate with changed values. For example, new FQDN and new IP address.	✓	✓	Not applicable
7	Replacing an identity certificate issued by the System Manager CA with a new certificate issued by a third-party CA	Configuring the System Manager web interface to use a certificate issued by a well-known CA, for example, VeriSign, instead of a certificate issued by own CA. This applies for products that use System Manager for administration. For example, Session Manager and CS 1000.	✓	✓	✓
8	Replacing an existing identity certificate issued by a third-party CA with a new certificate issued by System Manager CA	Reverting System Manager, Session Manager, and CS 1000 that use third-party identity certificates to use certificates issued by the System Manager CA.	✓	✓	✓
9	Renewal of an existing identity certificate	Manual or automatic renewing of a certificate that is about to expire.	✓	✓	X

Table continues…

#	Use case	Example	With System Manager CA as Root CA Default mode	With System Manager CA as SubCA	With third-party CA signed identity certificates
		This capability is also available for products such as Session Manager.			
10	Exporting an identity certificate to a PEM certificate file	Exporting any identity certificate to a standard PEM format files so that the certificate can be manually imported to the trust stores of various products.	✓	✓	✓
11	Adding new certificates to the truststore of the product.	Installing a new certificate to the truststores of the product, such as Session Manager.	✓	✓	✓
12	Removing existing certificates from the truststore of the product	Deleting a certificate, for example, SIPCA root certificate, from the truststores of the product such as Session Manager.	✓	✓	✓
13	Installing a new identity certificate issued by a third-party CA on Session Manager	Configuring the System Manager web interface to use a certificate issued by a third-party CA on Session Manager for SIP communication.	✓	✓	✓

The certificate that is used to assert its identity is called a product certificate or an identity certificate. The issuer or CA certificate used to verify and validate the identity of the far end is referred to as the trusted certificate or root CA certificate. Trusted certificates are typically used to make secure connections to a server over the Internet.

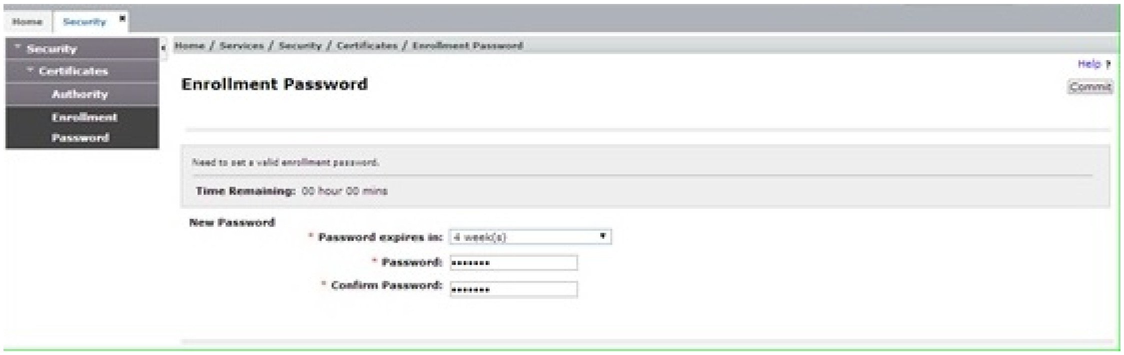
Setting the enrollment password

About this task

You can use this functionality to generate the enrollment password for managed elements. The managed elements require the enrollment password to request certificates from System Manager Trust Management.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Enrollment Password**.
3. On the Enrollment Password page, in the **Password expires in** field, select a password expiration time in hours, days, or weeks.



Enrollment Password

Need to set a valid enrollment password.

Time Remaining: 00 hour 00 mins

New Password

* Password expires in: 4 week(s)

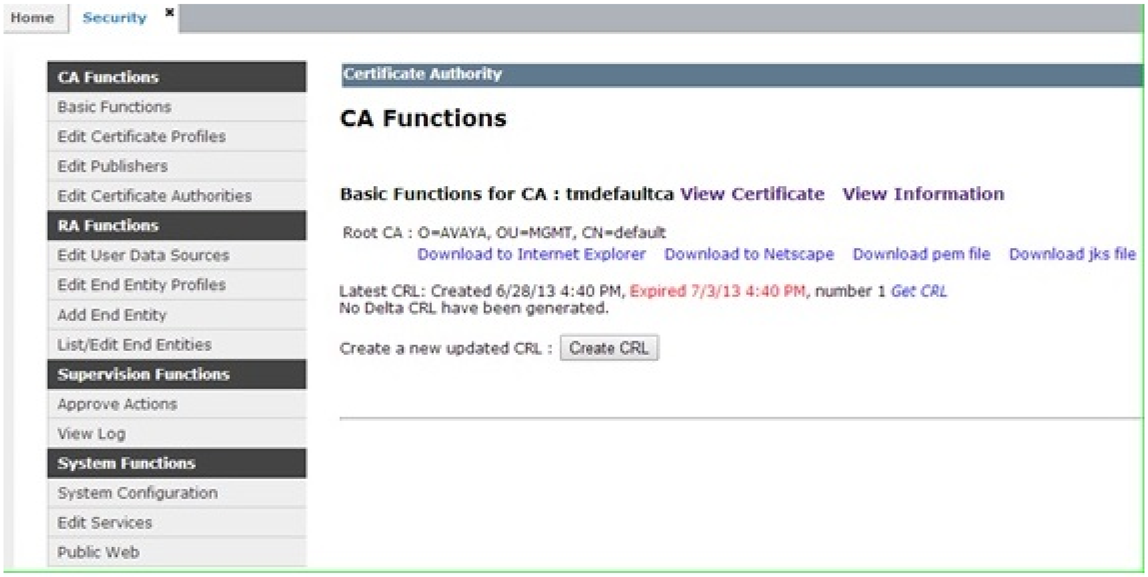
* Password: •••••••

* Confirm Password: •••••••

4. In **Password** and **Confirm Password** fields, enter the password.
5. Click **Commit**.

   The system updates the time displayed in the Time remaining section with the value that you selected in **Password expires in**.
6. Note the password for future reference.

   The Authority link is used for launching EJBCA administration. A customer can configure the settings here, based on its PKI plan.



CA Functions

Basic Functions for CA : tmdefaultca View Certificate View Information

Root CA : O=AVAYA, OU=MGMT, CN=default
Download to Internet Explorer Download to Netscape Download pem file Download jks file

Latest CRL: Created 6/28/13 4:40 PM, Expired 7/3/13 4:40 PM, number 1 Get CRL
No Delta CRL have been generated.

Create a new updated CRL : Create CRL

Related links

Enrollment Password field descriptions on page 1093

Managing trusted certificates

Obtaining the SSL certificate for Microsoft Active Directory

Procedure

1. Install the certification authority (CA) on your Microsoft Active Directory server. For detailed instructions to configure an SSL certificate for Microsoft Active Directory, see https://confluence.atlassian.com/display/ALLDOC/Atlassian+Documentation.
2. Run the following command on the Microsoft Active Directory server to export the certificate:

```
certutil  -ca.cert  client.crt
```

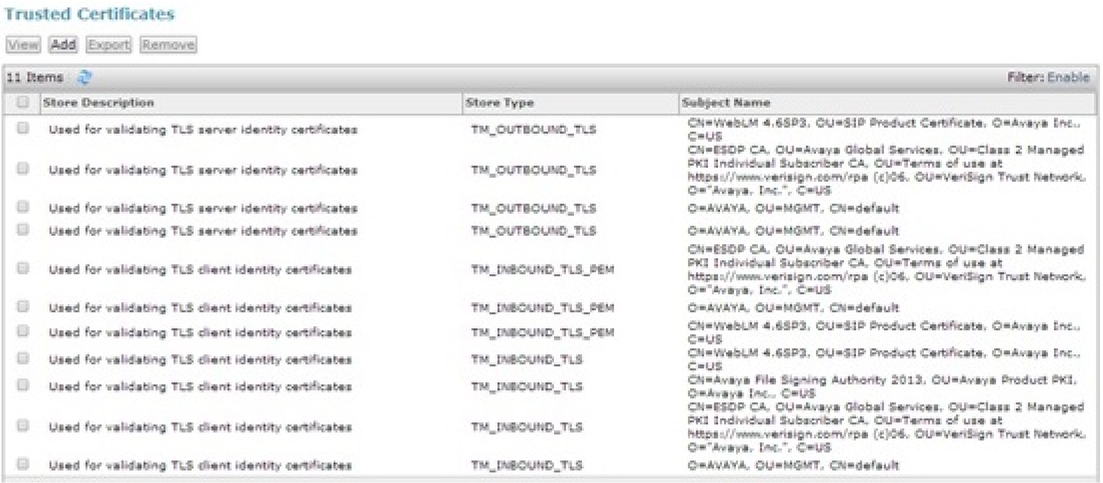
3. Copy the `client.crt` file from the Microsoft Active Directory server to your computer.

Next steps

- Import the certificate for Microsoft Active Directory server to System Manager

  For instructions, see Adding trusted certificates.
- On the Manage Elements page, click **More Option** > **Configure Trusted Certificate**.

  The system displays the Trusted Certificate Management page, and lists all Trusted Certificates that apply to all interfaces requiring certificate authentication.



□	Store Description	Store Type	Subject Name
□	Used for validating TLS server identity certificates	TM_OUTBOUND_TLS	CN=WebLM 4.6SP3, OU=SIP Product Certificate, O=Avaya Inc., C=US
□	Used for validating TLS server identity certificates	TM_OUTBOUND_TLS	CN=ESDP CA, OU=Avaya Global Services, OU=Class 2 Managed PKI Individual Subscriber CA, OU=Terms of use at https://www.verisign.com/rpa (c)06, OU=VeriSign Trust Network, O="Avaya, Inc.", C=US
□	Used for validating TLS server identity certificates	TM_OUTBOUND_TLS	O=AVAYA, OU=MGMT, CN=default
□	Used for validating TLS server identity certificates	TM_OUTBOUND_TLS	O=AVAYA, OU=MGMT, CN=default
□	Used for validating TLS client identity certificates	TM_INBOUND_TLS_PEM	CN=ESDP CA, OU=Avaya Global Services, OU=Class 2 Managed PKI Individual Subscriber CA, OU=Terms of use at https://www.verisign.com/rpa (c)06, OU=VeriSign Trust Network, O="Avaya, Inc.", C=US
□	Used for validating TLS client identity certificates	TM_INBOUND_TLS_PEM	O=AVAYA, OU=MGMT, CN=default
□	Used for validating TLS client identity certificates	TM_INBOUND_TLS_PEM	CN=WebLM 4.6SP3, OU=SIP Product Certificate, O=Avaya Inc., C=US
□	Used for validating TLS client identity certificates	TM_INBOUND_TLS	CN=WebLM 4.6SP3, OU=SIP Product Certificate, O=Avaya Inc., C=US
□	Used for validating TLS client identity certificates	TM_INBOUND_TLS	CN=Avaya File Signing Authority 2013, OU=Avaya Product PKI, O=Avaya Inc., C=US
□	Used for validating TLS client identity certificates	TM_INBOUND_TLS	CN=ESDP CA, OU=Avaya Global Services, OU=Class 2 Managed PKI Individual Subscriber CA, OU=Terms of use at https://www.verisign.com/rpa (c)06, OU=VeriSign Trust Network, O="Avaya, Inc.", C=US
□	Used for validating TLS client identity certificates	TM_INBOUND_TLS	O=AVAYA, OU=MGMT, CN=default

- To add a new root certificate for a service, click **Add**.

  The system displays the Add Trusted Certificate.

Related links

Adding trusted certificates on page 1085

Adding trusted certificates

About this task

Import the certificates that you want to add as trusted certificate in the trust store of the element.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **Add**.
5. On the Add Trust Certificates page, in the **Select Store Type to add trusted certificate** field, select a store type or select **All** if you are unsure of the store type.
6. To import a trusted certificate in the trust store for an element, perform one of the following:
   - To import certificates from a file:
     a. Click **Import from file**.
     b. Type the name of the file or click **Browse** to select a file.
     c. Click **Retrieve Certificate**.
     d. Click **Commit**.
   - To import certificates in the PEM format:
     a. Locate the PEM certificate.

b. Open the certificate in the Notepad application.

c. Select and copy the contents in the file.

d. Click **Import as PEM certificate**.

e. Paste the contents from the file in the box provided at the bottom of the page.

> **Note:**
>
> You might include the start and end tags “ -----BEGIN CERTIFICATE-----” and“ -----END CERTIFICATE----”.

f. Click **Commit**.

- To import certificates from existing certificates:

  a. Click **Import from existing certificates**.

  b. In the Global Trusted Certificate section, select a certificate.

  c. Click **Commit**.

- To import certificates by using TLS:

  a. Click **Import using TLS**.

  b. In the **IP Address** field, type the IP address of the computer.

  c. In the **Port** field, type the port of the computer.

  d. Click **Retrieve Certificate**.

  e. Click **Commit**.

Related links

Add Trusted Certificate field descriptions on page 1094
Obtaining the SSL certificate for Microsoft Active Directory on page 1084

Viewing trusted certificates

About this task

You can view the trusted certificates of System Manager and its managed elements.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, select the required certificate and click **View**.

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

Related links

View Trust Certificate field descriptions on page 1096

Removing trusted certificates

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page , select an application and click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, select the certificates you want to remove.
5. Click **Remove**.

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

Trusted certificate management

Participants in a Public-Key Infrastructure (PKI) scheme use root certification authorities and other intermediate certification authorities to determine the trustworthiness of an identity certificate. These certification authorities are collectively known as trust anchors or trusted certificates.

System Manager certificate management supports the following tasks on the trusted certificate of a service:

- View: Trust Management provides details about the subject, issuer, key size, fingerprint, and expiry date of the certificate that a service uses.
- Add: A service may require to communicate with another service outside the deployment PKI of Avaya Aura®. For example, for a service to gain access to a remote database or a directory service which presents an identity certificate signed by a commercial CA, include the certificate of the CA in the list of trusted certificates of the service.

  For example, if a service is exposed to multiple SIP endpoints, you cannot add the certificate of the private Certificate Authority (CA) to the trusted certificate store of each client. If each SIP endpoint is configured to trust certificates issued by a commercial CA, replace the certificate presented by the endpoint with a certificate of the commercial CA or the root certificate of the commercial CA. You can add a certificate to a trusted certificate store of the service in the following encodings:

  - ASN.1 DER
  - PEM (OpenSSL)

  You can also get a certificate from an SSL socket or from the built-in certificate store.
- Export: Trust Management supports exporting the selected certificate from the list of trusted certificates to a PEM formatted file.
- Delete: When you do not need a service to participate in an external PKI hierarchy, the administrator can remove the trusted certificate from the trusted certificate store of the service. For example, when CA changes, you do not require the existing CA.

Managing identity certificates

Viewing identity certificates

Procedure

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

   The Identity Certificate page displays the identity certificates for the element that you selected. The certificate signed by the Avaya CA is the default.

Related links

Identity Certificates field descriptions on page 1090

Replacing an identity certificate

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **More Actions** > **Configure Identity Certificates**.
4. On the Identity Certificates page, select the certificate that you want to replace.
5. Click **Replace**.
6. On the Replace Identity Certificate page, do one of the following:
   - Click **Replace this Certificate with Internal CA Signed Certificate**, and do the following:
     a. Select the check box and type the common name (CN) that is defined in the existing certificate.

     b. Select the key algorithm and key size from the respective fields.

        Note:

        System Manager uses the SHA2 algorithm for generating certificates.

     c. (Optional) In **Subject Alternative Name**, select the check box, and perform the following:

        - In the **DNS Name** field, select the check box and enter the values.
        - In the **IP Address** field, select the check box and enter the values.
        - In the **URI** field, select the check box and enter the values.

> **Note:**
>
> In all three fields, you can enter more than one values separated by a comma.

  d. To replace the identity certificate with the internal CA signed certificate, click **Commit**.

  e. Restart the service for which you replaced the certificate.

- Click **Import third party PCKS # 12 file** and do the following:

  a. In the **Please select a file** field, type the file name.

  b. In the **Password** field, type the password.

  c. Click **Retrieve Certificate**.

  The **Certificate Details** section displays the details of the certificate.

  d. To replace the certificate with the third-party certificate that you imported, click **Commit**.

  e. Restart the service for which you replaced the certificate.

7. For the new generated certificates to take effect, restart JBoss on System Manager.

Related links

Replace Identity Certificate field descriptions on page 1091

Renewing identity certificates

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **More Actions** > **Configure Identity Certificates**.
4. On the Identity Certificates page, select the certificate that you want to renew.
5. Click **Renew**.

   Wait until the system renews the certificate.
6. Restart the service for which you renewed the certificate.
7. For the new certificates to take effect, restart JBoss on System Manager.

   You must also restart JBoss on System Manager if certificates are auto renewed.

Identity certificate management

In Public-Key Infrastructure (PKI), an identity certificate is an electronic document, which uses a digital signature to bind a public key with an identity information such as the name of a person or an organization and address of a person or an organization. The identity certificate is also known as digital certificate or public key certificate. You can use the certificate to verify if a public key belongs to a service.

System Manager supports the following tasks on the identity certificate of a service:

- View: Trust Management provides details about the subject, issuer, key size, fingerprint, and expiry date of the certificate that a service uses.

  Additionally, Trust Management provides subject alternative name.
- Replace: Services that are exposed to external clients may require to present an identity certificate issued by a commercial root CA.

  For example, if a service is exposed to multiple SIP endpoints, you cannot add the certificate of the private Certificate Authority (CA) to the trusted certificate store of each client. If each SIP endpoint is configured to trust certificates issued by a commercial CA, then replace the certificate presented by the service with a certificate issued by a commercial CA. Also, in protocols like HTTP, the CN value of the certificate must match the host name of the server presenting the certificate. If the host name changes, the CN must change.
- Export: Trust Management supports exporting the selected certificate from the list of trusted certificates to a PEM formatted file.
- Renew: Central administrator might need to reissue an identity certificate that was originally issued by the deployment CA. For example, an identity certificate has a validity date. Therefore, the administrator must replace the certificate before the certificate expires to avoid rejection of the certificate by the service peer.

Identity Certificates field descriptions

Field	Description
Service Name	The name of the service that uses the identity certificate.
Common Name	The common name to identify the service.
Valid To	The date until which the certificate is valid.
Expired	Specifies whether the certificate is expired.
Service Description	A brief description about the service.

Button	Description
Replace	Opens the Replace Identity Certificate page. Use this page to replace a selected identity certificate with a new certificate.
Export	Exports the certificate that you select. The exported certificate is in the form of a PEM file.
Renew	Renews the certificate that you select. After you renew a certificate, the system automatically updates the **Valid To** column.

Replace Identity Certificate field descriptions

Certificate Details

Name	Description
Subject Details	The certificate holder details.
Valid From	The date and time from when the certificate is valid.
Valid To	The date and time till the certificate is valid.
Key Size	The key size in bits for encryption. The default key size is 2048.
Issuer Name	The name of the certificate issuer.
Certificate Fingerprint	The fingerprint that authenticates the certificate.
Subject Alternative Name	An alternate name for the certificate holder.

Name	Description
Replace this Certificate with Internal CA Signed Certificate	The option to replace the current certificate with the internal CA signed certificate.
Import third party certificate	The option to replace the identity certificate with the PKCS #12 file that you imported from a third-party source.

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

Field	Description
Common Name (CN)	The common name of the certificate holder. You must select the check box to enter the name.
Key Algorithm	The algorithm used to generate the key for the certificate. The option is RSA. System Manager uses the SHA2 hash algorithm for generating certificates.
Key Size	The key size in bits for encryption. The options are: • **1028** • **2048** • **4096** **Note:** Session Manager Release 6.3.12 and later support 4096. Use 2048 as the key size.

Table continues…

Field	Description
Subject Alternative Name	An alternate name for the certificate holder. The fields are: • **DNS Name**: DNS IP address. • **IP Address**: IP address. • **URI**: URI address. ✳ **Note:** To type the values, you must select the check boxes. In all three fields, you can enter more than one values separated by a comma. Do not add spaces between comma separated IP addresses and DNS names.

The page displays the following fields when you select **Import third party certificate**.

Name	Description
Please select a file (PKCS #12 format)	The full path of the PKCS #12 file where you saved the certificate.
Password	The password to retrieve the certificate.

Button	Description
Retrieve Certificate	Retrieves the details of the imported certificate and displays in the Certificate Details section.
Commit	Replaces the current identity certificate with the selected certificate.
Cancel	Cancels the certificate replacement operation.

Related links

Replacing an identity certificate on page 1088

Retrieving the System Manager CA certificate

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. On the CA Functions page click **Download pem file**.
4. Click **Save** to save the certificate to a file.

Certificate Authorities

This section applies only if you deploy legacy Nortel applications.

In System Manager, element installation sets up the trust between System Manager and its managed elements. Similarly, UCM has a trust management process to set up the trust between UCM and its managed elements. To enable managed elements of UCM to be in the same trust domain as the System Manager managed elements, you must import the UCM Certificate Authority (CA) certificate to the System Manager managed element's trusted certificate list. Also, import the System Manager CA certificate to UCM managed element's trusted certificate list.

Certificate Authorities in a Geographic Redundancy setup

In System Manager configured with Geographic Redundancy, the system replicates the CA certificate from the primary System Manager server to the secondary System Manager server. By default, the primary System Manager server, the secondary System Manager server and their elements are part of the same trust domain. For the initial trust relationship, during the configuration, the secondary System Manager server uses the Certificate Enrollment password that is set on the primary server. The primary System Manager server issues a certificate to the secondary System Manager server.

When the secondary System Manager server is active, do not configure System Manager as a sub CA.

Enrollment Password field descriptions

Name	Description
Time Remaining	The time in hours and minutes remaining for expiration of the current password.
Password expires in	The duration in hours for which the existing password is valid.
Password	The password that the external clients use to request for a certificate.
Confirm Password	The password that you retype.

Button	Description
Commit	Updates the **Existing Password** and **Time Remaining** fields.

Trusted Certificates field descriptions

Use this page to view, export, and remove the trusted certificates listed on the page. You can add more certificates in the existing list of trusted certificates.

Field	Description
Store Description	The purpose of the trusted certificate.
Store Type	The type of the store associated with the certificate.
Subject Name	The name of the certificate holder.

Button	Description
View	Opens the View Trust Certificate page. Use this page to view the certificate details.
Add	Opens the Adds Trusted Certificate page. Use this page to import certificates from the selected resource.
Remove	Removes the selected certificate from the list of trusted certificates.
Export	Exports the selected certificate from the list of trusted certificates to a PEM formatted file.

Add Trusted Certificate field descriptions

Name	Description
Store Type	The store type that is based on inbound and outbound connection.
Import from existing	The option to import a certificate from the existing imported certificates.
Import from file	The option to import a certificate from a file. The file format is `.cer` or `.crt`.
Import as PEM Certificate	The option to import a certificate in the PEM format.
Import using TLS	The option to import a certificate if the element 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
Certificate Name	The fully qualified domain name of the certificate.
Subject Name	The fully qualified domain name of the certificate holder.
Valid To	The date until which the certificate is valid.
Filter: Enable	Displays fields in select columns where you can set the filter criteria. This is a toggle button.

Table continues…

Name	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters certificates based on the filter criteria.
Select: All	Selects all the certificates in the table.
Select: None	Clears all the check box selections.
Refresh	Refreshes the certificates information.

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

Name/Button	Description
Please select a file	The file that contains the certificates.
Browse	Displays the choose file dialog box where you can choose the file from which you want to import the certificates.
Retrieve Certificate	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
Subject Details	The details of the certificate holder.
Valid From	The date and time from when the certificate is valid.
Valid To	The date and time until when 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.
Certificate Fingerprint	The fingerprint that authenticates the entire certificate.
Key Fingerprint	The fingerprint that authenticates the key. The Key fingerprint applies only for CA certificate. Therefore, any element, which calculates fingerprint using the key, can use this authentication.
CA Certificate	The field that specifies whether the certificate is a CA certificate.

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

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

Related links

Adding trusted certificates on page 1085

View Trust Certificate field descriptions

Name	Description
Subject Details	The 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.
Certificate Fingerprint	The fingerprint that authenticates the entire certificate.
Key Fingerprint	The fingerprint that authenticates the key. The Key fingerprint applies only for CA certificate. Therefore, any element, which calculates fingerprint using the key, can use this authentication.

Button	Description
Done	Closes the page and returns 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 element.

Field	Description
Certificate Name	The common name of the certificate.
Store Type	The type of the store associated with the certificate.
Subject Name	The name of the certificate holder.

Button	Description
Delete	Deletes the trusted certificate from the corresponding store.
Cancel	Cancels the delete operation and takes you back to the Add Trusted Certificate page.

Generating certificates from System Manager

Certificate generation

Generation of certificates from the System Manager web console includes the following tasks:

- (Optional) Creating a certificate signing request (CSR).
- Creating an end entity.
- Generating the certificate keystore.
- Creating the certificate using CSR.
- Viewing contents of the certificate.

Creating a certificate signing request

Before you begin

Install the OpenSSL command line tool.

About this task

Perform this procedure if you want to generate the certificate with the key that you generate and get System Manager to sign your keys.

Do not perform the procedure if you want System Manager to generate the public and private keys for the certificate.

Procedure

1. Start an SSH session on System Manager.
2. To generate the keys and a corresponding certificate signing request (CSR), type the following command:

   ```
   openssl req -out <CSR name> -new -newkey rsa:2048 -nodes -keyout <PvtKey_Filename>
   ```

   Where:

   - CSR name is the name of the output CSR file. For example, `mycsr.csr`.
   - rsa:2048 instructs the system to create a 2048-bit RSA key.
   - PvtKey_Filename is the filename where the system stores the private key. For example, `privateKey.key`.

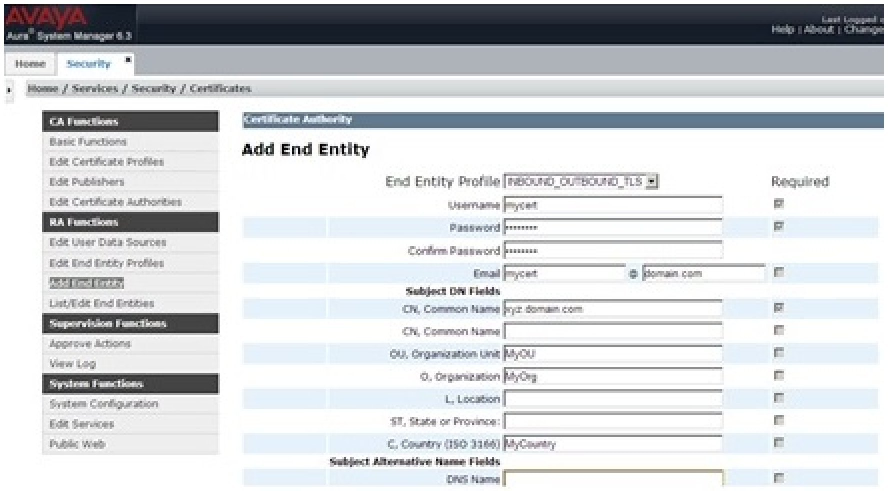
Creating an end entity

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **RA Functions** > **Add End Entity**.
4. On the Add End Entity page, in **End Entity Profile**, click **INBOUND_OUTBOUND_TLS**.
5. Type the username and password.

   The password is mandatory for each end entity. Without the password, you cannot generate the certificate from System Manager because you require the password to authenticate the certificate generation request.

6. Complete the fields that you want in your certificate.

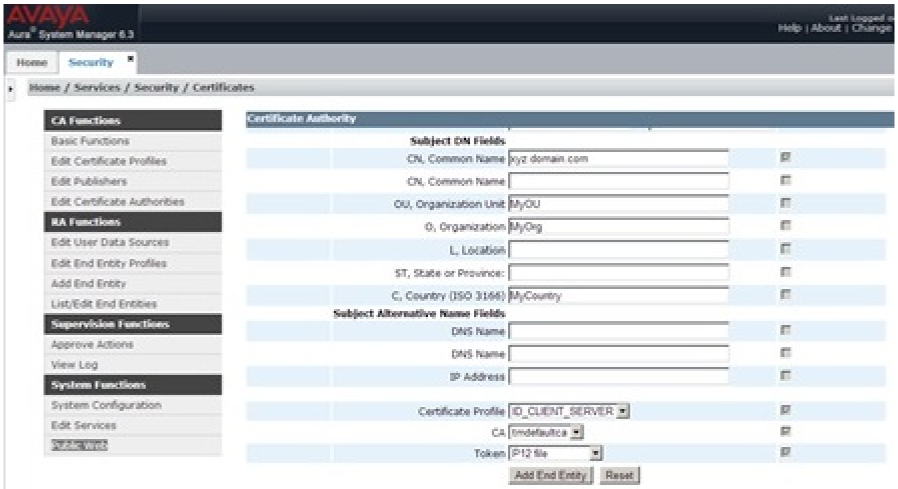
   Add End Entity

End Entity Profile	INBOUND_OUTBOUND_TLS	Required
Username	mycert	☑
Password	••••••••	☑
Confirm Password	••••••••	
Email	mycert @ domain.com	□
Subject DN Fields		
CN, Common Name	xyz.domain.com	☑
CN, Common Name		□
OU, Organization Unit	MyOU	□
O, Organization	MyOrg	□
L, Location		□
ST, State or Province:		□
C, Country (ISO 3166)	MyCountry	□
Subject Alternative Name Fields		
DNS Name		□

   The system automatically selects the following:

   - **ID_CLIENT_SERVER** in **Certificate Profile**
   - **tmdefaultca** in **CA**
   - **User Generated** in **Token**

     With **User Generated**, the system generates the certificate by using CSR. You can also select **P 12 file**.



Subject DN Fields

CN, Common Name	xyz domain com	☑
CN, Common Name		☐
OU, Organization Unit	MyOU	☐
O, Organization	MyOrg	☐
L, Location		☐
ST, State or Province:		☐
C, Country (ISO 3166)	MyCountry	☐

Subject Alternative Name Fields

DNS Name		☐
DNS Name		☐
IP Address		☐
Certificate Profile	ID_CLIENT_SERVER	☑
CA	tmdefaultca	☑
Token	P12 file	☑

7. Click **Add End Entity**.

   The system displays the message `End Entity <username> added successfully`.

Generating the certificate keystore

Before you begin

Create an end entity.

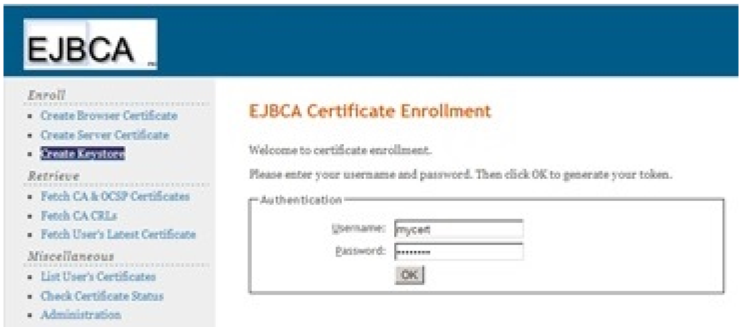
For more information, see Creating an end entity.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. In the left navigation pane, click **Public Web**.
4. On the public EJBCA page, do one of the following:
   - If you are generating the certificate by using certificate signing request (CSR), click **Enroll** > **Create Certificate from CSR** and continue with the steps in Creating the certificate by using certificate signing request.
   - Do the following:
     - Click **Enroll** > **Create Keystore**.
     - On the Keystore Enrollment page, type the username and password.

       Note:

       Provide the same username and password that you entered while creating the end entity on the Add End Entity page.



EJBCA Certificate Enrollment

Welcome to certificate enrollment.

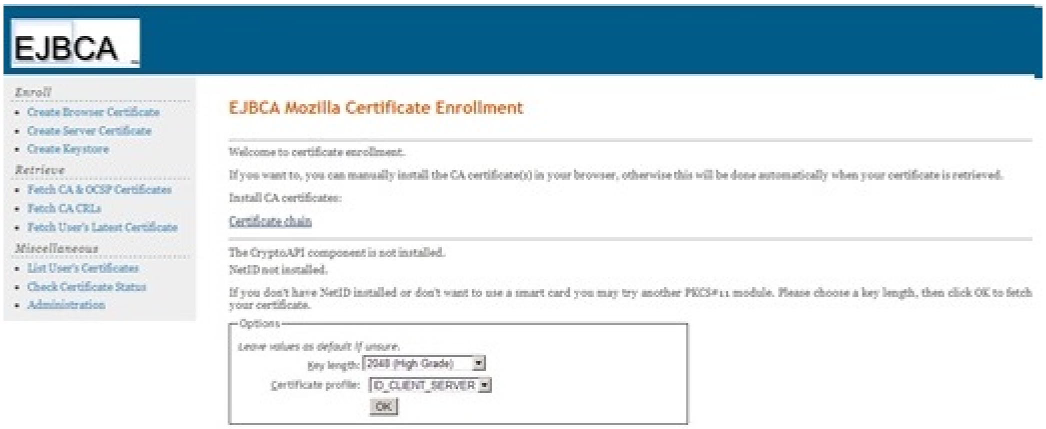
Please enter your username and password. Then click OK to generate your token.

Authentication

Username: mycert

Password: ••••••••

- Click **OK**.
- On the next page, retain the values in the **Key length** field, and click **OK**.



EJBCA Mozilla Certificate Enrollment

Welcome to certificate enrollment.

If you want to, you can manually install the CA certificate(s) in your browser, otherwise this will be done automatically when your certificate is retrieved.

Install CA certificates:

Certificate chain

The CryptoAPI component is not installed.
NetID not installed.

If you don't have NetID installed or don't want to use a smart card you may try another PKCS#11 module. Please choose a key length, then click OK to fetch your certificate.

Options

Leave values as default if unsure.

Key length: 2048 (High Grade)

Certificate profile: ID_CLIENT_SERVER

The system generates a PKCS12 format keystore with the identity certificate that contains values provided in the end entity.

Related links

Creating an end entity on page 1098

Creating the certificate by using certificate signing request

Before you begin

Create an end entity.

For more information, see Creating an end entity.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. In the left navigation pane, click **Public Web**.
4. On the public EJBCA page, click **Enroll** > **Create Certificate from CSR**.

5. To get your certificate, on the Certificate Enrollment from a CSR page, do the following:
    a. Enter the same username and the password that you provided while creating the end entity.
    b. In the text box, paste the PEM-formated PKCS10 certification request.
    c. Click **OK**.

       The system signs the certificate signing request (CSR) and generates a PEM-formatted certificate that contains the values provided in the end entity.

Related links

Creating an end entity on page 1098

Viewing contents of the certificate

Before you begin

Install the tool that you want to use to view the keystore.

About this task

You can view the contents of the certificate in a keystore by using any common tool, such as keytool.

Procedure

1. Start an SSH session.
2. To view the contents of the certificate in a keystore, type the following command:

   ```
   keytool -list -keystore <keystore> -storepass <keystorepassword> -storetype PKCS12
   -v
   ```

   Where:

   - keystore is the path to the keystore.
   - keystorepassword is the password of the keystore
   - PKCS12 is the format of the keystore. Use JKS for the JKS format keystores.
3. To view the contents of a PEM certificate, type the following command:

   ```
   openssl x509 -in <certificate> -text noout
   ```

   Where: certificate is the path to the PEM certificate.

Creating a new Certificate Authority by using SHA2 signing algorithm and 2048 key size

About this task

System Manager systems that are upgraded from releases earlier than Release 7.0, contain Certificate Authority with root CA cert signed by using SHA1 algorithm and with key size=1024 bits. You can use the createCA utility to create a default Certificate Authority with root CA certificate signed by using SHA2 algorithm and with key size=2048.

Procedure

1. On System Manager, start an SSH session.
2. Type `createCA`.

   The createCA utility is an interactive tool.
3. At the prompt, provide the desired Common Name (CN) for the new CA certificate.

Related links

System Manager command line interface operations on page 1298

External SSL configurations in System Manager

Using third-party identity certificate for System Manager

From the System Manager web interface, you can install an identity certificate for System Manager that is issued by a certificate authority. After the certificate installation, during SSL communications, System Manager presents the identity that the third-party identity certificate issue.

Installing and using the third-party identity certificate for the System Manager web interface includes the following key tasks:

1. Replacing the System Manager web server certificate with third-party certificate.
2. Updating the trust stores for internal services, clients, or managed elements with third-party root and subordinate CA certificate.

For more information about installing the third-party identity certificate, see *Application notes for supporting third-party certificate in Avaya Aura® System Manager* on the Avaya Support site at http://support.avaya.com.

Setting the System Manager CA as the subordinate CA

About this task

You can change the default Certificate Authority (CA) that the system generated during the System Manager installation to an externally signed subordinate CA (SubCA). Using this capability, you can add System Manager CA to an existing CA hierarchy in the customer environment.

In a Geographic Redundancy enabled system, EJBCA configured as SubCA on the primary System Manager server is also provisioned on the secondary System Manager server.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **Certification Authorities**.
4. On the Manage Certification Authorities page, in the **Add CA** field, type the name ExtenalSubCA, and click **Create**.

5. On the Create CA page, perform the following:
    a. In **Signing Algorithm**, click a value.

       Avaya suggests SHA256WithRSA.
    b. In **Description**, provide a description.
    c. In **Subject DN**, enter a DN for your SubCA.

       For example, CN=ExernalSubCA-1,O=AVAYA,C=US.
    d. In **Signed By**, click **External CA**.
6. Click **Choose File** and open the CA certificate file on your computer.

   Note:

   You must have the CA certificate that is used to sign the CA. The certificate must be in the PEM format and available on the same computer on which you run the browser.
7. Click **Make Certificate Request**.

   You receive a request for a PEM-formatted certificate.
8. Click **Download pem file**.
9. Click **Save File**, and save the file on your computer.

   You must get the certificate request signed by CA. If you use Openssl, move the certificate request to the computer where your Openssl CA is set up and sign the request.

   Note:

   By default, Openssl reorders DN to whatever the Openssl policy file is set up to do. Use the -preserveDN flag while you sign the request by running the **`openssl ca`** command. If you do not use the -preserveDN flag, EJBCA does not recognize the CA and the certificate request fails.

   Use **`openssl x509 -in cert.pem -text`** command to ensure that the signed request has the X.509 extension **CA:TRUE**.

   After you get the signed certificate from the CA in the PEM format, delete any data other than the certificate itself. Ensure that there is no carriage return after the last line.
10. To set the preserveDN flag, on the Linux server, perform the following steps:
    a. From the `/etc/pki/tls/misc` directory, open the `CA` file and search for -sign|-signreq.
    b. To add the preserveDN attribute, type `$CA -policy policy_anything -preserveDN -out newcert.pem -infiles newreq.pem`.
11. On the Linux server, from the `/etc/pki/tls` directory, open the `openssl.cnf` file and change all occurrences of basicConstraints=CA:FALSE to basicConstraints=CA:TRUE.

Related links

Receiving certificate response on page 1104
Setting the new CA as the default CA on page 1104

Modifying the default end entities to use the new CA on page 1105
Generating new identity certificates for System Manager on page 1106
Confirming identity certificate updates on System Manager on page 1107

Receiving certificate response

About this task

Ensure that the certificate you have received is properly signed by the CA. You can do this using openssl using `openssl verify -CAfile ca-cert.pem subca-cert.pem`

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **Certification Authorities**.
4. Select ExternalSubCA that you created earlier with the “Waiting for Certificate Response” status, and click **Edit CA**.
5. In Externally signed CA creation/renewal section, in **Path to certificate signed by external CA**, click **Choose File** and browse to the signed certificate.
6. Click **Receive Certificate Response**.

   The system displays a message that the certificate response is received successfully and that the CA is activated. If you do not see this message, double check the contents of the certificate file.

Related links

Setting the System Manager CA as the subordinate CA on page 1102

Setting the new CA as the default CA

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **Certification Authorities**.
4. Select the new Sub CA, ExternalSubCA, and ensure that the status is **Active**.
5. On the Manage Certification Authorities page, perform the following to rename the existing CA, tmdefaultca:
   a. From the list, highlight tmdefaultca.
   b. In the text box at the bottom of the page, type in a new name. For example, oldtmdefaultca.
   c. Click **Rename**.

> **Important:**
>
> The CRD files refer to tmdefaultca. Therefore, rename the CA that you want to make as default to tmdefaultca.

6. Perform the following to rename ExternalSubCA to tmdefaultca:
   1. From the list, highlight ExternalSubCA.
   2. In the text box at the bottom of the page, type `tmdefaultca`.
   3. Click **Rename**.

      The system sets your new ExternalSubCA as the default CA.

Next steps

Create a backup. For more information, see Creating a data backup.

Related links

Setting the System Manager CA as the subordinate CA on page 1102
Creating a data backup on a local server on page 780

Modifying the default end entities to use the new CA

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **Certificate Profiles**.
4. For **ID_CLIENT**, click **Edit**.
5. On the Edit page, in **Available CAs**, highlight tmdefaultca.
6. Click **Save**.
7. On the Manage Certificate Profiles page, repeat Step 4 through Step 6 for **ID_CLIENT_SERVER** and **ID_SERVER**.
8. Click **RA Functions** > **Edit Entity Profiles**.
9. Select **INBOUND_OUTBOUND_TLS** and click **Edit End Entity Profile**.
10. On the Edit End Entity Profile page, in **Default CA**, ensure that you select tmdefaultca.
11. In **Available CAs**, highlight tmdefaultca.
12. Click **Save**.
13. Repeat Step 9 through Step 12 for **INBOUND_TLS**, **OUTBOUND_TLS**, and **EXTERNAL_CSR_PROFILE**.
14. Click **RA Functions** > **Search End Entities**.
15. On the Search End Entities page, in **Search end entities with status**, click **All**.
16. Click **Search**.

17. Ensure that the list contains the end entities: INBOUND_OUTBOUND_TLS, INBOUND_TLS, OUTBOUND_TLS, and EXTERNAL_CSR_PROFILE.

    If the required end entity in unavailable:

    - Geographic Redundancy configuration might fail.
    - The system displays the message `The secondary System Manager server is unable to POST a CSR for signing`.
    - The primary System Manager server error log displays the message `Unable to sign csr for user EXTERNAL_CSR_PROFILE, 1, ….`

18. On the Search End Entities page, for each end entity listed in earlier step, perform the following:

    a. Click **Edit End Entity**.

    b. On the Edit End Entity Profile page, in **CA** field, ensure that the value is set to tmdefaultca.

    c. Click **Save**.

19. Click **Close**.

20. On the Search End Entities page, click **Reload**.

    The system displays the new value in the **CA** column for all four entities.

Related links

Setting the System Manager CA as the subordinate CA on page 1102

Generating new identity certificates for System Manager

About this task

After CA is set up to issue certificates by using the new SubCA, update the identity certificates that are created for System Manager during the initialization of System Manager. These certificates are signed by tmdefaultca, and not by the new CA. Also, the new CA must be added to the System Manager trust stores.

Procedure

1. On the System Manager web console, click **Services** > **Security**.

2. In the left navigation pane, click **Certificates** > **Enrollment Password**.

3. Set a new enrollment password by providing information in the required fields, and click **Commit**.

   The system resets the enrollment password that was lost after you changed the CA.

4. Start an SSH session on System Manager.

5. Go to the `cd /opt/Avaya/Mgmt/<System Manager version>/trs` location, where the installation scripts are available.

> **Note:**
>
> The file path might differ in different directory versions. For example in Release 6.3.8, the scripts are available at `/opt/Avaya/Mgmt/6.3.8/trs`.

6. To run the trust initializer script, type `./trust_initializer_install.sh -RMIPORT 1399 -HTTPSPORT 443 -TMCONFIGLOC /opt/Avaya/JBoss/6.1.0/jboss-as/server/avmgmt/conf/tm/`.

   Ensure that all System Manager identity certificates are updated so that the certificates are signed by the new CA, and the new CA is available in the trust stores.

Related links

Setting the System Manager CA as the subordinate CA on page 1102

Confirming identity certificate updates on System Manager

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. On the Manage Elements page, select a System Manager instance and click **More Actions** > **Configure Identity Certificates**.
3. On the Identity Certificates page, select any of the certificates, except weblm_legacy, which is self-signed, and verify that the **Issuer Name** in the window below is the DN of your new CA.
4. On the Manage Elements page, select a System Manager instance and click **More Actions** > **Configure Trusted Certificates**.

   On the Trusted Certificates page, the system must display one certificate with DN of your new CA certificate in each of the StoreTypes. The system must display three instances on this page.

   Restart all System Manager applications JBoss and systemMonitor so that the new certificates are read. Alternatively, you can reboot the System Manager server.
5. To restart System Manager applications, reboot the System Manager server.

   The System Manager CA changes from the internally generated CA to an externally signed SubCA.
6. **(Optional)** In a Geographic Redundancy setup, reconfigure the System Manager secondary server.

Related links

Setting the System Manager CA as the subordinate CA on page 1102

Configuring DTLS for CS 1000

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.

2. In the left navigation pane, click **Manage Elements**.
3. Select the CS 1000 element.
4. Click **More Actions** > **Configure Identity Certificates**.
5. Select the Dtls and click **Replace**.
6. Select **Replace this Certificate with Internal CA Signed Certificate** and provide the common name, keysize, and the algorithm.
7. Click **Commit**.

Configuring SIP TLS for CS 1000

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Select the CS 1000 element.
4. Click **More Actions** > **Configure Identity Certificates**.
5. Select SipTls and click **Replace**.
6. Select **Replace this Certificate with Internal CA Signed Certificate** and provide the common name, keysize, and the algorithm.
7. Click **Commit**.

External authentication

External authentication

The External Identity Repositories Web page in System Manager contains a summary page for Authentication scheme and Authentication servers. You can configure the authentication scheme and the authentication servers for System Manager.

System Manager supports the following authentication authorities:

- Local users
- External RADIUS users
- External LDAP users
- External Security Assertion Markup Language (SAML) users

The authentication scheme policy determines the order in which you can use the authentication authorities. The supported order is as follows:

1. Local users (default)
2. External RADIUS users then local users
3. External LDAP users then local users
4. External LDAP users, then external RADIUS users, then local users
5. External RADIUS users, then external LDAP users, then local users
6. External KERBEROS server

The authentication servers policy controls the settings for the external SAML, LDAP, RADIUS, and KERBEROS servers.

Authentication scheme policy

System Manager supports the following authentication authorities:

- Local servers
- External RADIUS servers
- External LDAP servers (including Sun ONE or Microsoft active directory server)
- KERBEROS server
- SAML

Editing the authentication scheme

About this task

✱ **Note:**

The edit operation might reset the authentication scheme for the user. Ensure that the authentication scheme is correct.

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **User Services** > **External Authentication**.
3. On the External Identity Repositories page, in the Authentication Scheme section, click **Edit**.
4. On the Authentication Scheme page, select the required authentication scheme.
5. Click **Save**.

Provision the authentication servers

When the LDAP server is Microsoft Active Directory, the full name of the external user must be the same as the logon name that makes the cn attribute of the external users the same as the logon name.

The TCP port used for the external LDAP server and the UDP port used for the external RADIUS server must be open in the Linux iptables firewall, on both the primary security service, and the backup primary security service. To check the status of the iptables rules, use service iptables status.

Provisioning the LDAP server

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **User Services** > **External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.
4. On the Authentication Servers page complete the **Provision LDAP Server** section.
5. Click **Save**.

   Note:

   Ensure that the Linux iptable firewall setting, on both the primary and backup security service, allows the TCP port as the source port.

Related links

Provision LDAP/Radius/Kerberos server field descriptions on page 1112

Provisioning the RADIUS server

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **User Services** > **External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.
4. On the Authentication Servers page, complete the following information in the Provision RADIUS Server section:
   - **IP (or DNS)**: Type the IP address or DNS name of the primary RADIUS server.
   - **UDP Port**: Type the UDP port number of the primary RADIUS server.

- **Shared Secret**: Type the shared secret of the RADIUS server.

  Note:

  You must create two records in the external RADIUS server with the same shared secret for both the primary security server and backup security server IP address.

5. Click **Save**.

   Note:

   Ensure the Linux iptable firewall setting on both the primary and backup security service allows the UDP port as the source port.

Related links

Provision LDAP/Radius/Kerberos server field descriptions on page 1112

Provisioning the Kerberos server

To use Kerberos authentication, configure System Manager with the required information for the Kerberos server.

Before you begin

- If you use Firefox to gain access to System Manager, perform the following:
  1. In the address bar of the web browser, type `about:config`.
  2. Select the network.negotiate-auth.trusted-uris attribute.
  3. Right-click, select **Modify**, and add the URL of System Manager.
- Log on to System Manager as admin.

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **User Services** > **External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.
4. On the Authentication Servers page, in the **Provision Kerberos Server** section, complete the following information:
   - **DC Host Name (FQDN)**: Type your FQDN in the format `machineName.domainName.com`. For example, `xyz.somecompany.com`.
   - **DC Computer Domain**: Type the domain name of the Kerberos server.
   - **Keytab File**: Click **Browse** and select the Kerberos server key file.
5. Click **Save**.

Important:

When you log on to the Kerberos server using Single Sign-on (SSO), the system automatically authenticates you in the Domain Controller (DC) domain. Therefore, you cannot exit from UCM by using the **Logout** link. Close the web browser to exit the application.

Related links

Provision LDAP/Radius/Kerberos server field descriptions on page 1112

Provision LDAP/Radius/Kerberos server field descriptions

Provision LDAP Server

Name	Description
IP (or DNS)	The IP address or the DNS name of the LDAP server.
TCP Port	The TCP port of the LDAP server.
Base Distinguished Name	The base distinguished name of the LDAP server.
SSL/TLS Mode	Specifies whether the LDAP server supports SSL/TLS connections.
Is Active Directory	Select this check box if active directory does not support anonymous binding.
Supports Anonymous Binding	Select this check box if anonymous binding is supported.
Distinguished Name for Root Binding	Type the distinguished name for the root binding. For example, type `cn` for Users.
Password for Root Binding	Type the password for the root binding in this field.

Provision Radius Server

Name	Description
IP (or DNS)	The IP address or the DNS name of the primary RADIUS server.
UDP Port	The UDP port number of the primary RADIUS server.
Shared Secret	Shared secret of the RADIUS server.

Provision SAML Remote Identity Provider

Name	Description
Metadata Type	The method to query the metadata for Remote Identity Provider. The values are: • URL. A valid HTTP URL.

Table continues…

Name	Description
	• File. A valid XML file.
Metadata Url	The valid HTTP URL for the metadata of Remote Identity Provider.
Metadata File	The valid XML file for the metadata of Remote Identity Provider.
Choose File	Click to select an XML file that contains the metadata for Remote Identity Provider.

Provision Kerberos Server

Name	Description
DC Host Name (FQDN)	Enter your FQDN in the following format: machineName.domainName.com/net/.
DC Computer Domain	The domain name of the Kerberos server.
Keytab File	Type the encrypted Kerberos server key in this field.

Button	Description
Save	Saves your settings in the Authentication Servers page.
Cancel	Cancels your action and takes you to the previous page.

SAML authentication

SAML authentication

For enterprise level Single Sign On, System Manager provides Security Assertion Markup Language (SAML) authentication.

SAML protocol

SAML is an XML-based open standard used for exchanging authentication and authorization data between an identity provider, a producer of assertions, and a service provider, a consumer of assertions. SAML product belongs to the OASIS Security Services Technical Committee.

SAML protocol does not provide rules for determining the identity and access levels of a subject. The SAML protocol shares the authentication and authorization information of an identity between the issuer of the information, called as the identity provider and the relying party or the consumer of the information, called as the service provider.

Key components of SAML protocol

Assertions

Assertions are the packets of security information transferred from the Identity Provider to the Service Provider. The following are three different types of statements in an Assertion:

- Authentication Statements
- Attribute Statements
- Authorization Decision Statements

Assertions that the Identity Provider issues have a validity period beyond which the service provider must reject the information. SAML uses Authentication Statement to validate identity of the user.

Protocols

SAML protocol provides rules on how SAML elements must be packaged in SAML request and response messages. The following are some of the key SAML protocols:

- Authentication Request Protocol
- Artifact Resolution Protocol
- Assertion Query and Request Protocol

Assertions that the Identity Provider issues have a validity period beyond which the service provider must reject the information. SAML/System Manager uses Authentication Statement to validate user's identity.

Bindings

SAML binding refers to the mapping of a SAML message to a communication protocol or method. The following are some of the main SAML binding mechanisms:

- HTTP POST
- HTTP Redirect
- HTTP Artifact
- SOAP

Profiles

SAML profile describes how various SAML messages, protocols, and bindings can combine together to achieve a particular use case.

Web Browser SSO Profile is the widely used SAML Profile. Web Browser SSO Profile provides the use case to achieve Single Sign On from a Web browser when you gain access to a protected resource on the service provider.

SAML implementation in System Manager

System Manager uses SAML implementation version 2.0 of OpenAM Release 9.5.4 to provide SAML based authentication with external/remote Identity Providers. System Manager functions as a Service Provider, consumer of assertions. You can configure CA Siteminder or a similar solution as a Remote Identity Provider, the producer of assertions.

System Manager uses Web Browser Single Sign On profile of SAML authentication. In System Manager, authentication using SAML differs from other external authentication methods such as remote LDAP and RADIUS in the following ways:

- You require a special URL to invoke SAML based authentication. You can bookmark a URL as https://smgr.ca.avaya.com/?performsso=saml.

  The system subjects:

  - Any incoming HTTP request to System Manager with a request parameter performsso set to saml to SAML based authentication.
  - All other URLs to existing authentication handling and redirects an unauthenticated request to the login screen of System Manager.
- System Manager does not provide its own login screen for SAML authentication. The system redirects an unauthenticated user to the login screen of Remote Identity Provider (R-IDP). On successful authentication, the system redirects you to System Manager.

Salient features of SAML implementation in System Manager

- R-IDP and System Manager always communicates through HTTPS.
- System Manager and identity provider communicates through HTTP-POST binding.
- SAML implementation module does not validate CRL However, SSL communication fails with a certificate that is revoked since, SSL setup in System Manager jboss container ensures CRL validation.
- The system rejects expired Assertions.

Guidelines for SAML authentication in System Manager

- You can use the NameID of a subject in an Assertion as the login ID to create a user account for the subject in System Manager. If the system encrypts the NameID, R-IDP must include the attributes of authenticated subject such as uid and email. in the Assertion. The system uses the attributes to create a user account in System Manager. If the Assertion does not contain attributes, the R-IDP must act as an Attribute Authority. In System Manager, you require an account for RBAC.
- Assertions must be signed and not encrypted.
- The system uses assertions from trusted sources only. An administrator must setup SSL trust between System Manager and R-IDP by adding the CA certificate of R-IDP’s Web server certificate into the CA truststore in System Manager.
- Condition statement in an Assertion can have multiple AudienceRestriction statements. The condition statement must have SAML entity ID of System Manager as one of the AudienceRestriction.

Configuring System Manager for SAML authentication

Configuring Hosted Service Provider on System Manager

About this task

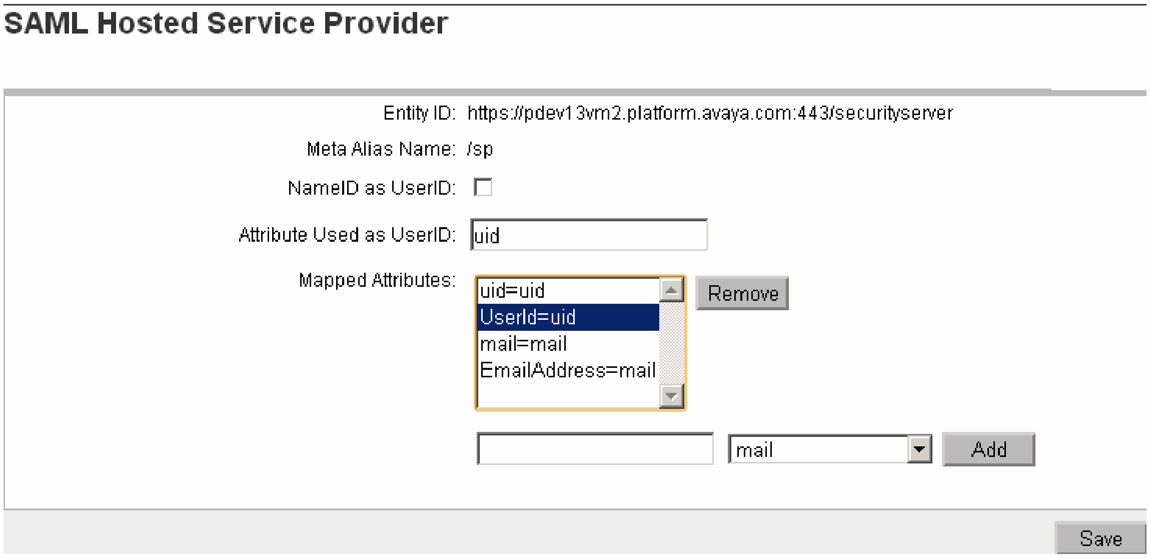
The system automatically configures System Manager as Hosted Service Provider during the installation of System Manager and upgrade of System Manager from Release 6.2.

However, you can modify the configuration using the following procedure.

As an administrator, you can enable or disable SAML authentication in System Manager from the SAML Configuration page.

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **User Services** > **External Authentication** > **SAML Configuration**.
3. Click **Edit**.
4. On the SAML Hosted Service Provider page, perform the following:
    a. Perform one of the following:
    - Select the **NameID as UserID** check box.
    - In the **Attribute Used as UserID** field, enter the name of the attribute that you want to use as the login ID of the user in System Manager.



SAML Hosted Service Provider

Entity ID: https://pdev13vm2.platform.avaya.com:443/securityserver

Meta Alias Name: /sp

NameID as UserID: □

Attribute Used as UserID: uid

Mapped Attributes:
uid=uid
UserId=uid
mail=mail
EmailAddress=mail

mail

    b. In the **Mapped Attributes** field, enter an attribute that you require to map between R-IDP and H-SP for a user.

    c. Click **Save**.

Configuring Remote Identity Provider

Procedure

1. Download the XML metadata from the Identity Provider:
    a. Download the metadata in XML format that contains the service descriptor information of Remote Identity Provider (R-IDP) from the R-IDP server or using a valid HTTP URL that R-IDP provides.

       For example, if OpenAM is configured as the R-IDP, download the metadata from `https://my-openam.ca.avaya.com/opensso/saml2/jsp/exportmetadata.jsp`.

    b. Save the data in an XML file on the file system or save the URL that points to the metadata.
2. Setup SSL trust between R-IDP and System Manager for successful communication of SAML messages using the following steps:
    a. On System Manager Web Console, click **Services** > **Inventory**.

    b. In the left navigation pane, click **Manage Elements** and add the CA certificate of R-IDP Web server certificate to System Manager truststore using the instructions outlined in Adding trusted certificates.
3. Add Remote Identity Provider:
4. Click **Save**.

   On successful configuration of R-IDP, the system automatically enables the SAML authentication. An administrator can disable or enable the SAML authentication using the **Provision SAML Remote Identity Provider** check box.

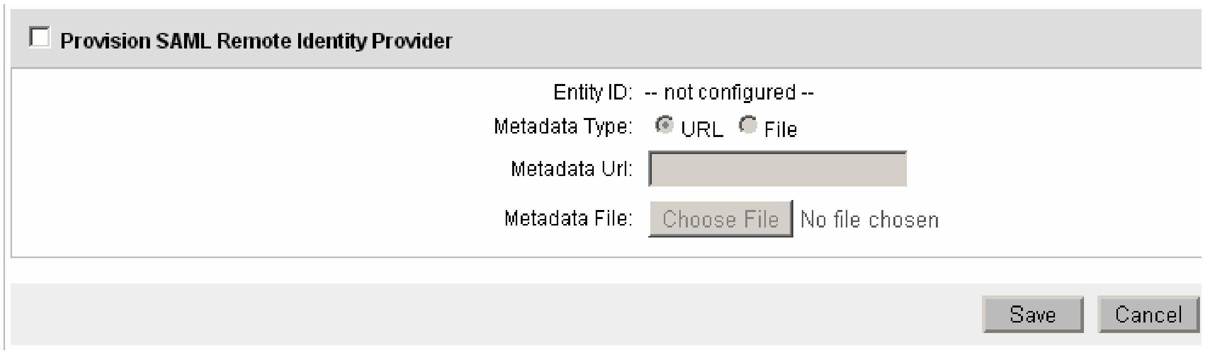
Related links

Adding trusted certificates on page 1085
Provisioning Remote Identity Provider on page 1117

Provisioning Remote Identity Provider

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **User Services** > **External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.
4. On the Authentication Servers page, select the **Provision SAML Remote Identity Provider** check box and get the metadata of R-IDP using one of the following:
    - Through a valid HTTP URL.
    - Using a valid XML file.



☐ Provision SAML Remote Identity Provider

Entity ID: -- not configured --

Metadata Type: ● URL ○ File

Metadata Url:

Metadata File: Choose File No file chosen

5. Click **Save**.

   If R-IDP is successfully configured, the system automatically enables SAML authentication. An administrator can disable or enable SAML authentication using the **Provision SAML Remote Identity Provider** check box.

Related links

Provision LDAP/Radius/Kerberos server field descriptions on page 1112

Active sessions

Viewing active sessions

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Security** > **Active Sessions**.
3. On the Active Sessions page, the sessions are sorted in the **User ID** column.

Terminating Single Sign-On sessions

About this task

Use this functionality to terminate selected Single Sign-On (SSO) sessions.

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Security** > **Active Sessions**.
3. On the Active Sessions page, select the check box beside the required sessions to terminate.

4. Click **Terminate**.

   The system deletes the selected sessions from the current sessions table. Administrators with terminated sessions are required to log on again.

Chapter 23: Managing tenants

Multi Tenancy

Tenant is a client organization that uses Team Engagement OnAvaya Aura – Unified Communication as a Service (UCaaS) (Avaya CE for UC) or Private Cloud in a shared, hosted environment. The tenant purchases the services on a pay-per-usage basis from the service provider. The tenant can contain a list of sites.

Multi Tenancy

By default, the Multi Tenancy feature is disabled. You must enable the Multi Tenancy feature. After you enable the Multi Tenancy feature, you cannot disable the feature.

The Service Provider Administrator and System Administrator can assign an element that supports:

- Multi Tenancy to more than one tenants. For example, Communication Manager.
- Single tenancy to only one tenant. For example, Messaging and IP Office.

Tenant Management

To support Multi Tenancy, System Manager provides Tenant Management.

System Manager supports three levels of organization hierarchy for tenant management. The following lists the default names of the levels:

- Level 1: Site
- Level 2: Department
- Level 3: Team

The administrator can modify the default level names. The organization hierarchy levels, level 2 and level 3, are optional.

Tenant Management on Out of Band Management-enabled System Manager

By default, the Multi Tenancy feature is disabled on System Manager when Out of Band Management is enabled. You must enable Multi Tenancy on Out of Band Management-enabled System Manager for the Tenant Management administrator to manage tenant users.

For more information about configuring Multi Tenancy on Out of Band Management-enabled System Manager, see *Deploying Avaya Aura® System Manager in Virtualized Environment*.

Related links

Tenant Management web console on page 39

Enabling Multi Tenancy

Before you begin

Log on to the System Manager web console as Service Provider Administrator or Tenant Administrator.

About this task

To perform tenant-related administration, you must enable the Multi Tenancy feature on System Manager web console.

After you enable the Multi Tenancy feature, you cannot disable the feature. To disable the Multi Tenancy feature, you must reinstall System Manager. By default, the system disables the Multi Tenancy feature.

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Settings** > **SMGR**.
3. On the View Profile:SMGR page, click **Edit**.

   The system displays the Edit Profile:SMGR page.
4. In Multi Tenancy Properties, set **Multi Tenancy Status** to `true`.
5. Click **Commit**.
6. Log off from System Manager, and log on to System Manager again.

   The administrator can now manage tenants from the **Services** > **Tenant Management** page on the System Manager web console.

Related links

Edit Profile:SMGR field descriptions on page 811
Tenant Management field descriptions on page 1132
Create Tenant field descriptions on page 1132

Creating a tenant

Before you begin

- Log on to the System Manager web console as Service Provider Administrator or Tenant Administrator.
- Enable the Multi Tenancy feature.
- After you enable Multi Tenancy, log off and log on to the System Manager web console again.

About this task

Use the procedure to create a tenant, assign a tenant administrator to the tenant, create tenant organization, and assign elements and user provisioning rule.

You can create one or more tenants.

System Manager supports a maximum of 250 tenant partitions as part of System Manager Multi Tenant Management.

Procedure

1. On the System Manager web console, click **Services** > **Tenant Management**.
2. On the Tenant Management page, click **New Tenant**.

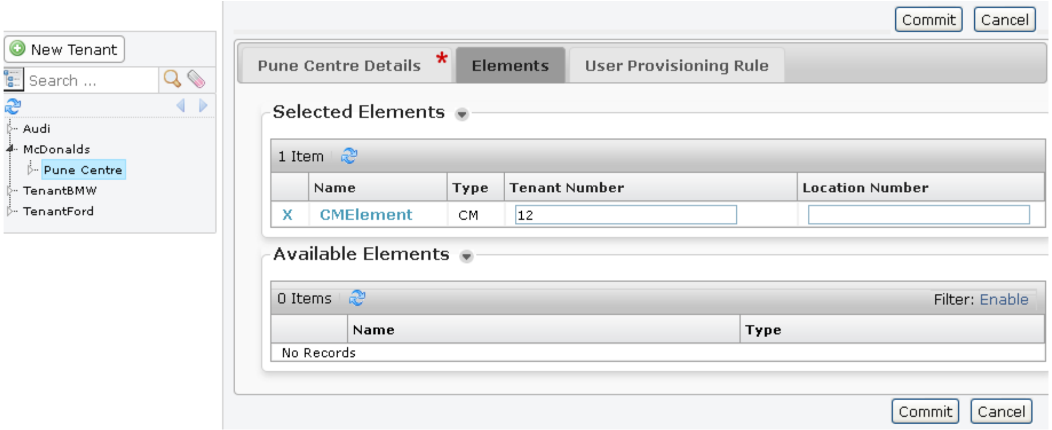
   The system displays the Create Tenant page.
3. On the Tenant Details tab, provide the details for the tenant.

   For more information, see Create Tenant field descriptions.
4. On the Administrators tab, in the Assigned Admin Users section, perform the following:
   a. Click **New**.
   b. In the Create Admin User area, provide the details of the administrator that you want to assign to the tenant.
   c. Click **Commit**.
5. **(Optional)** On the Organization Hierarchy tab, in the Organization level names section, change the names for **Level 1**, **Level 2**, and **Level 3**.

   Level 2 and Level 3 are optional.
6. To view the new tenant node, click **Update Hierarchy**.

   If you do not click **Update Hierarchy**, the page does not display the new tenant that you created. Therefore, you cannot add a site to this tenant.
7. Perform the following to add a site or level 1 organization to the tenant:
   a. In the Tenant Hierarchy section, select the tenant that you created and click **Add**.
   b. Provide the following details for the site:
      - **Site Details**: Details of the site. For more information, see Create Tenant field descriptions.
      - **Elements**: Perform the following:
        a. To assign an element to the site, click the plus sign (**+**) in the Available Elements section.

           Click ✕ to unassign an element if required. You can assign more than one element to a site. The Selected Elements section displays the elements that you assign to the site. Provide the tenant number or tenant ID and the location number for the element.



Audi
McDonalds
Pune Centre
TenantBMW
TenantFord

Selected Elements

1 Item

	Name	Type	Tenant Number	Location Number
X	CMElement	CM	12	

Available Elements

0 Items — Filter: Enable

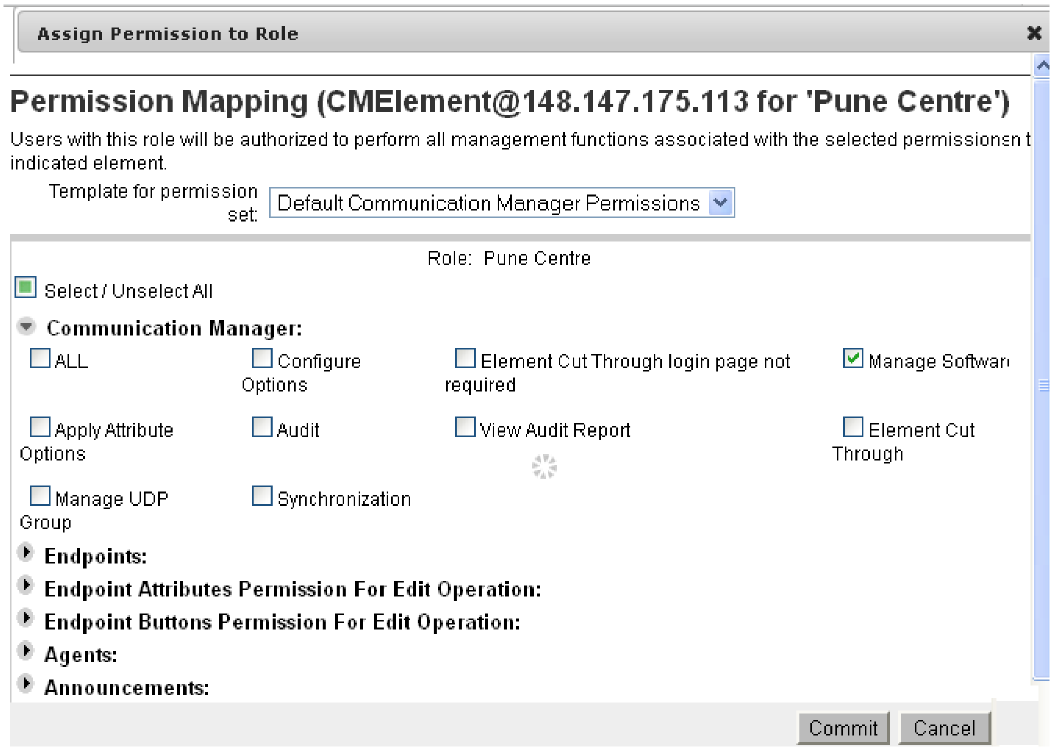
Name	Type
No Records	

Note:

The Communication Manager element that you select in the Elements tab and the User Provisioning Rule tab must be the same. If you select a different Communication Manager element, the tenant creation fails.

b. To assign permissions to the tenant administrator, click the element, select the permissions on the Permission Mappings page, and click **Commit**.

For more information, see the “Managing roles”.



Permission Mapping (CMElement@148.147.175.113 for 'Pune Centre')

Users with this role will be authorized to perform all management functions associated with the selected permissionsn t indicated element.

Template for permission set: Default Communication Manager Permissions

Role: Pune Centre

☑ Select / Unselect All

Communication Manager:

□ ALL
□ Configure Options
□ Element Cut Through login page not required
☑ Manage Softwar
□ Apply Attribute Options
□ Audit
□ View Audit Report
□ Element Cut Through
□ Manage UDP Group
□ Synchronization

Endpoints:

Endpoint Attributes Permission For Edit Operation:

Endpoint Buttons Permission For Edit Operation:

Agents:

Announcements:

Note:

For Communication Manager, do not provide permissions for Audit, Element Cut Through, and Synchronization functions.

- **User Provisioning Rule**: Click the plus sign (+) in the Available User Provisioning Rules section to assign a rule to the site. Click ✕ to unassign a user provisioning rule.

c. Click **Update Hierarchy** to view the new site in the tenant organization.

The system displays the site that you added to the tenant.

If you do not click **Update Hierarchy**, the system does not display the new site that you created. Therefore, you cannot add a department to this site.

Note:

Add at least one site for the tenant.

d. Repeat Step a through Step c to add more than one site for the tenant.

8. **(Optional)** Perform the following to add a department or level 2 organization to the site:

a. In the Tenant Hierarchy section, select the site, and click **Add**.

b. Provide the details for the department.

c. Click **Update Hierarchy** to view the new department in the tenant organization.

If you do not click Update Hierarchy, the system does not display the new department that you created. Therefore, you cannot add a team to this department.

d. Repeat Step a through Step c to add more than one department for the site.

9. **(Optional)** Perform the following to add a team or level 3 organization to the department:

a. In the Tenant Hierarchy section, select the department, and click **Add**.

b. Provide the details for the team.

c. Click **Update Hierarchy** to view the new team in the tenant organization.

If you do not click **Update Hierarchy**, the system does not display the new team that you created.

d. Repeat Step a through Step c to add more than one team for the department.

10. Click **Commit**.

The system displays the tenant organization on the Tenant Management page.

11. Repeat Step 2 through Step 9 to create more than one tenant.

Related links

Adding a custom tenant administrator role on page 149
Adding a custom tenant administrator role on page 149
Unassigning the tenant administrator on page 1125
Tenant Management field descriptions on page 1132
Create Tenant field descriptions on page 1132

Assigning the tenant administrator to the tenant

Before you begin

- Log on to the System Manager web console as the Cloud Service Provider administrator.
- Enable the Multi Tenancy feature.

Procedure

1. On the System Manager web console, click **Services** > **Tenant Management**.
2. On the Tenant Management page, select a tenant in the left pane, and click the **Administrators** tab.
3. In the **Assigned Admin Users** section, perform one of the following steps:
   - Click **Edit** or **Search** and select the administrator that you must assign to this tenant.
   - Perform the following:
     a. Click **New**.
     b. In the **Create Admin User** area, provide the details of the administrator that you must assign to the tenant.
     c. Click **Commit**.

   The system assigns the tenant administrator to the tenant.

Unassigning the tenant administrator

Before you begin

- Log on to the System Manager web console as the Service Provider Administrator.
- Enable the Multi Tenancy feature.
- Create the tenant.

Procedure

1. On the System Manager web console, click **Services** > **Tenant Management**.
2. On the Tenant Management page, select the tenant in the left pane, and click the **Administrators** tab.
3. In the **Assigned Admin Users** section, click **Edit** or **Search**, and select the administrator that you must unassign.
4. Click **Unassign**.
5. Click **Commit**.

   The system removes the association of the tenant administrator with the tenant.

Related links

Tenant Management field descriptions on page 1132
Create Tenant field descriptions on page 1132

Viewing the tenant

Before you begin

- Log on to System Manager Web Console.
- Enable the Multi Tenancy feature.
- Create a tenant.

Procedure

1. On the System Manager web console, click **Services** > **Tenant Management**.
2. From the tenant organization, click the tenant, site, department, or team that you must view.
3. View the details of Tenant, Site, Department, or Team.

Related links

Tenant Management field descriptions on page 1132
Create Tenant field descriptions on page 1132

Modifying the tenant

Before you begin

- Log on to the System Manager web console as Service Provider Administrator or Tenant Administrator.
- Enable the Multi Tenancy feature.

About this task

Use the procedure to modify the following:

- The tenant, organization hierarchy, and tenant administrator details.
- The assignment of elements, user provisioning rule, and resource permissions to the site.

Procedure

1. On the System Manager web console, click **Services** > **Tenant Management**.
2. On the Tenant Management page, select the tenant, site, department, or team that you must modify.
3. Click **Edit**.

4. Modify the following information as appropriate:
   - Tenant details, tenant administrator, and organization hierarchy labels
   - Site details, assignment of elements, user provisioning rule, and permissions to the site
   - Department details
   - Team details

   For information, see Create Tenant field descriptions.
5. Click **Commit**.

Related links

[Tenant Management field descriptions](#) on page 1132

[Create Tenant field descriptions](#) on page 1132

Deleting a tenant

The Service Provider Administrator can delete the tenant and the tenant organization hierarchy.

Before you begin

- Log on to System Manager Web Console as Service Provider Administrator.
- Enable the Multi Tenancy feature.
- Delete all users associated with the tenant.

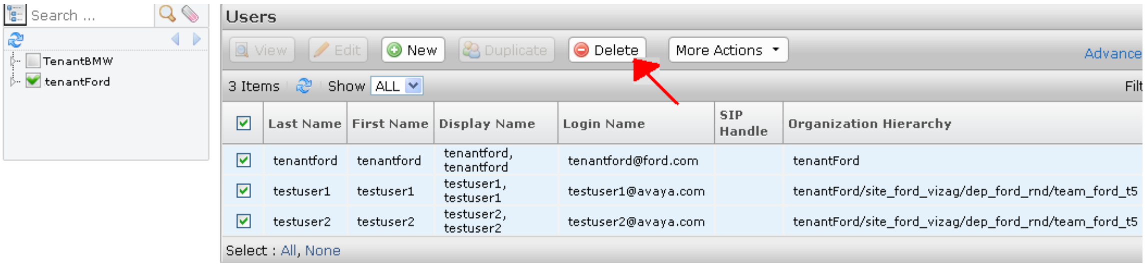
Procedure

1. On the System Manager web console, click **Services** > **Tenant Management**.
2. On the Tenant Management page, select the tenant that you must delete.
3. Click Delete.

   If any users associated with the tenant exist, the system displays a message to delete all users.
4. **(Optional)** Perform the following steps to delete users associated with the tenant:

   a. On the User Management page, in the tenant organization, select a tenant.

      The system displays the users associated with this tenant on the right pane. You can search for a tenant if you cannot view the tenant in the left pane.



☑	Last Name	First Name	Display Name	Login Name	SIP Handle	Organization Hierarchy
☑	tenantford	tenantford	tenantford, tenantford	tenantford@ford.com		tenantFord
☑	testuser1	testuser1	testuser1, testuser1	testuser1@avaya.com		tenantFord/site_ford_vizag/dep_ford_rnd/team_ford_t5
☑	testuser2	testuser2	testuser2, testuser2	testuser2@avaya.com		tenantFord/site_ford_vizag/dep_ford_rnd/team_ford_t5

   b. Select the users, and click **Delete**.
   c. On the User Delete Confirmation page, click **Delete**.

      The system deletes the users that are associated with the tenant.

5. On the Organization Unit Delete Confirmation page, click **Delete**.

   The system deletes the tenant, tenant administrator, and all roles created for the tenant, sites, departments, and organization for the tenant.

Related links

Tenant Management field descriptions on page 1132
Create Tenant field descriptions on page 1132

Multi Tenancy for Avaya SIP AST endpoints

During the search for enterprise users that must be added as contacts, Avaya SIP AST endpoints retrieve the enterprise users from:

- The tenant partition to which the enterprise user who started the search belongs
- The enterprise users in the default tenant partition
- All public contacts

Multi Tenancy for Communication Manager objects

With the Multi Tenancy feature, Communication Manager provides telecommunication services to multiple, independent groups of users through a single Communication Manager server. Each tenant appears to have a dedicated Communication Manager server, though in reality, the tenants share the same Communication Manager server.

As an administrator, you can gain access to one or more tenant partitions in System Manager, and you can administer tenant numbers for several Communication Manager objects. You can segregate tenants through tenant numbers. The following Communication Manager objects support Multi Tenancy:

- Agents
- Announcements
- VDN
- Endpoints
- Term Extension Group
- Trunk Group

- Hunt Group

When a user is added to a tenant, the **Tenant Number** field is autopopulated for these Communication Manager objects.

The Communication Manager Objects page displays specific Communication Manager objects based on the tenant permissions and the Communication Manager permissions that you specify.

Note:

For a Communication Manager instance, do not assign the same tenant number for more than one tenant.

After the tenant administrator selects the site and the tenant from the Tenant Management web console, the Communication Manager Objects page displays the tenant and site combination. Depending on the tenant and site a user selects, the tenant range and tenant permissions take effect.

Multi Tenancy and tenant partitioning in Communication Manager

The native tenant partitioning feature of Communication Manager provides multiple services to independent groups of users through a single Communication Manager server. Communication Manager also offers the following features:

- Segmenting call processing and feature processing by the Inter-Tenant Communications Control (ITCC) feature
- Tenant management of users and system administrators through System Manager

With System Manager Inter-tenant Communication Control (ITCC), Communication Manager can segregate features for each customer. System Manager tenants are shared across multiple adopters. Communication Manager is one of the adopters. Based on the roles and permissions assigned on the Communication Manager instances in a tenant, the Communication Manager objects are segregated for the tenant.

Notes on Multi Tenancy for Communication Manager

Scheduling jobs with Multi Tenancy

When the Multi Tenancy feature is enabled you cannot schedule the following operations:

- Clear amw
- Delete station
- Delete agent
- Delete announcement
- Backing up announcements
- Backing up all announcements
- Restoring announcements
- Restoring all announcements

- Moving announcements
- Broadcasting announcements
- Bulk operations including adding stations in bulk, deleting stations in bulk, adding agents in bulk, deleting agents in bulk, editing agents in bulk
- Global endpoint change

Tenant administrators cannot delete Communication Manager objects in System Manager. To assign delete permissions to a tenant administrator, the Service Provider Administrator must provide delete and scheduler permissions to the tenant administrator.

This will not impact the current implementation of Element Cut Through, notify sync, and adding Off PBX entries for a SIP station.

User Provisioning Rule and Multi Tenancy

When you assign a user provisioning rule to a tenant, the same Communication Manager element must be present in User Provisioning Rule and Elements tabs. If the Communication Manager element that you selected is available in the User Provisioning Rule tab but unavailable in the Elements tab, the tenant creation fails.

When you create a new tenant, the system validates the tenant number based on the Communication Manager that you selected. Depending on the tenant configuration in the Communication Manager you selected, you can choose a tenant number between 1 to 100 or 1 to 250.

User Management and Multi Tenancy

When you enable the Multi Tenancy feature, and you choose the tenant and site for a user in User Management, the system displays Communication Manager **System** in the endpoint agent communication profile sections based on the tenant and site values you selected in the Identity tab. The User Management values override the values selected on the **Multi Tenancy** dashboard.

The system displays the available extensions in the endpoint, agent communication profile sections according to the tenant and Communication Manager permissions.

Field level permissions and Multi Tenancy

Apart from the tenant permissions, object-level and field-level permissions are also valid for the tenant hierarchies. For example, admin A with access to Tenant Partition 1 can modify hunt-group 12 in Tenant Partition 1, but admin A cannot assign a station in Tenant Partition 2 to that hunt group.

The object and field-level permissions are valid for the following objects:

Communication Manager object	Fields
Hunt Group	Group Number Range Group Extension Member Extensions Night Attendant Extension
Agents	Agent Login ID Coverage Path

Table continues…

Communication Manager object	Fields
	Port Extension COR Tenant Number
VDN	Extension COR Tenant Number VDN of Origin Annc Extension Return Destination Conference Controller for meetme
Endpoint	COR Emergency Location Extension Message Lamp Extension Tenant Number Media Complex Extension Hunt-to Station
Terminating Extension Group	Group Extension COR Tenant Number 4 Extension fields
Trunk Group	COR Tenant Number Incoming Destination Night Service Extension List of Trunk Group Data

- Do not provide Element Cut-Through access for a tenant administrator, because the administrator can bypass the tenant restrictions.
- In the Tenant Management web console, when the tenant administrator assigns a single number or a range in the **Tenant Number** field, the Communication Manager that the administrator selects is associated with the tenants.

  The **Tenant Number** field is autopopulated for the Communication Manager objects that you create through Communication Manager. In the **Tenant Number** field, you can specify only the values or range that you configured in System Manager. If you specify a range, the system uses the smallest value in the tenant range. This scenario is also valid when you create Communication Manager objects such as endpoints or agents using User Management or Directory Synchronization.
- When you create tenants, if you specify the location, then you can enter only valid values. Location can be a single number, a range, or blank. When you enable multi-location field in

System-Parameters customer-options, the availabe values for the **Location Number** field are 1 to 250 for Communication Manager 6.0 and 6.2, and 1 to 2000 for Communication Manager 6.3 and later. You must type `blank` or leave the **Location** field blank to choose blank as a value for tenant objects. For example, to specify blank and the range 1 to 10, you must type `blank,1:10` in the **Location** field.

- When you change or select a template, the **Tenant Number** in the template takes precedence over the smallest, default tenant value. This scenario is valid only if the tenant number present in the template is within the valid tenant range. Otherwise, the system uses the smallest value in the specified tenant range. The value in the **Location** field specified in the template also takes precedence over the default value. The system validates against incorrect and out of range values.

Tenant Management field descriptions

Tenant Hierarchy

Button	Description
New Tenant	Displays the Create Tenant page where you can create new tenants and the organization hierarchy.
Add	Displays the following tabs when you select a tenant and click **Add**. • **Level 1 Details** or **Site Details** • **Elements** • **User Provisioning Rule**
	Displays the **Department Details** section when you select the level 1 or site, and click **Add**.
	Displays the **Team Details** section when you select the level 2 or department, and click **Add**.

Icon	Name	Description
🔍	Search	Searches for the tenant that you specified.
✏	Clear	Clears the search text.

Create Tenant field descriptions

The system displays the Create Tenant page when you click **New Tenant** or select a tenant organization from the tree.

Note:

Fields marked with an asterisk are mandatory.

Tenant Details

Name	Description
Name	The name or unique identifier of the tenant.
Contact ID	The contact ID of the tenant.
Max no of users	The maximum number of users that an administrator can associate with this tenant. This number does not include admin users who can manage this tenant but are not associated with this tenant. You can administer 10–250000 end users in System Manager. The default is 10.
Description	A brief description of the tenant.

Administrators

The Assigned Admin Users section displays the fields in the Create Admin User area when you click **New**.

Name	Description
First Name	The first name of the administrator.
Last Name	The last name of the administrator.
Login	The login name of the administrator. The login name must be a fully qualified domain name. For example, jmiller@avaya.com.
Password	The password to log on to the System Manager web console.
Confirm Password	The password that you must re-enter for confirmation.

Button	Description
New	Creates a new tenant administrator with the details that you provide.
Search	Searches for the administrator using the search criteria that you provide.
Unassign	Removes the administrator that you selected.
Commit	Saves the administrator details that you provided.
Cancel	Cancels the operation.

Organization Hierarchy

The page displays the fields in the Organization Level Names area.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><b>Level 1</b></td><td>The name for level 1.
<table>
<tr><th>Organization level</th><th>Default</th><th>Example</th></tr>
<tr><td>Level 1</td><td>Site</td><td>Hyderabad</td></tr>
<tr><td>Level 2</td><td>Department</td><td>Loans Division</td></tr>
<tr><td>Level 3</td><td>Team</td><td>Customer Relations</td></tr>
</table>
</td></tr>
<tr><td><b>Level 2</b></td><td>The name for level 2. The field is optional.</td></tr>
<tr><td><b>Level 3</b></td><td>The name for level 3. The field is optional.</td></tr>
</table>

Button	Description
Update Hierarchy	The system performs the following: • Refreshes the page with the details that you provided during the creation of the tenant, site, department, and team. • Displays the tenant node that you created. • Displays the level 1 or site that you created. • Displays the level 2 or department that you created. • Displays the level 3 or team. **Note:** The system displays the newly created organizational unit only when you click **Update Hierarchy**.
Commit	Saves the changes you made to the tenant, site, department, or team, and displays the Tenant Management page.
Cancel	Cancels the current operation.

Level 1 Details or Site Details

The system displays the Level 1 Details or Site Details, Elements, and User Provisioning Rule tabs only when you select a tenant, and click **Add**.

Name	Description
Name	The name of the level 1 hierarchy or site.
Address	The address of the level 1 hierarchy or site.
Description	A brief description of the level 1 hierarchy or site.

Elements

Name	Description
Selected Elements	The elements that you can assign to the level 1 hierarchy or site. The system adds the elements to the section from the **Available Elements** section when you click the plus sign (+). **Note:** The element that you select in the **Elements** tab and the **User Provisioning Rule** tab must be the same. If you select a different element, the tenant creation fails.
X	Unassigns the element from the level 1 hierarchy or site. The system displays the element in the **Available Elements** section.
Name	The name of the element.
Type	The element type.
Tenant No.	The tenant unique identifier. The **Tenant No.** and **Location No**. must be created in the element before you associate the numbers with the tenant. For information, see the documentation for the appropriate element.
Location No.	The site that contains elements and other network element resources. For example, Communication Manager, Session Manager, endpoints, and other resources.
Available Elements	
+	Click to assign the element to the site.
Name	The name of the element.
Type	The element type.

User Provisioning Rule

Field	Description
Available User Provisioning Rules	
Name	The name of the user provisioning rule.
+	Assigns the user provisioning rule to the level 1 hierarchy or site. The system moves the user provisioning rule to the Selected User Provisioning Rules section.

Table continues…

Field	Description
Selected User Provisioning Rules	
Name	The name of the user provisioning rule that you selected from the Available User Provisioning Rules section.
✕	Unassigns the user provisioning rule from the level 1 hierarchy or site. The system moves the user provisioning rule to the Available User Provisioning Rules section.

Level 2 Details or Department Details

The system displays the section when you select a level 1 hierarchy or site, and click **Add**.

Name	Description
Name	The name of the level 2 hierarchy or department.
Description	A brief description of the level 2 hierarchy or department.

Level 3 Details or Team Details

The system displays the section when you select a level 2 hierarchy or department, and click **Add**.

Name	Description
Name	The name of the level 3 hierarchy or team.
Description	A brief description of the level 3 hierarchy or team.

Chapter 24: Shutting down System Manager

Overview

System Manager executes several scheduled processes in the background. When System Manager shuts down, the system must stop the processes that System Manager runs in the background. This is to ensure that the system is stable and does not contain incomplete data in any data store when System Manager starts the next time. The system must also ensure that the background process that stops does not leave the system in an unstable state.

The shutdown process stops all running jobs and then shuts down System Manager.

Note:

You cannot cancel the process after you select the shutdown process.

To ensure that System Manager shuts down completely, the shutdown feature provides a user interface that displays all scheduled jobs that are running on System Manager and active user sessions. Based on the criticality and priority of scheduled jobs, the administrator can shut down the system immediately or wait for the scheduled jobs to complete.

- If the administrator chooses to shut down the system, the shutdown service performs the following actions:
    - Sends the shutdown notification to active users so that users can commit or rollback the operation. The shutdown framework waits for the specified grace period that the administrator sets for active users to complete the operations.
    - Sends the shutdown signal to the Scheduler of System Manager to interrupt the running jobs. Scheduler service must not start any new scheduled jobs.
    - Blocks access to the System Manager web console during a shutdown. After the grace period, the system disallows new logins. The system stops all existing sessions when the shutdown begins and redirects the sessions to the Login page. The system displays `Shutdown in progress` message on Login page.
    - Logs an audit message indicating that a request for shutdown is made.
    - Makes an entry in a file about the shutdown request. The system uses the shutdown request information to display the shutdown history.
    - Shuts down all applicable services such as JBoss, Postgres, and CND.

  - If any of the steps fail, the system logs a message and performs the next step.
- Administrator can shut down System Manager from the command line interface or System Manager web console.

Shutting down System Manager from the Web console

Before you begin

Log on to System Manager web console of the active server.

About this task

You cannot gain access to System Manager Web Console during the shutdown process.

Procedure

1. On the System Manager web console, click **Services** > **Shutdown**.
2. In the left navigation pane, click **Shutdown** > **Shutdown System Manager**.
3. On the Initiate Shutdown page, perform one of the following actions:
   - Wait for the completion of jobs running on System Manager, and then click **Shutdown**.
   - Click **Shutdown** to shut down System Manager immediately.
4. To see the history of the last shutdown actions, click **Shutdown** > **Shutdown History**.

   The Shutdown History page displays the date, time, and status of the shutdown action.

Related links

Edit Profile:Shutdown field descriptions on page 815
View Profile:Shutdown field descriptions on page 814

Chapter 25: Solution deployment and upgrade

Solution Deployment Manager

Solution Deployment Manager overview

Solution Deployment Manager is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to suite of Avaya Aura® 7.0 applications. Solution Deployment Manager supports the operations on customer Virtualized Environment and Avaya-provided appliance model.

Solution Deployment Manager provides the combined capabilities that Software Management, Avaya Virtual Application Manager, and System Platform provided in earlier releases.

System Manager Release 7.0 is the primary management solution for Avaya Aura® 7.0 applications.

System Manager with the Solution Deployment Manager runs on:

- An Avaya-provided appliance: Contains server, Appliance Virtualization Platform, and Avaya Aura® application OVA. Appliance Virtualization Platform includes a VMware ESXi 5.5 hypervisor.

  From Release 7.0, Appliance Virtualization Platform replaces System Platform.
- Customer-provided Virtualized Environment solution: Avaya Aura® applications are deployed on customer-provided, certified VMware® hardware.

With Solution Deployment Manager, you can perform the following operations in Virtualized Environment and Avaya appliance models.

- Deploy Avaya Aura® applications
- Upgrade and migrate Avaya Aura® applications
- Download Avaya Aura® applications
- Install service packs, feature packs, and software patches for the following Avaya Aura® applications:
  - Communication Manager and associated devices, such as gateways, media modules, and TN boards.
  - Session Manager
  - Branch Session Manager

  - Utility Services
  - Appliance Virtualization Platform. The ESXi host running on Avaya-provided appliance.

The upgrade process involves the following key tasks:

- Discover the Avaya Aura® application.
- Analyze and download the necessary software components.
- Run the preupgrade check to ensure successful upgrade environment.
- Upgrade the Avaya Aura® application.

Solution Deployment Manager options

Avaya provides the following Solution Deployment Manager options:

- Centralized Solution Deployment Manager: The System Manager capability to deploy, upgrade, migrate, and install software patches for Avaya Aura® applications. Release 7.0 supports migration of System Platform-based Avaya Aura® 6.x applications to Release 7.0 on Avaya-provided appliance.

  However, in Release 7.0, Solution Deployment Manager does not support migration of Virtualized Environment-based 6.x applications to 7.0 in customer Virtualized Environment. Use vSphere Client to migrate to customer Virtualized Environment.

- Solution Deployment Manager client: A lightweight tool that can reside on the computer of a technician. The technician can gain access to the client by using the web browser.

  Use the Solution Deployment Manager client to:

  - Deploy virtual appliances on Virtualized Environment or Avaya-provided appliance.
  - Upgrade System Manager, install System Manager patches, and install hypervisor patches.
  - Start, stop, and restart a virtual machine.
  - Change the footprint size based on the capacity requirements of the Avaya Aura® application.

The centralized and client Solution Deployment Manager provide the following capabilities:

Centralized Solution Deployment Manager	Solution Deployment Manager client
Manage virtual machine lifecycle	Manage virtual machine lifecycle
Deploy Avaya Aura® applications	Deploy Avaya Aura® applications
Deploy hypervisor patches only for Appliance Virtualization Platform	Deploy hypervisor patches only for Appliance Virtualization Platform
Upgrade Avaya Aura® applications Release 7.0 supports upgrades from Linux-based or System Platform-based to Virtualized Environment or Appliance Virtualization Platform. Release 7.0 does	Upgrade System Platform-based System Manager

Table continues…

Centralized Solution Deployment Manager	Solution Deployment Manager client
not support Virtualized Environment to Virtualized Environment upgrades.	
Install software patches for Avaya Aura® applications	Install System Manager patches
Discover Avaya Aura® applications	Deploy System Manager
Analyze Avaya Aura® applications	-
Create and use the software library	-

Solution Deployment Manager client

For the initial System Manager deployment or when System Manager is inaccessible, you can use the Solution Deployment Manager client. The client can reside on the computer of the technician. The Solution Deployment Manager client provides the functionality to install the OVAs on an Avaya-provided server or customer-provided Virtualized Environment. The user interface of the Solution Deployment Manager client looks similar to the centralized Solution Deployment Manager.

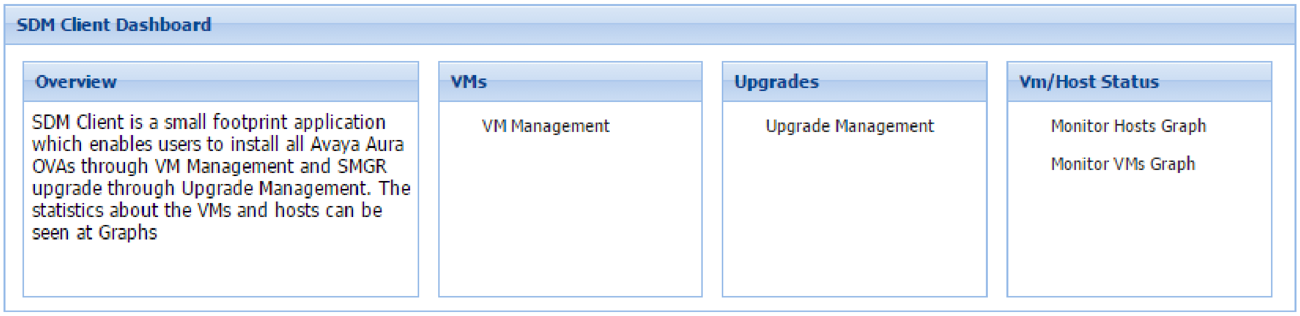
System Manager supports the Solution Deployment Manager client. A technician can gain access to the user interface of the Solution Deployment Manager client from the computer or web browser.

The Solution Deployment Manager client runs on Windows 7.0 and Windows 8, 64 bit.

Use the Solution Deployment Manager client to:

- Deploy System Manager and Avaya Aura® applications on Virtualized Environment or Avaya appliances.
- Upgrade System Platform-based System Manager and install System Manager and hypervisor patches.
- Start, stop, and restart a virtual machine.
- Change the footprint size based on the capacity requirements of the Avaya Aura® application.

You can deploy or upgrade the System Manager virtual machine only by using the Solution Deployment Manager client.



SDM Client is a small footprint application which enables users to install all Avaya Aura OVAs through VM Management and SMGR upgrade through Upgrade Management. The statistics about the VMs and hosts can be seen at Graphs

Figure 1: Solution Deployment Manager client dashboard

Related links

Installing the Solution Deployment Manager client on your computer on page 1142

Accessing the Solution Deployment Manager client dashboard on page 1144
Solution Deployment Manager client capabilities on page 1145

Installing the Solution Deployment Manager client on your computer

About this task

In Avaya-appliance offer, when the centralized Solution Deployment Manager on System Manager is unavailable, use the Solution Deployment Manager client to deploy the Avaya Aura® applications.

You can use the Solution Deployment Manager client to install software patches and hypervisor patches.

Use the Solution Deployment Manager client to deploy, upgrade, and update System Manager.

Important:

For deployments through service port by using the Solution Deployment Manager client, get the Solution Deployment Manager client software from the Avaya support site at http://support.avaya.com. The Solution Deployment Manager client software version available in the media does not support the service port deployment.

Before you begin

1. Ensure that Windows 7.0 or 8.1 operating system is installed on the computer.

   Tip:

   On **Computer**, right-click properties, and ensure that Windows edition section displays the version of Windows operating system.

2. Ensure that at least 5 GB of disk space is available at the location where you want to install the client.

   Tip:

   In the explorer, click **Computer**, and verify that the Hard Disk Drives section displays the available disk space available.

3. To avoid port conflict, stop any application server that is running on your computer.

   Tip:

   From the system tray, open the application service monitor, select the application server that you want to stop, and click **Stop**.

4. Ensure that the firewall allows the ports that are required to install the Solution Deployment Manager client installation and use the Solution Deployment Manager functionality.
5. Ensure that 443 and 1527 ports are available.
6. Close all applications that are running on your computer.
7. Do not set CATALINA_HOME as environment variable on the computer where you install the Solution Deployment Manager client.

Tip:

On **Computer**, right-click properties, and perform the following:

a. In the left navigation pane, click **Advanced system settings**.

b. On the System Properties dialog box, click Advanced tab, and click **Environment Variables**.

c. Verify the system variables.

8. Ensure that the computer on which the Solution Deployment Manager client is running is connected to the network.

   Any operation that you perform might fail if the computer is not connected to the network.

Procedure

1. Download the `Avaya_SDMClient_win64_7.0.0.1.17824_7.zip` file from the Avaya PLDS website at https://plds.avaya.com/.

   On the Avaya PLDS website, you can provide the application name as **System Manager**, and version as **7.0**.

2. Copy the zip file, and extract to a location on your computer by using the WinZip application.
3. Using the **Run as administrator** option, run the `Avaya_SDMClient_win64_7.0.0.1.17824_7.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.

4. On the Welcome page, click **Next**.
5. On the License Agreement page, click **I accept the terms of the license agreement** and click **Next**.
6. On the Install Location page, perform one of the following:
   - To install the Solution Deployment Manager client in the system-defined folder, click **Restore Default Folder**.
   - To specify a different location for installation, click **Choose** and browse to an empty folder.
7. Click **Next**.
8. On the Preinstallation Summary page, review the information, and click **Next**.
9. On the Summary and Validation page, perform the following:

   a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.

   b. To change the default directory, in Select Location of Software Library Directory, click **Choose** and select a directory.

   The system saves the artifacts in the specified directory. During deployments, you can select the OVA file from the directory.

   c. Verify the product information and the system requirements.

The system performs the feasibility checks, such as disk space and memory. If the requirements are not met, the system displays an error message. To continue with the installation, make the disk space, memory, and the ports available.

Important:

If port 443 is unavailable, verify if the Skype application is running on the computer, and quit the application. If you close Skype, the application continues to run in the background. For more information, see “Solution Deployment Manager client installation fails” in *Troubleshooting Avaya Aura® System Manager*.

10. Click **Install**.
11. To exit the installer, on the Install Complete page, click **Delete**.

    The installer creates a shortcut on the desktop.
12. To start the client, click SDM CLIENT.

Next steps

To enable the Solution Deployment Manager client to communicate with the services port of Appliance Virtualization Platform, set the following on the technician computer:

- IP address: 192.168.13.5
- Netmask: 255.255.248
- Gateway: 192.168.13.1

Related links

Solution Deployment Manager client on page 1141

Accessing the Solution Deployment Manager client dashboard

About this task

Note:

If you perform deploy, upgrade, and update operations from the Solution Deployment Manager client, ignore the steps that instruct you to access System Manager Solution Deployment Manager and the related navigation links.

Procedure

To start the Solution Deployment Manager client, perform one of the following:

- Click **Start** > **All Programs** > **Avaya**, and click **SDM Client** > **Avaya SDM Client**.
- Click SDM CLIENT.

Related links

Solution Deployment Manager client on page 1141

Solution Deployment Manager client capabilities

The Solution Deployment Manager client provides the following capabilities and functionality:

- Runs on the technician computer on the following operating systems:
  - Windows 7 Professional or Enterprise
  - Windows 8.1 Professional or Enterprise
- Supports the same web browsers as System Manager Release 7.0.
- Provides the user interface with similar look and feel as the central Solution Deployment Manager in System Manager Release 7.0
- Supports deploying the System Manager OVA. The Solution Deployment Manager client is the only option to deploy System Manager.
- Supports Flexible footprint feature. The size of the virtual resources depends on the capacity requirements of the Avaya Aura® applications.
- Defines the physical location, Appliance Virtualization Platform or ESXi host, and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Manages lifecycle of the OVA applications that are deployed on the ESXi host. The lifecycle includes start, stop, and reset virtual machines.
- Deploys the Avaya Aura® applications that can be deployed from the central Solution Deployment Manager for Avaya-provided appliance and customer Virtualized Environment. You can deploy one application at a time.
- Configures application and networking parameters required for application deployments.
- Supports the local computer or an HTTP URL to select the application OVA file for deployment. You do not need access to PLDS.
- Supports changing the hypervisor IP address on Appliance Virtualization Platform.
- Supports installing patches for the hypervisor on Appliance Virtualization Platform.
- Supports installing patches for only System Manager.

  Avaya Aura® applications must use centralized Solution Deployment Manager from System Manager to install software patches.

Related links

Solution Deployment Manager client on page 1141

Solution Deployment Manager

The Solution Deployment Manager capability simplifies and automates the deployment and upgrade process.

With Solution Deployment Manager, you can deploy the following Avaya Aura® Release 7.0 applications:

- Utility Services 7.0
- System Manager 7.0
- Session Manager 7.0
- Branch Session Manager 7.0
- Communication Manager 7.0
- Application Enablement Services 7.0
- WebLM 7.0
- Engagement Development Platform 3.1
- SAL 2.5
- Communication Manager Messaging 7.0
- Avaya Aura® Media Server 7.7

With Solution Deployment Manager, you can migrate, upgrade, and update the following applications:

- Linux-based Communication Manager and the associated devices, such as Gateways, TN boards, and media modules.
- Linux-based Session Manager
- System Platform-based Communication Manager
    - Duplex CM Main / Survivable Core with Communication Manager
    - Simplex CM Main / Survivable Core with Communication Manager, Communication Manager Messaging, and Utility Services
    - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
    - Embedded CM Main with Communication Manager, Communication Manager Messaging, and Utility Services
    - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- System Platform-based Branch Session Manager
    - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
    - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services

Note:

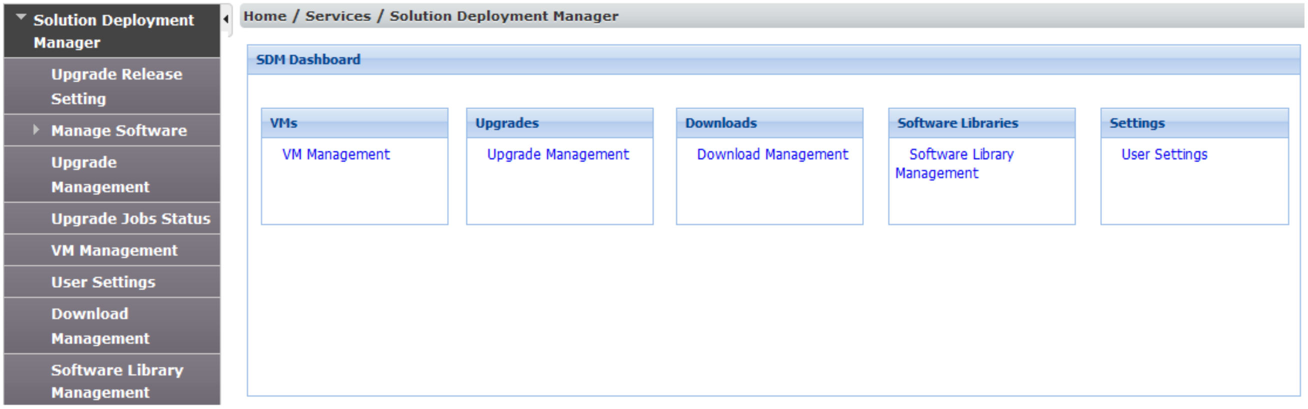
However, you must manually migrate Services VM that is part of the template.

You require only one SAL or Services VM per enterprise to support an Avaya Services offer.

The centralized deployment and upgrade process provide better support to customers who want to upgrade their systems to Avaya Aura® Release 7.0. The process reduces the upgrade time and error rate.

Solution Deployment Manager dashboard

You can gain access to the Solution Deployment Manager dashboard from the System Manager web console or by installing the Solution Deployment Manager client.



Solution Deployment Manager capabilities

With Solution Deployment Manager, you can perform deployment and upgrade-related tasks by using the following links:

- **Upgrade Release Setting**: To select **Release 7.0** or **6.3.8** as the target upgrade. Release 7.0 is the default upgrade target.
- **Manage Software**: To upgrade the legacy IP Office and B5800.
- **VM Management**: To deploy OVA files for the supported Avaya Aura® application.
- **Upgrade Management**: To upgrade Communication Manager that includes TN boards, media gateways and media modules, Session Manager, Communication Manager Messaging, Utility Services, Branch Session Manager to Release 7.0.
- **User Settings**: To configure the location from where System Manager displays information about the latest software and firmware releases.
- **Download Management**: To download the OVA files and firmware to which the customer is entitled. The download source can be the Avaya PLDS or an alternate source.
- **Software Library Management**: To configure the local or remote software library for storing the downloaded software and firmware files.

Solution Deployment Manager configuration settings

User settings

You require the PLDS connection to gain access to Avaya from where you can obtain all software and firmware files that are required for upgrade, migration, and updates. Ensure that you add the required ports and websites to the customer firewall. For example, you require access to the ftp.avaya.com website to get the `versions.xml` and http to grant access to plds.avaya.com. If the customer decides not to open PLDS in the organization firewall, an alternate source must be set to access the software. For example, if the customer wants to test the latest versions of software before using the software for production. By using the alternate source, the customers can get the software that is recommended by the analyze operation.

Establishing PLDS connection to Avaya

About this task

Use the procedure to configure the location from where System Manager displays information about the latest software and firmware releases during Analyze operation. The entitlements depend on the credentials that you provide on the **User Settings** page.

Before you begin

- Obtain a company ID to configure PLDS.
- Add the required ports and websites to a firewall of customer.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **User Settings**.
3. On the User Settings page, click **Edit**.
4. Select the **Use Avaya Support Site** check box, and provide the SSO user name and SSO password for PLDS, and the company ID.
5. Configure the PLDS settings and proxy settings for the software download.
6. If your network configuration requires a proxy, select the **Use Proxy** check box, and provide the details.
7. Click **Commit**.

Related links

Obtaining a company ID on page 1149
User Settings field descriptions on page 1151

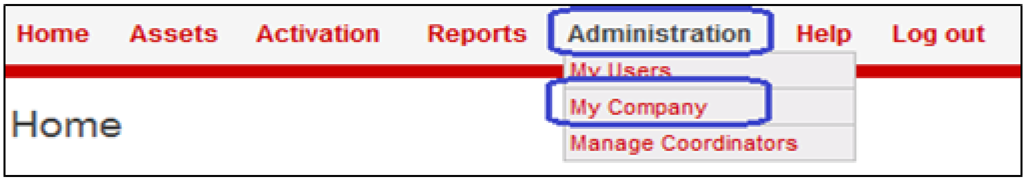
Obtaining a company ID

Before you begin

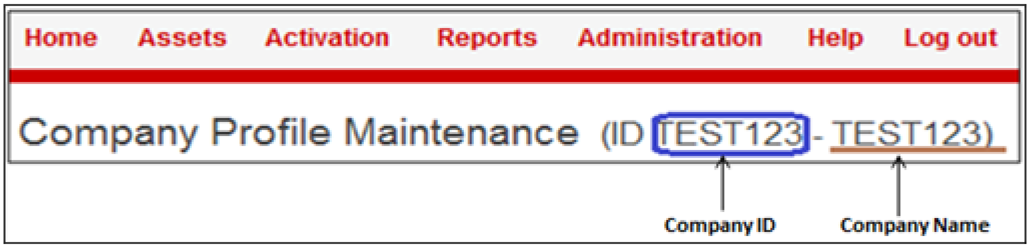
Ensure that you have a access and user credentials to log in to the PLDS website at https://plds.avaya.com.

Procedure

1. On the web browser, type the PLDS URL, `https://plds.avaya.com`.
2. In the **Email address** field, enter the user name, and in the **Password** field, enter the password.
3. Click **Submit**.
4. After successful log in, on the Home page, select **Administration** > **My Company**.



The system displays the company ID followed by a company name.



Establishing the connection to an alternate source

About this task

If you decide to close the PLDS website in the customer firewall, an alternate source must be configured to get the software. For example, if you want to test the latest versions of software before using the software for production.

Before you begin

To use an alternate source:

1. Set up the HTTP server for alternate-source and create a directory with a valid name, such as alternate-source in the `http://<ip-addresss>OR<FQDN>/<alternate-source` location.

   Ensure that the URL http://<ip-addresss>OR<FQDN>/<alternate-source> is accessible through the web browser.

2. From Avaya Support Site at ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/SUM/, copy the following xml files to the `alternate-source` directory:
   - `versions.xml`
   - `versions_compatibility.xml`
   - `versions_systemplatform.xml`
   - `versions_cmm.xml`
   - `versions_us.xml`
   - `versions_bsm.xml`
   - `versions_sp.xml`
   - `versions_others.xml`
3. From PLDS, download the software on your computer, and copy to the `http://<ip-addresss/FQDN>/<alternate-source>/` location for the following:
   - For Communication Manager upgrades: Communication Manager, Communication Manager Messaging,Branch Session Manager, Session ManagerUtility Services, TN boards, and Media Gateways or media modules based on your entitlements.
   - For IP Office upgrades: IP Office Manager Admin Lite, VM Pro Client, IP Office, Unified Communications Module (UCM), and IP Office Application Server binary files.

     Note:

     You cannot use My Computer on the File Download Manager page to upload IP Office Manager Admin Lite, VMPro Client, UCM, and IP Office Application Server binary files.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **User Settings**.
3. On the User Settings page, click **Edit**.
4. Clear the **Use Avaya Support Site** check box.
5. In **Alternate Source**, type the server path for an alternate source, that is mentioned in the prerequisites.

   Note:

   The IP address for the alternate source and the software library can be the same. However, ensure that locations for the alternate source URL and software library server path in software library configuration are different. To configure an alternate source and software library on the same server with the artifacts, allocate at least 20 GB disk space each for alternate source and software library.

   The size depends on the number of artifacts that you want to save in the alternate source and the number of artifacts that you want to download in the software library during the upgrade.

6. Click **Commit**.
7. Download the specified xml files on your computer.

   For help to download contact the Avaya support team.
8. Upload the xml files to the HTTP server.
9. Download the required firmware files from PLDS.

   To download the firmware files, contact the Avaya support team.
10. Upload the firmware files to the http server.

    Ensure that you update the firmware files and the xml files in the http server from `ftp.avaya.com`.

User Settings field descriptions

Source configuration

Field	Description
Use Avaya support site	The option to find the information and download the software releases from the Avaya support site. **Note:** • To download the firmware and analyze the software on System Manager, you must gain access to `ftp.avaya.com` and `pldsxml.avaya.com` on the Avaya support site. • Select the **Use Avaya Support Site** check box, to use **Avaya Support Site**. Enter the SSO user name, SSO password, and the Company ID. The SSO authentication is required to get entitlements for **Analyze** and artifacts for download. • If you select the check box, the **Alternate Source** is unavailable.
Alternate Source	The website location from where you can get the latest software. The alternate source is an HTTP URL and an alternate to the Avaya support site. You must set the alternate source. For more information, see *Setting up an alternate source*.

Table continues…

Field	Description
	Note: - The XML files compare the available software version and the latest available version in PLDS. - Clear the **Use Avaya Support Site** check box, to use alternate source repository. You must enter a http URL, for example `http://148.147.216.220/SUMDATA/`. - The IP address of the alternate source can be the same as the IP address of the software library. However, ensure that the URL location and the server path for software library configuration are different.

PLDS configuration

Field	Description
SSO User Name	The user name used as a single sign on for PLDS.
SSO Password	The single sign on password for PLDS.
Confirm SSO Password	The SSO password that you retype in this field.
Company ID	The company ID for PLDS. For more information, see Obtaining a company ID.

Proxy settings

You require proxy settings to use the Avaya PLDS and the Avaya support site. If your network configuration requires a proxy, enter the details in the **Proxy Settings** section.

Field	Description
Use Proxy	The option to use the proxy server for PLDS.
Host	The host name of the proxy.
Port	The port of the proxy.
Password	The password of the proxy server for the Avaya support site.
Confirm Password	The password of the proxy server that you retype for the Avaya support site.

Button	Description
Edit	To display the edit page where you can change the user settings.
Commit	To save the user settings that you enter.

Table continues…

Button	Description
Reset	To reset the page and clear the values that you enter.
Cancel	To cancel your action and return to the previous page.

Software library management

Software library

Using Software Library, you can store the software and firmware files that you download. After you download a firmware file in the Software Library, you can use the downloaded file across multiple devices.

With Software Library, you can also create, modify, view, and delete the firmware files.

For upgrading the firmware files, you must use an external server that functions as a remote software library. To upload the firmware files from System Manager, you must configure an FTP, SCP, or SFTP protocol for the external server.

Note:

A local, non-editable software library with the name SMGR_DEFAULT_LOCAL will be available residing within System Manager post installation. You will require remote software library only for upgrading TN boards, media gateways, media modules and IP Office. For upgrading other elements, you can use a local or remote library.

Related links

Editing a software library on page 1161
Viewing a software library on page 1161
Deleting a file from the software library on page 1165
System requirements for the external server on page 1167
Software library field descriptions on page 1162
Software library files field descriptions on page 1166

Configuring external server as a remote software library for upgrades

Protocol requirements to configure a remote server

To configure an external server as a remote software library, you must configure HTTP, FTP, SCP, or SFTP protocol on the external server. For the external server that you select, you must install separate executable files as listed in the following table:

External server	File for deployment
Apache HTTP server	`httpd-2.0.64-win32-x86-openssl-0.9.8o.msi`
FileZilla FTP server	`FileZilla_Server-0_9_43.exe`
Linux® SCP/SFTP server	`SftpServerInstaller.msi`

Note:

Do not use the SolarWinds SCP/SFTP server to configure the software library for upgrades. System Manager might become nonfunctional. Instead, use the Linux® server.

For every release of the Avaya Aura® application that you want to upgrade, you require a combination of protocols listed in the table. The information applies only for the Windows environment.

Note:

If you use multiple protocols, use the same user name or same directory for all protocols.

Device for upgrade	Required protocols
Avaya Aura® 6.x applications	• HTTP/HTTPS • FTP/SCP
Communication Manager 5.2.1 release	• FTP **Note:** For upgrading the Communication Manager 5.2.1 release, use the FTP protocol. • HTTP/HTTPS

Related links

Installing and configuring an HTTP server as a remote server on page 1154
Installing and configuring an FTP server as a remote server on page 1155
Installing and configuring an SCP or SFTP server as a remote server on page 1158

Installing and configuring an HTTP server as a remote server

Procedure

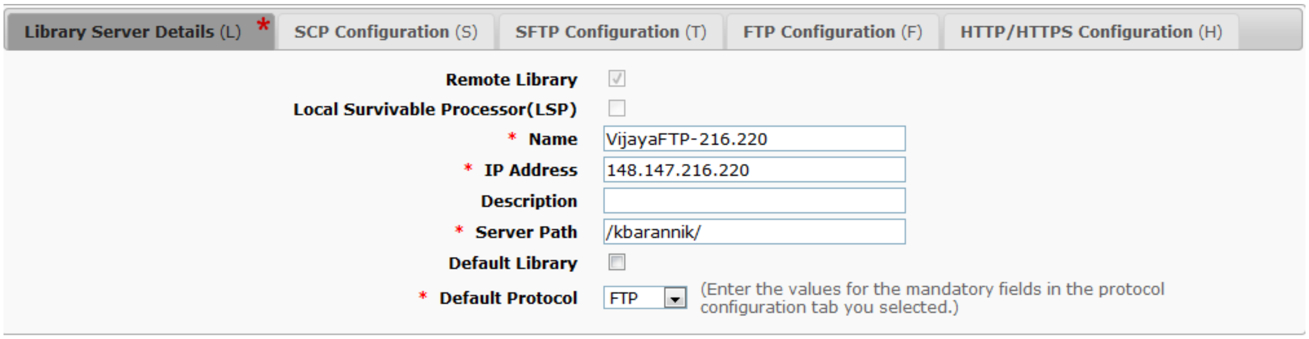
1. Run `httpd-2.0.64-win32-x86-openssl-0.9.8o.msi` as an administrator.

2. Type the domain name, server name and email ID.
3. Complete the installation.
4. Start the application server.
5. In the `C:\Program Files(x86)\Apache Group\Apache2\htdocs\` location, create a folder named `downloads` .

   For example, `C:\Program Files(x86)\Apache Group\Apache2\htdocs\downloads\`
6. Provide the `downloads` folder with full privileges.
7. To verify the privileges, do the following:
   a. Add a file to the `downloads` folder.
   b. Open the file from the browser.

Result

On the System Manager web console, on the Software Library Configuration page, the Library Server Details tab displays the following details:



Remote Library ☑

Local Survivable Processor(LSP) □

* Name: VijayaFTP-216.220

* IP Address: 148.147.216.220

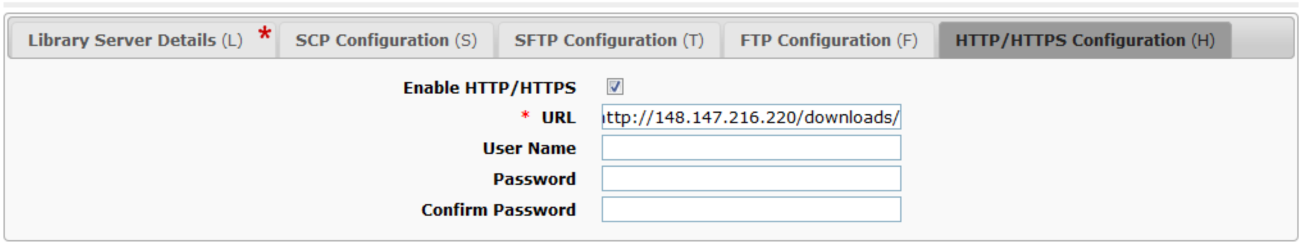
Description:

* Server Path: /kbarannik/

Default Library □

* Default Protocol: FTP (Enter the values for the mandatory fields in the protocol configuration tab you selected.)

The HTTP/HTTPS Configuration tab displays the following http/https configuration details:



Enable HTTP/HTTPS ☑

* URL: ıttp://148.147.216.220/downloads/

User Name:

Password:

Confirm Password:

Related links

[Protocol requirements to configure a remote server](#) on page 1154

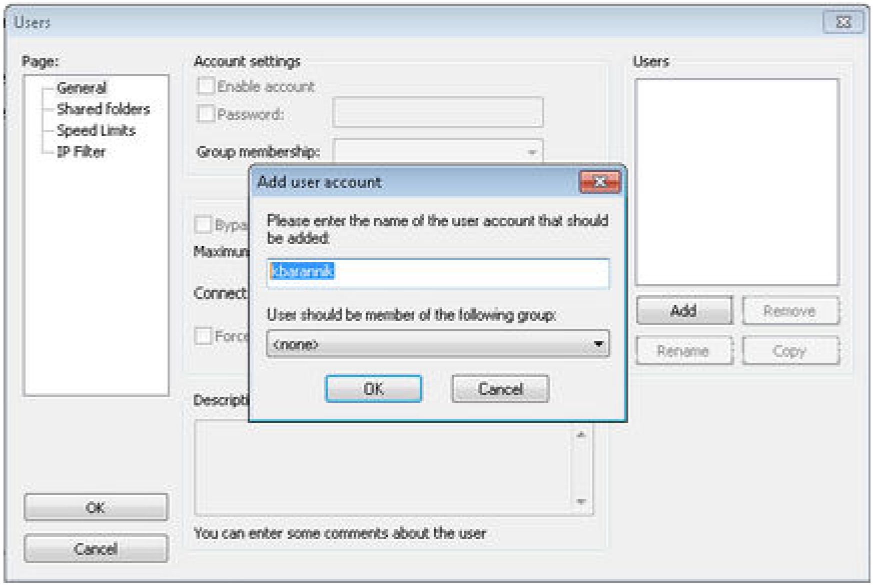
Installing and configuring an FTP server as a remote server

Procedure

1. Run `FileZilla_Server-0_9_43.exe` as an administrator.

   Wait until the installation is complete.

2. Open the FileZilla server interface.
3. On the **Edit** menu, click **Users**.
4. In the Users dialog box, in the left navigation pane, click **General**.
5. In the **Users** section, click **Add**.



Please enter the name of the user account that should be added:

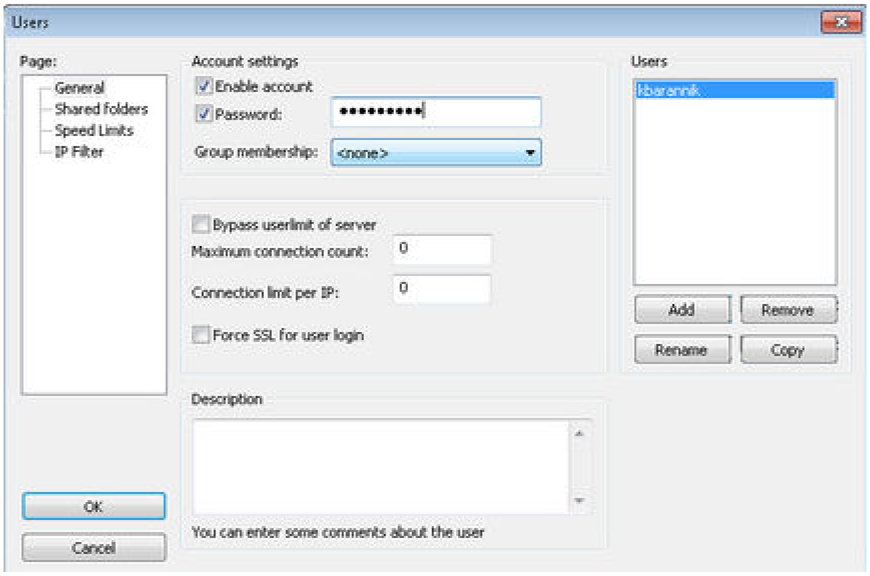
kbarannik

User should be member of the following group:

<none>

You can enter some comments about the user

6. In the Add user account dialog box, type a user name and click **OK**.
7. Select the **Password** check box.
8. Type a password and click **OK**.



☑ Enable account

☑ Password: ••••••••••

Group membership: <none>

☐ Bypass userlimit of server

Maximum connection count: 0

Connection limit per IP: 0

☐ Force SSL for user login

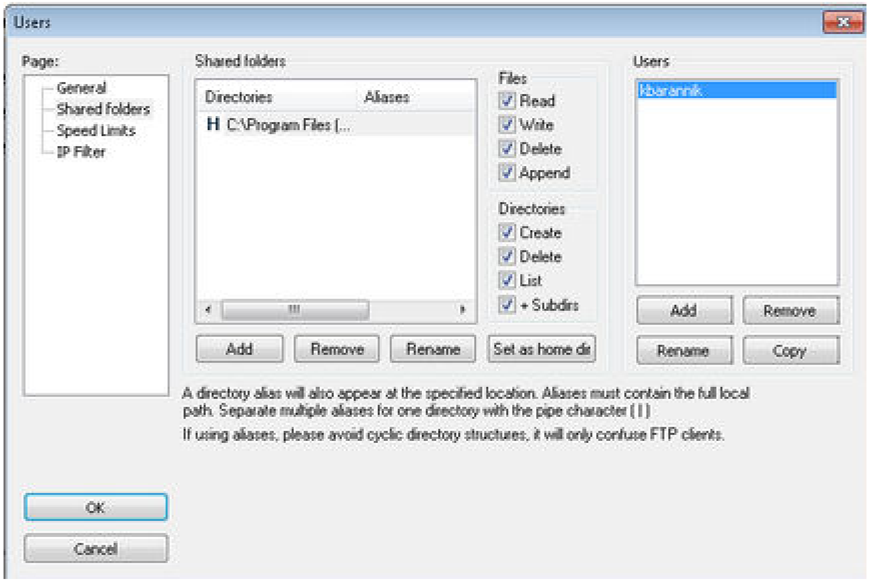
Users: kbarannik

You can enter some comments about the user

The system prompts you to provide a folder.

9. In the left pane, click **Shared folders**.

10. In the **Shared folders** section, click **Add** and provide the folder location till the `downloads` folder.
11. Click **OK**.
12. To provide the privileges, in the **Files** section, select the check boxes, such as **Read**, **Write**, and **Delete**.



Files
☑ Read
☑ Write
☑ Delete
☑ Append

Directories
☑ Create
☑ Delete
☑ List
☑ + Subdirs

Users: kbarannik

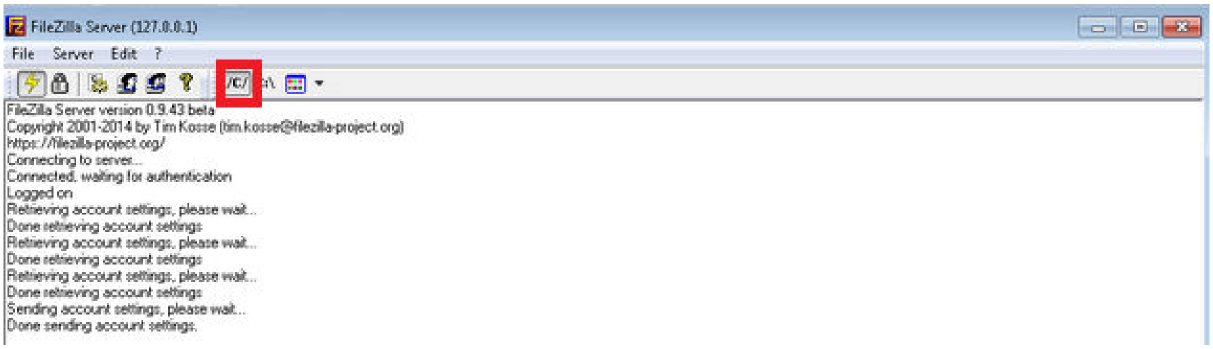
A directory alias will also appear at the specified location. Aliases must contain the full local path. Separate multiple aliases for one directory with the pipe character (|)

If using aliases, please avoid cyclic directory structures, it will only confuse FTP clients.

13. To set the `downloads` folder as the home directory, do the following:
    a. Click **Set as home dir** and navigate to the `C:\Program Files (x86)\Apache Group\Apache2\htdocs\downloads\` folder.
    b. Click **OK**.

Important:

Ensure that you select a logical file name option. By default, the system selects `/C/`.

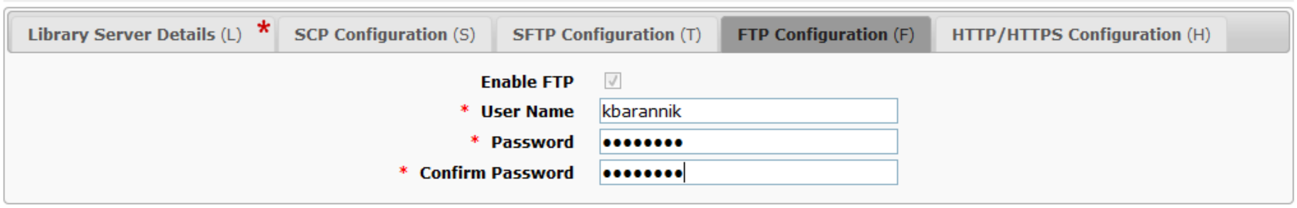


```
FileZilla Server version 0.9.43 beta
Copyright 2001-2014 by Tim Kosse (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server...
Connected, waiting for authentication
Logged on
Retrieving account settings, please wait...
Done retrieving account settings
Retrieving account settings, please wait...
Done retrieving account settings
Retrieving account settings, please wait...
Done retrieving account settings
Sending account settings, please wait...
Done sending account settings.
```

14. To verify the privileges, using the **FTP** client, navigate to the `downloads` folder and open a file.

Result

On the System Manager web console, on the **Software Library Configuration** page, the FTP Configuration tab displays the following FTP configuration details:



Enable FTP ☑

* User Name kbarannik

* Password ••••••••

* Confirm Password ••••••••

Related links

Protocol requirements to configure a remote server on page 1154

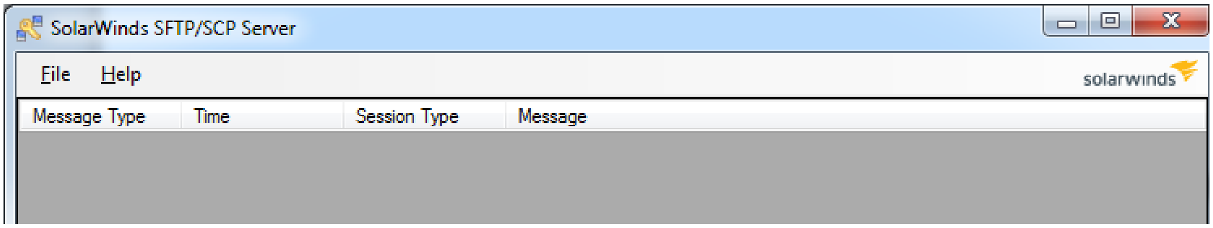
Installing and configuring an SCP or SFTP server as a remote server

Procedure

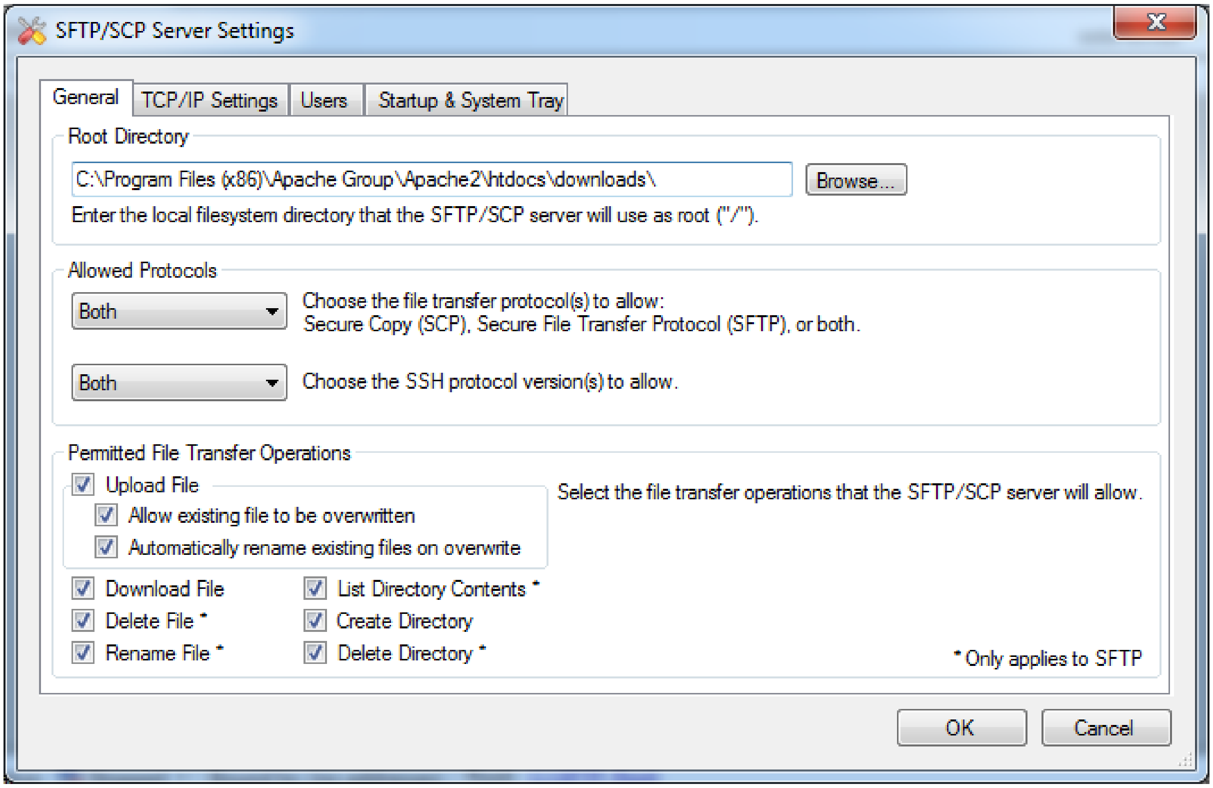
1. Run `SftpServerInstaller.msi` as administrator.

   Wait until the installation is complete.

2. Open the **SolarWinds SFTP & SCP Server** server interface.



3. On the **File** menu, click **Configure**.
4. Navigate to `C:\Program Files (x86)\Apache Group\Apache2\htdocs \downloads\`.
5. Set the required parameters and click **OK**.



Root Directory

C:\Program Files (x86)\Apache Group\Apache2\htdocs\downloads\

Enter the local filesystem directory that the SFTP/SCP server will use as root ("/").

Allowed Protocols

Both — Choose the file transfer protocol(s) to allow: Secure Copy (SCP), Secure File Transfer Protocol (SFTP), or both.

Both — Choose the SSH protocol version(s) to allow.

Permitted File Transfer Operations

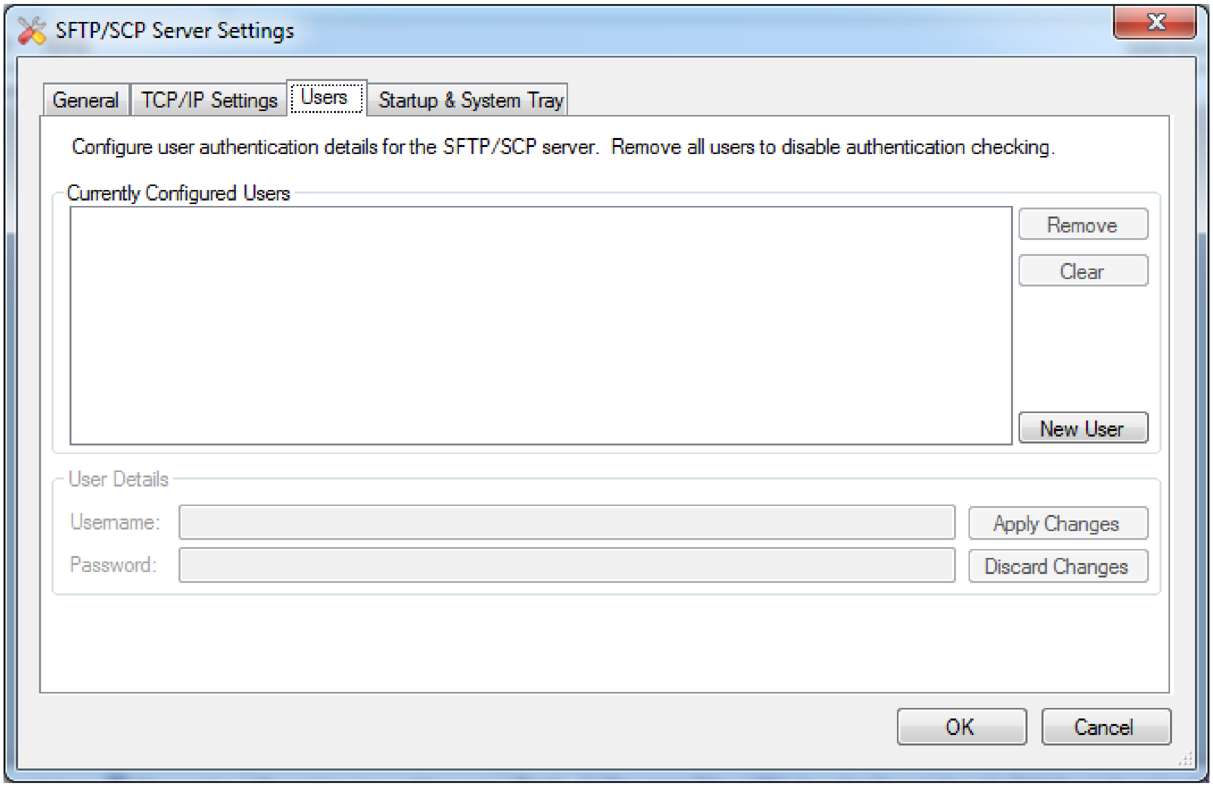
☑ Upload File
- ☑ Allow existing file to be overwritten
- ☑ Automatically rename existing files on overwrite

☑ Download File
☑ Delete File *
☑ Rename File *
☑ List Directory Contents *
☑ Create Directory
☑ Delete Directory *

Select the file transfer operations that the SFTP/SCP server will allow.

* Only applies to SFTP

6. Click the Users tab.



Configure user authentication details for the SFTP/SCP server. Remove all users to disable authentication checking.

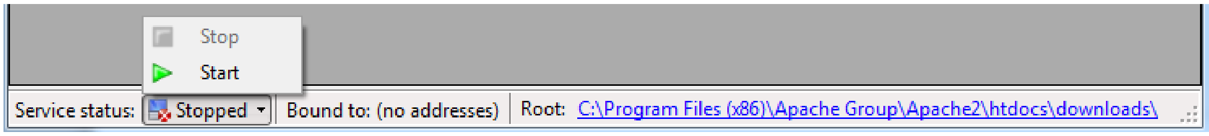
Currently Configured Users

User Details

Username:

Password:

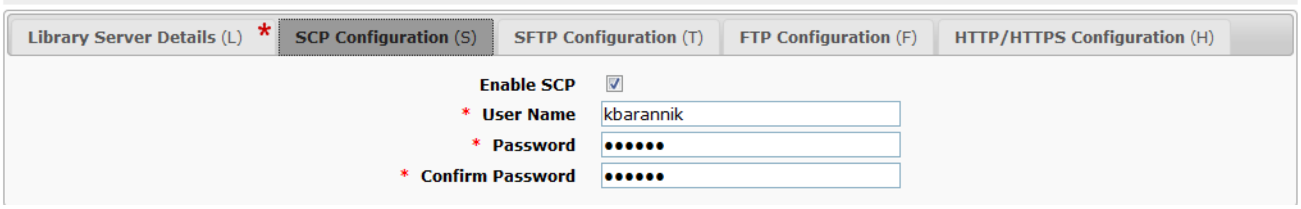
7. Click **New User**.
8. Enter the user name and the password.
9. Click **Apply Changes**.
10. Start the server.


Stop
Start
Service status: Stopped
Bound to: (no addresses)
Root: C:\Program Files (x86)\Apache Group\Apache2\htdocs\downloads\

11. To verify the privileges, using the SCP or the SFTP client, navigate to the `downloads` folder and open a file.

Result

On the Software Library Configuration page of System Manager, the **SCP Configuration** tab displays the following:



Enable SCP ☑

* User Name: kbarannik

* Password: ••••••

* Confirm Password: ••••••

Related links

Protocol requirements to configure a remote server on page 1154

Creating a software library

Before you begin

For upgrades to Release 6.3.8, create the new EPW file for the Communication Manager to be upgraded, and provide all credentials to the EPW file including System Platform details. Store the EPW file on the HTTP or HTTPS server. For more information, contact the Avaya support team.

Note:

You cannot set System Manager as a software library. You must set an external server as a software library.

For more information, see *Protocol requirements for configuring a remote server*.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Software Library Management**.
3. Click **New**.
4. Complete the Add Software Library page.

5. Click **Commit**.
    - To reset the page, click **Clear Configuration**.

Editing a software library

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Software Library Management**.
3. Select the software library whose details you want to edit.
4. Click **Edit**.
5. Edit the required fields in the Edit Software Library page, and click **Commit**.

Viewing a software library

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Software Library Management**.
3. Select the software library whose details you want to view.
4. Click **View**.

    The system displays the details of the software library you selected on the View Software Library page.

Deleting a software library

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Software Library Management**.
3. Select the software library you want to delete.
4. Click **Delete**.
5. On the confirmation page, click **Delete**.

Software library field descriptions

Library Server Details (L)

Name	Description
Remote Library	An option to select a remote library to: • Download files to a remote software library. • Indicate that the local software library is hosted on another server, and not on System Manager. The system selects the **Remote Library** option by default.
Local Survivable Processor(LSP)	An option to select the survivable remote server to add as a software library. The **Local Survivable Processor(LSP)** option applies only for gateways, and supports FTP and SCP only.
Name	The name of the software library.
IP Address	The IP address of the software library. If you select **Local Survivable Processor(LSP)** , the **IP Address** field displays the list of survivable remote servers that are added to the System Manager inventory.
Description	A description of the software library.
Server Path	The software library path where the downloaded files are stored. **Note:** The server path must not contain white spaces. For example, `/user/mydownload` is valid and `/user/my download` is invalid.
Default Library	An option to use a library as the default library when you download the firmware files.
Default Protocol	The default protocol for the software library where you download the firmware files. The options are: • **FTP** • **SCP** • **SFTP** **Note:** When you select the library on the File Download Manager page, the associated protocol is selected by default.

SCP Configuration (S)

Use the SCP configuration to configure the SCP protocol details for the software library.

Name	Description
Enable SCP	An option to enable the SCP configuration. For this release, the **Enable SCP** option is selected by default. You cannot clear the selection.
User Name	The user name for the SCP configuration.
Password	The password for the SCP configuration.
Confirm Password	The password that you retype for the SCP configuration.

SFTP Configuration (T)

Use the SFTP configuration to configure the SFTP protocol details for the software library.

Name	Description
Enable SFTP	An option to enable the SFTP configuration.
User Name	The user name for the SFTP configuration.
Password	The password that you type for the SFTP configuration.
Confirm Password	The password that you retype for the SFTP password.

FTP Configuration (F)

Use the FTP configuration to configure the FTP protocol details for the software library.

Name	Description
Enable FTP	An option to enable the FTP configuration.
User Name	The user name for the FTP configuration.
Password	The password that you type for the FTP configuration.
Confirm Password	The password that you retype for the FTP password.

HTTP/HTTPS Configuration (H)

Use the HTTP/HTTPS configuration to configure the HTTP/HTTPS protocol details for the software library.

Name	Description
Enable HTTP/HTTPS	An option to enable the HTTP/HTTPS configuration.
URL	The software library URL.
User Name	The user name for the HTTP/HTTPS configuration.

Table continues…

Name	Description
Password	The password for the HTTP/HTTPS configuration.
Confirm Password	The password that you retype for the HTTP/HTTPS password.

Button	Description
Commit	Saves the value you enter for the software library.
Clear Configuration	Clears all entries you make, and resets the page.
Cancel	Cancels your action and takes you to the previous page.

Viewing a file in the software library

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Software Library Management**.
3. Click **Manage Files**.
4. On the Software Library Files page select the file that you want to view.
5. Click **View**.

   You can view the details of the file in the View File page.

Uploading a file to the software library

About this task

Use the procedure to upload software files such as OVA, images, and firmware that are required during the deployment, migration, upgrade, and update of Avaya Aura® applications.

Before you begin

- Start an SSH session.
- On Download Management page, click **Refresh Families**.
- When you add or update details in the `versions.xml` file, click **Refresh Families** again to get the updated information.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Software Library Management**.
3. Click **Manage Files**.

4. From System Manager command line interface, copy the required OVA file to the `/swlibrary/staging/sync/` location that you had created in System Manager.

   Note:

   You require admin privileges to the `/swlibrary/staging/sync/` location.

   The system displays the file that you copied in the Sync Files from directory section.

5. Provide the following information:

   - **MD5 Checksum**: The value mentioned in the source or original location of the file.
   - **Software Library**: The local or remote software library.
   - **Product Family**

     Note:

     For SAL, in **Product Family**, **Device Type**, and **Software Type** fields, select **Others**.

   - **Device Type**
   - **Software Type**

   If the file is already in `versions.xml`, the system populates the information.

   If the file does not already exist in `versions.xml`, the system does not display the file details. You cannot use the file for upgrade in Upgrade Management. You can use the file only for new deployment from VM Management.

6. Select the file.

7. Click **Sync**.

   In File Sync Started Message, the system displays a message about the status of the schedule of the job.

8. Click **OK**.

   When the job completes, the system displays the file in the Software Library Files section.

9. To check the status of the job, click **Services** > **Scheduler** > **Pending Jobs**.

   When the job is complete, the system displays the file in the Software Library Files and removes from Sync Files from directory.

Deleting a file from the software library

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Software Library Management**.
3. Click **Manage Files**.
4. On the Software Library Files page, select the file or files you want to delete.

5. Click **Delete**.
6. On the confirmation page, click **Delete**.

Software library files field descriptions

Name	Description
File Name	The software file that you upload from your local directory to the selected library.
Device Type	The device type that you want to upgrade using the software library file. For example, CM_Duplex and CM_Simplex are device types for Communication Manager.
Software Type	The type of software file that includes OVA file, firmware, and images.
Version	The software file version that you want to upload.
Hardware Compatibility	The hardware compatibility for the file you upload. For IP Office, this field can be blank.
File Length	The file length of the software file.
Software Library	The software library where the file is created.

Name	Description
File Name	The software file that you upload from your local directory to the selected library.
MD5 Checksum	The md5 checksum value of the file that you upload as mentioned in the source location of the file.
Software Library	The software library where the file is created.
Product Family	The product family to which the file belongs. In a product family, the number of devices are listed.
Device Type	The device type that you can upgrade using the software library file. For example, B5800 and IP Office are the device types for IP Office.
Software Type	The type of software file which includes firmware and images.

Button	Description
View	Displays the file details page where you can view the details of the software library file.
Delete	Displays the Delete Software Files Confirmation page.
Done	Saves your action and takes you to the previous page.

System requirements for the external server

Component	Requirement	Recommendation
Operating System	Any standalone or virtualized Windows or Linux Distribution.	
Hard Drive	20–GB free space	Ensure that the hard drive has enough free space to store the firmware files.
Memory	2GB	As required by the operating system and the supported protocol services.
Protocols: for the devices to download files from the external server	FTP, SCP, SFTP, or HTTP service	Any supported HTTP server installation. **Note:** Currently, System Manager does not support HTTPS.
Protocols: for downloading the firmware upgrade files to the external server from PLDS site through System Manager	An FTP, SCP, or an SFTP server running on default ports	Use SFTP or SCP for secure file transfer.

Solution Deployment Manager upgrades and updates

Refreshing elements

Before you begin

- Configure the SNMP parameters on the device before you configure the same device in System Manager from Manage Elements.

  Note:

  Use the same SNMP credentials for the device in System Manager.
- On the User Settings page, configure the user settings.
- To upgrade a Communication Manager device, you must configure a profile 18 user on Communication Manager. You cannot use init and craft user profiles while configuring a profile 18 user.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click Upgrade Management.

3. On the Upgrade Management page, do the following:
    a. Select one or more devices.
    b. Click **Pre-upgrade Actions** > **Refresh Element(s)**.
4. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

    The **Last Action Status** column displays ✓and the **Current Version** column displays the current version of the element.

Analyzing software

Before you begin

- On the Roles page, set the Software Management Infrastructure permission.
- Perform the Refresh elements operation.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click Upgrade Management.
3. On the Upgrade Management page, do the following:
    a. Select a device that you want to analyze.
    b. Click **Pre-upgrade Actions** > **Analyze**.
4. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

    The **Last Action Status** column displays a ✓, the **Current Version** column displays the current version of the element, and the **Entitled Upgrade Version** column displays the next version of the element for which the element is entitled to be upgraded.

Downloading the software

About this task

You can download the software releases that you are entitled from Avaya PLDS, or from an alternate source to System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click Upgrade Management.
3. On the Upgrade Management page, select an element from the list.
4. In the left navigation pane, click **Download Management**.

   The system displays the File Download Manager page.
5. To change the display settings, click one of the following:
   - **Tree View**: To view the list of elements in the tree format. The system displays each element with the list of components associated with the element that you selected.
   - **List View**: To view the list of elements in the list format. Every element is displayed individually.
6. In **Select Software/Hardware Types**, select the software or firmware that you want to download.
7. To get the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page, click **Refresh Families**.

   The time to complete the refresh operation depends on the source configuration in **User Settings**.
8. Click **Show Files**.
9. In **Select Files Download Details**, do the following:
   a. In **Source**, click **Avaya PLDS/Alternate Source** or **My Computer** from where you want to download the files.

   b. Select the files that you want to download.

   c. Click **Download**.

   In File Download Status, the system displays the file that you selected for download.

File Download Manager field descriptions

Select Software/Hardware Types

Name	Description
Family Name	The name of the device family.
Hardware/Software	The name of the associated software or hardware.

Select Files Download Details

Name	Description
File name	The file name.
Version	The file version.
Entitled	The file entitlements.
File Size (in bytes)	The file size in bytes.
Hardware/Software	The name of the hardware or the software
Family Name	The name of the device family.
Content Type	The type of the content.
Software Library	The status of the file download.
File Description	A description of the file that you download.

Button	Description
Refresh Families	Gets the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page. **Note:** When you add or update details in the `versions.xml` file, you must click **Refresh Families** to get the updated information.
Show Files	Displays the files associated with the element that you selected.

File Download Status

Name	Description
File Name	The file name.
Job Name	The name of the download job.
Current Step	The current status.
Percentage Completed	The status of completion.

Table continues…

Name	Description
Status	The status of the download activity.
Scheduled By	The user who scheduled the download job.

Button	Description
Delete	Deletes the files that you have selected.

Performing the preupgrade check

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click Upgrade Management.
3. On the Upgrade Management page, do the following:
   a. Select an application to upgrade.
   b. Click **Pre-upgrade Actions** > **Pre-upgrade Check**.
4. On the Pre-upgrade Configuration page:
   a. To migrate to an ESXi host from the old server, in **Target Host**, select the ESXi host.
   b. Fill in the required information.
5. On the Job Schedule page, click one of the following:
   - **Run Immediately**: To perform the job.
   - **Schedule later**: To perform the job at a scheduled time.
6. Click **Schedule**.

   On the Upgrade Management page, the status of the **Last Action Status** and **Pre-upgrade Check Status** columns display a ✓.

Preupgrade Configuration field descriptions

Pre upgrade Configuration Parameters

Name	Description
Element name	The name of the application that you want to upgrade.
Parent name	The parent of the application that you want to upgrade.

Table continues…

Name	Description
IP Address	The IP address of the application that you want to upgrade.
Current Version	The current version of the application that you want to upgrade.
Target Host	The Appliance Virtualization Platform or ESXi host to which you want to upgrade the virtual machine. For upgrades on a different server, add Appliance Virtualization Platform from VM Management.
Data Store	The data store. When you set the **Target Host** as **Same Box**, the system enables the **Data Store** field.
Upgrade Source	The location where OVA or the software patches are available in the local storage or remote server.
Upgrade/Update To	The OVA file or the software patch to which you want to upgrade.
Flexi Footprint	The file based on the storage, CPU, and memory capacity of your system.

Job Schedule

Name	Description
Schedule Job	The option to schedule a job: • **Run immediately**: To run the upgrade job immediately. • **Schedule later**: To run the upgrade job at the specified date and time.
Date	The date on which you want to run the job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date. This field is available when you select the **Schedule later** option for scheduling a job.
Time	The time when you want to run the 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 **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Name	Description
Schedule	Runs the job or schedules to run at the time that you configured in Job Schedule.

Virtual machine management

Virtual machine management

VM Management link from Solution Deployment Manager provides the virtual machine management.

VM Management provides the following capabilities:

- Defines the physical location, Appliance Virtualization Platform or ESXi host, and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Manages lifecycle of the OVA applications that are deployed on the ESXi host. The lifecycle includes start, stop, and reset virtual machines.
- Deploy Avaya Aura® application OVAs on customer-provided Virtualized Environment and Avaya-provided appliance environments.
- Remove the Avaya Aura® application OVAs that are deployed on a virtual machine.
- Configures application and networking parameters required for application deployments.
- Supports flexible footprint definition based on capacity required for the deployment of the Avaya Aura® application OVA.

You can deploy the OVA file on the virtual machine by using the System Manager Solution Deployment Manager and the Solution Deployment Manager client.

Managing the location

Viewing a location

Procedure

1. Perform one of the following:
    - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
    - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.

2. Click the Locations tab.

Adding a location

About this task

You can define the physical location of the host and configure the location specific information. You can update the information later.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. On the Location tab, in the Locations section, click **New**.
3. In the New Location section, perform the following:
   a. In the Required Location Information section, type the location information.
   b. In the Optional Location Information section, type the network parameters for the virtual machine.
4. Click **Save**.

   The system displays the new location in the VM Management Tree section.

Related links

New and Edit location field descriptions on page 1178

Editing the location

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. On the Location tab, in the Locations section, select a location that you want to edit.
3. Click **Edit**.
4. In the Edit Location section, make the required changes.
5. Click **Save**.

Related links

New and Edit location field descriptions on page 1178

Deleting a location

Procedure

1. Perform one of the following:
    - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
    - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. On the Location tab, in the Locations section, select one or more locations that you want to delete.
3. Click **Delete**.
4. On the Delete confirmation dialog box, click **Yes**.

    The system does not delete the virtual machines that are running on the host, and moves the host to **Unknown location host mapping** > **Unknown location**.

VM Management field descriptions

Locations

Name	Description
Location Name	The location name.
City	The city where the host is located.
Country	The country where the host is located.

Button	Description
New	Displays the New Location section where you can provide the details of the location that you want to add.
Edit	Displays the Edit Location section where you can change the details of an existing location.
Delete	Deletes the locations that you select. The system moves the hosts associated with the deleted locations to unknown location.

Hosts

Name	Description
Host Name	The name of the ESXi host.
Host IP	The IP address of the ESXi host.
Host FQDN	FQDN of the ESXi host.

Table continues…

Name	Description
Current Action	The operation that is currently being performed on the ESXi host.
Last Action	The last completed operation on the ESXi host.
Data Store	The data store with the available size.
License Status	The status of the license.
ESXi Version	The VMware ESXi version. The options are 5.5, 5.1, and 5.0.
AVP	The ESXi host type. The options are: • **true**: Appliance Virtualization Platform host • **false**: VMware ESXi host

Button	Description
Add	Displays the New Host section where you can provide the details of the host that you want to add.
Edit	Displays the Host Information section where you can change the details of an existing host.
Remove	Removes the hosts that you select. The system moves the hosts associated with the deleted locations to unknown location.
Change Network Params	Displays the Network Parameters section where you can change the network parameters for the Appliance Virtualization Platform host.
Change Password	Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host.
Update	Displays the Update Host page where you can select the file for updating the Appliance Virtualization Platform host.
Refresh	Refreshes the status of the hosts.

Virtual Machines

Name	Description
VM Name	The name of the virtual machine.
VM IP	The IP address of the virtual machine.
VM FQDN	FQDN of the virtual machine.
VM App Name	The name of the application virtual machine . For example, Session Manager.
VM App Version	The version of the application virtual machine. For example, 7.0.0.0.

Table continues…

Name	Description
VM State	The state of the virtual machine. The states are **Started** and **Stopped**.
Current Action Status	The status of the current operation. The statuses are: • **Deploying** • **Starting** • **Stopping** The **Status Details** link provides the details of the operation in progress.
Last Action	The last action performed on the virtual machine.
Host Name	The hostname of the virtual machine
Trust Status	The trust status of the connection between System Manager and the virtual machine. The status can be **Success** or **Failed**. When the connection between System Manager and the virtual machine establishes, the **Trust Status** changes to **Success**. Only when the trust status is **Success**, you can perform other operations.
Data Store	The data store.

Button	Description
New	Displays the VM Deployment section where you can provide the host and deploy an application.
Edit	Displays the VM Deployment section where you can change the details of a virtual machine.
Delete	Turns off the virtual machines and deletes the selected virtual machines.
Start	Starts the selected virtual machines.
Stop	Stops the selected virtual machines.
Restart	Starts the selected virtual machines that were stopped earlier.
Refresh VM	Updates the status of the virtual machines.
Show Selected	Displays only the selected virtual machines.
More Actions > **Reestablish Connection**	Establishes the connection between System Manager and the virtual machine. When the connection between System Manager and the virtual machine establishes, the **Trust Status** changes to **Success**.

Table continues…

Button	Description
More Actions > **Update VM**	Displays the System Manager VM section where you can install the software patches and service packs for System Manager virtual machine.
More Actions > **Installed Patches**	Refreshes and displays the latest information of the software patch.
More Actions > **Update Static Routing**	Displays the VM Update Static Routing section where you can update the IP address of Utility Services for static routing.

New and Edit location field descriptions

Required Location Information

Name	Description
Name	The location name.
Avaya Sold-To #	The customer contact number. Administrators use the field to check entitlements.
Address	The address where the host is located.
City	The city where the host is located.
State/Province/Region	The state, province, or region where the host is located.
ZIP/PostalCode	The zip code of the host location.
Country	The country where the host is located.
Time Zone	The timezone of the host location.

Optional Location Information

Name	Description
Default Gateway	The IP address of the virtual machine gateway. For example, 172.16.1.1.
DNS Search List	The search list of domain names.
DNS Server 1	The DNS IP address of the primary virtual machine. For example, 172.16.1.2.
DNS Server 2	The DNS IP address of the secondary virtual machine. For example, 172.16.1.4.
NetMask	The subnetwork mask of the virtual machine.
NTP Server	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).

Button	Description
Save	Saves the location information and returns to the Locations section.
Edit	Updates the location information and returns to the Locations section.
Delete	Deletes the location information, and moves the host to the Unknown location section.
Cancel	Cancels the add or edit operation, and returns to the Locations section.

Managing the host

Adding an ESXi host

About this task

Use the procedure to add an Appliance Virtualization Platform or ESXi host. You can associate an ESXi host with an existing location.

Before you begin

A location must be available.

Procedure

1. Perform one of the following:
    - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
    - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Host for Selected Location <location name> section, click **New**.
4. In the New Host section, provide the ESXi host information.
5. Click **Save**.

    In the VM Management Tree section, the system displays the new host in the specified location. The system also discovers applications.
6. To view details of the discovered applications, establish trust between the application and System Manager using the following:
    1. Click **More Actions** > **Re-establish connection**.
    2. Click **Refresh VM**.

Important:

When you change the IP address or FQDN of the Appliance Virtualization Platform host from local inventory, you require Utility Services. To get the Utility Services application name during the IP address or FQDN change, refresh Utility Services to ensure that Utility Services is available.

Related links

New and Edit host field descriptions on page 1183

Editing an ESXi host

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Host for Selected Location <location name> section, select an ESXi host that you want to update.
4. Change the ESXi host information.
5. Click **Save**.

   The system updates the ESXi host information.

Related links

New and Edit host field descriptions on page 1183

Updating the Appliance Virtualization Platform host from Solution Deployment Manager

About this task

You can update only the Appliance Virtualization Platform host using this procedure.

Note:

Install only Avaya-approved service packs or software patches on Appliance Virtualization Platform. Do not install the software patches that are downloaded directly from VMware®. However, in Release 7.0, no upgrades or patches are available for Appliance Virtualization Platform.

Before you begin

1. Install the Solution Deployment Manager client on your computer.
2. Add a location.
3. Add a host.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM), and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the **Host** tab, in the Host for Selected Location <location name> section, select an Appliance Virtualization Platform host, and click **Update**.
4. On the Update Host page, select the file from the local System Manager or software library.
5. Click **Update Host**, and copy the Appliance Virtualization Platform host with the absolute path to the file.

   In the Host for Selected Location <location name> section, the system displays the update status.
6. To view the details, in the **Current Action** column, click **Patching**.

   Host Patching Status window displays the details. The patch installation takes some time. When the patch installation is complete, the **Current Action** column displays the status.

Related links

Update Host field descriptions on page 1185

Changing the network parameters for an ESXi host

About this task

Use this procedure to change the network parameters of Appliance Virtualization Platform after deployment. You can change network parameters only for the Appliance Virtualization Platform host.

Note:

If you are connecting to Appliance Virtualization Platform through the public management interface, you might lose connection during the process. When the IP address changes, you must reconnect by using the new IP address.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM), and then click **VM Management**.
2. In VM Management Tree, select a location.

3. On the Host tab, in the Host for Selected Location <location name> section, select an ESXi host and click **Change Network Params**.
4. In the Network Parameters section, change the IP address, subnetmask, and other parameters as appropriate.
5. To change the gateway IP address, perform the following:
   1. Click **Change Gateway**.

      The **Gateway** field becomes available for providing the IP address.
   2. In **Gateway**, change the IP address.
   3. Click **Save Gateway**.
6. Click **Save**.

   The system updates the Appliance Virtualization Platform host information.

Related links

Change Network Parameters field descriptions on page 1184

Changing the password for an ESXi host

About this task

You can change password only for the Appliance Virtualization Platform host.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. In VM Management Tree, select a location.
3. On the Host tab, in the Host for Selected Location <location name> section, select an ESXi host and click **Change Password**.
4. In the Change Password section, enter the current password and the new password, and reenter the password.

   For more information about password rules, see “Password policy”.
5. Click **Change Password**.

   The system updates the password of the Appliance Virtualization Platform host.

Related links

Change Password field descriptions on page 1185

Deleting an ESXi host

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. On the Host tab, in the Host for Selected Location <location name> section, select one or more hosts that you want to delete.
3. Click **Delete**.
4. On the Delete confirmation page, click **Yes**.

Mapping the ESXi host to an unknown location

About this task

When you delete a location, the system does not delete the virtual machines running on the host, and moves the host to **Unknown location host mapping** > **Unknown location**. You can configure the location of an ESXi host again.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. In the left navigation pane, click the **Unknown location host mapping** link.
3. In the Host Location Mapping section, select an ESXi host and click **Edit**.

   The system displays the Host Information page.
4. Select a location to which you want to map the ESXi host.
5. Click **Submit**.

   The system displays the ESXi host in the selected location.

New and Edit host field descriptions

Name	Description
Location	The location where the host is availabe. The field is read only.

Table continues…

Name	Description
Host Name	The hostname of Appliance Virtualization Platform or the ESXi host. For example, smgrdev.
Host FQDN or IP	The IP address or FQDN of Appliance Virtualization Platform or the ESXi host.
User Name	The user name to log in to Appliance Virtualization Platform or the ESXi host. **Note:** For Appliance Virtualization Platform, provide the root login and password that you configured in the spreadsheet.
Password	The password to log in to Appliance Virtualization Platform or the ESXi host.

Button	Description
Save	Saves the host information and returns to the Host for Selected Location <location name> section.

Change Network Parameters field descriptions

Network Parameters

Name	Description
Name	The name of the Appliance Virtualization Platform host. The field is display-only.
IP	The IP address of the Appliance Virtualization Platform host
Subnet Mask	The subnet mask the Appliance Virtualization Platform host
Host Name	The host name the Appliance Virtualization Platform host
Domain Name	The domain name the Appliance Virtualization Platform host
Preferred DNS Server	The preferred DNS server
Alternate DNS Server	The alternate DNS server
Gateway	The gateway IP address. The field is available only when you click **Change Gateway**.

Button	Description
Change Gateway	Makes the **Gateway** field available, and displays **Save Gateway** and **Cancel Gateway Change** buttons.
Save Gateway	Saves the gateway IP address value that you provide.
Cancel Gateway Change	Cancels the changes made to the gateway.

Button	Description
Save	Saves the changes that you made to network parameters.

Change Password field descriptions

Name	Description
Current Password	The current password
New Password	The new password
Confirm New Password	The new password

Button	Description
Change Password	Saves the new password.

Update Host field descriptions

Name	Description
Patch location	The location where the Appliance Virtualization Platform patch that is available. The options are: • **Select Patch from Local SMGR**: The Appliance Virtualization Platform patch is available on the local System Manager. • **Select Patch from software library**: The Appliance Virtualization Platform patch that is available in the software library.
Select patch file	The absolute path to the Appliance Virtualization Platform patch file.

Button	Description
Update Host	Updates the Appliance Virtualization Platform host.

Downloading the OVA file to System Manager

About this task

You can download the software from Avaya PLDS or from an alternate source to System Manager. Use the procedure to download the OVA files to your computer and upload the file to System Manager.

Before you begin

Set the local software library.

Procedure

1. Download the OVA file on your computer.
2. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
3. In the navigation pane, click **Download Management**.
4. On the Download Management page, perform the following:
    a. In the Select Files Download Details section, in the **Source** field, select **My Computer**.
    b. Click **Download**.

       The system displays the Upload File page.
5. In the **Software Library** field, select a local System Manager software library.
6. Complete the details for the product family, device type, and the software type.
7. Click **Browse** and select the OVA file from the location on the system.

   This system uploads the OVA file from local computer to the designated software library on System Manager.

Managing the virtual machine

Deploying the Utility Services OVA through System Manager Solution Deployment Manager

About this task

Use the procedure to create a virtual machine on the ESXi host, and deploy Utility Services OVA on the Avaya-provided server.

To deploy Utility Services, you can use the System Manager Solution Deployment Manager or the Solution Deployment Manager client, if System Manager is unavailable. Deploy Utility Services first and then deploy all other applications one at a time.

Before you begin

- Ensure you complete the Deployment checklist

For information about the Deployment checklist, see *Deploying Avaya Aura® applications from Avaya Aura® System Manager*.

- Add a location.
- Add Appliance Virtualization Platform or an ESXi host to a location.
- Download the required OVA files to System Manager.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Host <host name> section, click **New**.

   The system displays the VM Deployment section.
4. In the Select Location and Host section, perform the following:
   a. In **Select Location**, select a location.
   b. In **Select Host**, select a host.
   c. In **Host FQDN**, type the virtual machine name.
5. In **Data Store**, select a data store.

   The page displays the capacity details.
6. In the Deploy OVA section, perform the following:
   a. In **Select Software Library**, select the local or remote library where the OVA file is available.

   If you are deploying the OVA by using the Solution Deployment Manager client, you can use the default software library thatis set during the client installation.

   b. In **Select OVAs**, select the OVA file that you want to deploy.
   c. In **Select Flexi Footprint**, select the footprint size that the application supports.
      - **S8300D**: To reduce the memory allocated for Utility Services virtual machine on S8300D that has limited resources. With the minimal footprint on S8300D, the system might not run all required virtual machines.
      - **Default**: For all other server platforms.

   In Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to the application that you deploy.

7. In the Network Parameters section, ensure that the following fields are preconfigured:
   - **Public**
   - **Services**: Only for Utility Services
   - **Out of Band Management**: Only if Out of Band Management is enabled
8. In the Configuration Parameters section, complete the fields.

   For more information about Configuration Parameters, see Network Parameters and Configuration Parameters field descriptions.
9. Click **Deploy**.
10. Click **Accept the license terms**.

    In the Host for Selected Location <location name> section, the system displays the deployment status in the **Current Action Status** column.

    The system displays the virtual machine on the VMs for Selected Host <host name> page.
11. To view details, click the **Status Details** link.

    For information about VM Management field descriptions, see *Deploying Avaya Aura® applications from Avaya Aura® System Manager*.

Related links

VM Deployment field descriptions on page 1192
Network Parameters and Configuration Parameters field descriptions

Deploying an OVA file for an Avaya Aura® application

About this task

Use the procedure to create a virtual machine on the ESXi host, and deploy OVA for an Avaya Aura® application on the virtual machine.

To deploy an Avaya Aura® application, you can use the System Manager Solution Deployment Manager or the Solution Deployment Manager client if System Manager is unavailable.

Deploy Utility Services first, and then deploy all other applications one at a time.

Before you begin

- Add a location.
- Add Appliance Virtualization Platform or an ESXi host to a location.
- Download the required OVA files to System Manager.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.

2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Host <host name> section, click **New**.

   The system displays the VM Deployment section.
4. In the Select Location and Host section, perform the following:
   1. In **Select Location**, select a location.
   2. In **Select Host**, select a host.
   3. In **Host FQDN**, type the virtual machine name.
5. In **Data Store**, select a data store.

   The page displays the capacity details.
6. Click **Next**.
7. In the Deploy OVA section, perform the following:
   1. In **Select Software Library**, select the local or remote library where the OVA file is available.

      If you are deploying the OVA by using the Solution Deployment Manager client, you can use the default software library that is set during the client installation.
   2. In **Select OVAs**, select the OVA file that you want to deploy.
   3. In **Flexi Footprint**, select the footprint size that the application supports.
8. Click **Next**.

   In Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to the application that you deploy.
9. In the Network Parameters section, ensure that the following fields are preconfigured:
   - **Public**
   - **Services**: Only for Utility Services
   - **Out of Band Management**: Only if Out of Band Management is enabled
10. In the Configuration Parameters section, complete the fields.

    For each application that you deploy, fill the appropriate fields.
11. Click **Deploy**.
12. Click **Accept the license terms**.

    In the Host for Selected Location <location name> section, the system displays the deployment status in the **Current Action Status** column.

    The system displays the virtual machine on the VMs for Selected Host <host name> page.
13. To view details, click **Status Details**.

Next steps

- Install the Release 7.0 patch file for the Avaya Aura® application.
- After you deploy the virtual machine, manually update the user password for the system to synchronize data from applications.

  Note:

  If you fail to update the password after the deployment, for applications such as Communication Manager, synchronization operation fails.

Related links

VM Deployment field descriptions on page 1192
Downloading the OVA file to System Manager on page 1186

Editing a virtual machine

Before you begin

- An ESXi host must be available.
- When you change the IP address or FQDN:
- Utility Services must be available and must be discovered.
- If Utility Services is discovered, the system must display Utility Services in the **VM App Name** column. If the application name in **VM App Name** is empty, perform the following to establish trust between the application and System Manager:
  - Click **More Actions** > **Re-establish connection**.
  - Click **Refresh VM**.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. In VM Management Tree, select a host.
3. On the Virtual Machines tab, in the VMs for Selected Host <host name> section, select a host and click **Edit**.

   The system displays the Edit VMs section.
4. **(Optional)** Click **Change flexi footprint value** and perform the following:
   a. In the **Select Flexi Footprint** field, select a value that the application supports.
   b. Click **Change flexi foot print value**.

> **Important:**
>
> Each application must ensure that only the supported flexible footprint is selected.

5. To update the IP address and FQDN, perform the following:

   a. Click **Update IP/FQDN in Local Inventory**.

      The **Update IPFQDN in Local Inventory** option updates the IP address or FQDN only in the local database in System Manager. The actual IP address or FQDN of the host does not change. Use **Update Network Params** in the Host tab to update the IP address or FQDN of the host.

   b. Click **Update VM IP/FQDN**.

   c. Provide the IP address and FQDN of the virtual machine.

      Update IPFQDN in Local Inventory updates the IP address or FQDN only in the local database in System Manager. The actual IP address or FQDN of the host does not change. Use **Update Network Params** in the Host tab to update the IP address or FQDN of the host.

6. Click **Save**.

Starting a virtual machine from Solution Deployment Manager

Procedure

1. Perform one of the following:

   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.

2. From the virtual management tree, select a host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to start.
4. Click **Start**.

   In **VM State**, the system displays `Started`.

Stopping a virtual machine from Solution Deployment Manager

About this task

System Manager is operational and ESXi or vCenter is added to the VM Management page to deploy Avaya Aura® Application OVA on ESXi virtual machines.

Procedure

1. Perform one of the following:

   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.

- For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM), and then click **VM Management**.

2. From the virtual management tree, select a ESXi or vCentre host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to stop.
4. Click **Stop**.

   In **VM State**, the system displays `Stopped`.

Restarting a virtual machine from Solution Deployment Manager

Before you begin

- System Manager is operational, and ESXi or vCenter is added to the VM Management page to deploy Avaya Aura® Application OVA on ESXi virtual machines.
- Virtual machines must be in the running state.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM), and then click **VM Management**.
2. From the virtual management tree, select a host to which you added virtual machines.
3. On the Virtual Machines tab, select one or more virtual machines that you want to restart.
4. Click **Restart**.

   In **VM State**, the system displays `Stopped` and then `Started`.

VM Deployment field descriptions

Select Locations and Hosts

Name	Description
Select Location	The location name. The field is display-only.
Select Host	The hostname of the ESXi host. For example, smgrdev. The field is display-only.
Host FQDN	FQDN of the ESXi host.
VM Name	The name of the virtual machine.
ME Deployment	The option to perform the Midsize Enterprise deployment. The option is available only while deploying Communication Manager simplex OVA.

Select Resource Pool and Data Store

Button	Description
Resource Pool	The login to the resources. The field is display-only.
Datacentre/Cluster	The data centre or the cluster. The field is display-only.
AVP host	The host type. The values are: • **Yes**: An Appliance Virtualization Platform host • **No**: An ESXi host The field is display-only.
Model	The server model. For example, ProLiant DL360 G8 and PowerEdge™ R620.
Data Store	The data store with the available size.

Capacity Details

The system displays the CPU and memory details of the host in this section. The fields are read-only.

Name	Description
Name	The name
Full Capacity	The maximum capacity
Free Capacity	The available capacity
Reserved Capacity	The reserved capacity
Status	The status

Deploy OVA

Name	Description
Select the OVA from Local SMGR	The option to select a `.ova` file of the virtual machine that is available on System Manager.
Select OVA File	The absolute path to the `.ova` file of the virtual machine that you must provide. The field is available only when you click **Select the OVA from Local SMGR**.
Submit	Selects the `.ova` file of the virtual machine that you want to deploy. The field is available only when you click **Select the OVA from Local SMGR**.
Select OVA from software library	The option to get the `.ova` file of the virtual machine from the software library.
Select Software Library	The software library where the `.ova` file is available.

Table continues…

Name	Description
	The field is available only when you click **Select OVA from software library**.
Select OVAs	The `.ova` file that you want to deploy. The field is available only when you click **Select OVA from software library**.
Select Flexi Footprint	The footprint size supported for the selected host. **Important:** • Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory. • Ensure that the application contains the footprint size values that are supported.

Configuration Parameters

The system populates most of the fields depending on the OVA file.

Note:

For configuration parameter fields, for Communication Manager Messaging and Utility Services, see VM Deployment Configuration and Network Parameters field descriptions on page 1196.

Table 9: Configuration Parameters for Communication Manager simplex OVA deployment

Name	Description
CM IPv4 Address	The IP address of the Communication Manager virtual machine.
CM IPv4 Netmask	The network mask of the Communication Manager virtual machine.
CM IPv4 Gateway	The default gateway of the Communication Manager virtual machine.
Out of Band Management IPv4 Address	The IP address of the Communication Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.
Out of Band Management Netmask	The subnetwork mask of the Communication Manager virtual machine for out of band management.
CM Hostname	The hostname of the Communication Manager virtual machine.
NTP Servers	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).
DNS Servers	The DNS IP address of the Communication Manager virtual machine.

Table continues…

Name	Description
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
WebLM Server IPv4 Address	The IP address of WebLM. The field is mandatory.
CM Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time.
CM Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time.
Confirm Password	The password required to be confirmed.

Network Parameters

Name	Description
Public	The port number that is mapped to public port group. You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.
Services	The port number that is mapped to the services port group when Utility Services is deployed in the solution. Utility Services provides routing from the services port to the virtual machines and additional functions, such as alarm conversion.
Duplication Link	The connection for server duplication. The field is available only when you deploy duplex Communication Manager.
Out of Band Management	The port number that is mapped to the out of band management port group.

Button	Description
Deploy	Displays the EULA acceptance screen where you must click **Accept** to start the deployment process.
Cancel	Cancels the deploy operation and returns to the VMs for Selected Host <host name> section.

Related links

VM Deployment Configuration and Network Parameters field descriptions on page 1196

VM Deployment Configuration and Network Parameters field descriptions

Table 10: Configuration Parameters for Communication Manager Messaging deployment

Name	Description
Messaging IPv4 address	The IP address of the Communication Manager Messaging virtual machine.
Messaging IPv4 Netmask	The network mask of the Communication Manager Messaging virtual machine.
Messaging IPv4 Gateway	The default gateway of the Communication Manager Messaging virtual machine. For example, 172.16.1.1.
Out of Band Management IPv4 Address	The IP address of the Communication Manager Messaging virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network.
Out of Band Management IPv4 Netmask	The subnetwork mask of the Communication Manager Messaging virtual machine for out of band management.
Messaging Hostname	The hostname of the Communication Manager Messaging virtual machine.
NTP Servers	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,). The field is optional.
DNS Server(s)	The DNS IP address of the Communication Manager Messaging virtual machine. Separate the IP addresses with commas(,). The field is optional.
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
WebLM Server IPv4 Address	The IP address of WebLM. The field is mandatory.
Messaging Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time.
Messaging Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time.
Confirm Password	The password required to be confirmed.

Configuration and Network Parameters for Utility Services deployment

Name	Description
Configuration Parameters	
Communication Manager IP	IP address of Communication Manager.

Table continues…

Name	Description
	Note: A unique Communication Manager IP address is required for each Utility Services. If you are not associated with a Communication Manager server, specify a static IP that is in your network range.
Hostname	Linux hostname or fully qualified domain name for Utility Services virtual machine.
TImezone setting	The selected timezone setting for the Utility Services virtual machine.
NTP Server IP	IP address of a server running Network Time Protocol that Communication Manager can use for time synchronization.
Out of Band Management Mode	The Out of Band Management mode in which you want to deploy. The options are as follows: • **OOBM_Enabled**: To enable Out of Band Management. • **OOBM_Disabled**: To disable Out of Band Management. **Note:** **OOBM_Disabled** is the default setting. If the mode is set to **OOBM_Disabled**, then you do not need to configure Out of Band Management.
Utility Services Mode	The mode in which you want to deploy Utility Services. The options are: • **Services Port Only**: Deploys Services Port only. Use when the customer already has Utility Services running on another virtual machine and providing the services. With the services port feature, through a laptop connected to the services port of Appliance Virtualization Platform, you can gain access to Avaya virtual machines and the hypervisor that are deployed. • **Utility Servers Only**: Use to disable routing. Set this mode only for Virtualized Environment. If you set this mode for an Avaya appliance, the services port becomes non-operational. • **Full Functionality**: Utility Services and services port enabled. The default mode for Appliance Virtualization Platform. You can set the mode only during the deployment. You cannot change the mode after the virtual machine is deployed. **Note:** For the Solution Deployment Manager client to connect to the services port features of Utility Services, change the IP address to 192.11.13.5 on the computer of the technician

Table continues…

Name	Description
	Utility Services can gain access to the hypervisor and all virtual machines. Utility Services provides application routing between the physical port and virtual applications.
Primary System Manager IP address for application registration	The IP address of System Manager that is required for application registration.
Enrollment Password	The enrollment password.
Confirmation password	The confirmation password.
Network Parameters	
Default Gateway	The IP address of the default gateway. Required field unless you use DHCP.
DNS	The IP address of domain name servers for the Utility Services virtual machine. Separate each IP address by a comma. Required field unless you use DHCP.
Public IP address	The IP address for this interface. Required field unless you use DHCP.
Public Netmask	The netmask for this interface. Required field unless you use DHCP.
Out of Band Management IP Address	The IP address for this interface.
Out of Band Management Netmask	The netmask for this interface.

Update Static Routing field descriptions

Name	Description
VM Name	The virtual machine name
VM IP/FQDN	The VM IP/FQDN
Utility Services IP	The utility services IP

Button	Description
Update	Updates the VM static routing address.

Installed Patches field descriptions

Name	Description
Action to be performed	The operation that you want to perform on the software patch or service pack. The options are: • **All**: Displays all the software patches.

Table continues…

Name	Description
	• **Commit**: Displays the software patches that you can commit. • **Rollback**: Displays the software patches that you can rollback.
VM Name	The name of the System Manager virtual machine on which you want to install the patch.
VM IP	The IP address of System Manager on which you want to install the patch.
Patch Name	The software patch name that you want to install.
Patch Type	The patch type. The options are service pack and software patch.
Patch Version	The software patch version.
Patch State	The software patch state. The states are: • Activated • Deactivated • Removed • Installed
Patch Status	The software patch status.

Button	Description
Get Patch Info	Displays the information about the software patch.
Commit	Commits the selected software patch.
Rollback	Rolls back the selected software patch.

Update VM field descriptions

Name	Description
VM Name	The System Manager virtual machine name
VM IP	The IP address of System Manager
VM FQDN	FQDN of System Manager
Host Name	The host name
Select bin file from Local SMGR	The option to select the software patch or service pack for System Manager. The absolute path is the path on the computer on which the Solution Deployment Manager client is running. The patch is uploaded to System Manager. This option is available only on the Solution Deployment Manager client.

Table continues…

Name	Description
Auto commit the patch	The option to commit the software patch or service pack automatically. If the check box is clear, you must commit the patch from **More Actions** > **Installed Patches**.

Button	Description
Install	Installs the software patch or service pack on System Manager.

Reestablish Connection field descriptions

Name	Description
VM Name	The virtual machine name
VM IP/FQDN	The IP address or FQDN of the virtual machine
User Name	The user name
Password	The password

Button	Description
Reestablish Connection	Establishes connection between System Manager and the virtual machine.

Monitoring a host and virtual machine

Monitoring a host

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. Click the Monitor Hosts tab.
3. In the Monitor Hosts page, do the following:
   a. In **Hosts**, click a host.
   b. Click **Generate Graph**.

   The system displays the graph regarding the CPU/memory usage of the host that you selected.

Monitoring a virtual machine

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. Click the Monitor VMs tab.
3. In the Monitor VMs page, do the following:
   a. In **Hosts**, click a host.
   b. In **Virtual machines**, click a virtual machine on the host that you selected.
4. Click **Generate Graph**.

   The system displays the graph regarding the CPU/memory usage of the virtual machine that you selected.

Managing vCenter

Adding an ESXi host in vCenter

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 5.0, 5.1, and 5.5. When you add vCenter, System Manager discovers the ESXi hosts that this vCenter manages, adds to the repository, and displays in the Managed Hosts section. Also, discovers virtual machines running on the ESXi host and adds to the repository.

System Manager displays vCenter, ESXi host, and virtual machines on the Manage Elements page.

Before you begin

Ensure that you have the required permissions.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **New**.

4. In the New vCenter section, provide the following vCenter information:
   - **vCenter IP/FQDN**
   - **User Name**
   - **Password**
5. Click **Commit**.

   In the Managed Hosts section, the system displays the ESXi hosts that this vCenter manages.

Related links

Editing the ESXi host in vCenter on page 1202
Map vCenter field descriptions on page 1203
New vCentre and Edit vCentre field descriptions on page 1203

Editing the ESXi host in vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select an ESXi host and click **Edit**.
4. In the Edit vCenter section, change the ESXi host information as appropriate.
5. To edit the location of ESXi hosts, in the Managed Hosts section, perform one of the following:
   - Select an ESXi host and click the **Edit** icon.
   - Select more than one ESXi hosts, select the location, and click **Bulk Update** and click **Update**.

   If you do not click **Commit** after you move the host from Managed Hosts to NonManaged Hosts or vice versa, and you refresh the table, the page displays the same host in both the tables. Click **Commit** to get an updated list of managed and nonmanaged hosts.

Deleting the ESXi host in vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. Perform one of the following:
   - For System Manager Solution Deployment Manager, on the web console, click **Services** > **Solution Deployment Manager**, and then click **VM Management**.
   - For the Solution Deployment Manager client, on the desktop, click the SDM icon (SDM CLIENT), and then click **VM Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select one or more ESXi hosts and click **Delete**.

   The system deletes the ESXi host from the inventory.

Map vCenter field descriptions

Name	Description
Name	The name of the ESXi host.
IP	The IP address of the ESXi host.
FQDN	The IFQDN of the ESXi host.
License	The license status of the ESXi host.
Status	The license status of the ESXi host.

Button	Description
New	Displays the New vCenter page, where you can add a new ESXi host.
Edit	Displays the Edit vCenter page, where you can update the details and location of ESXi hosts.
Delete	Deletes the ESXi host.
Refresh	Updates the list of ESXi hosts in the Map vCenter section.

New vCentre and Edit vCentre field descriptions

Name	Description
vCenter IP/FQDN	The IP address or FQDN of vCenter.
User Name	The user name to log in to vCenter.
Password	The password that you use to log in to vCenter.

Button	Description
Commit	Saves the changes that you made to the Map vCenter page.
Refresh	Refreshes the vCenter details.

Managed Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
Host Name	The IP address of the ESXi host.
Location	The physical location of the ESXi host.
Edit	The option to edit the location and host.
Bulk Update	Provides an option to change the location of more than one ESXi hosts. **Note:** You must select a location before you click **Bulk Update**.
Update	Saves the changes that you make to the location or hostname of the ESXi host.
Commit	Commits the changes that you make to the ESXi host with location that is managed by vCenter.

Unmanaged Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
ESXi Version	The version of the ESXi host. The options are: 5.0, 5.1, and 5.5.

Upgrading Avaya Aura® applications

Upgrade Management overview

Solution Deployment Manager > **Upgrade Management**, a centralized upgrade solution of System Manager, provides an automatic upgrade of Communication Manager and associated devices, such as Gateways, TN boards, and media modules from a single view. You can upgrade Communication Manager Release 5.2.1 and 6.x to Release 7.0, and Session Manager and Branch Session Manager to Release 7.0. The centralized upgrade process minimizes repetitive tasks and reduces the error rate.

Important:

System Manager Release 7.0 also supports using System Manager Release 6.3.8 to upgrade Communication Manager, gateways, media modules, and TN boards to Release 6.3.8. However, the Release 6.3.8 user interface is available only when you select **Release 6.3.8** as target version on the **Solution Deployment Manager** > **Upgrade Release Setting** page.

Using System Manager Solution Deployment Manager, perform the following in the given sequence

1. Refresh elements: To get the current state or data such as current version of the Avaya Aura® application. For example, for Communication Manager, gateways, media modules, and TN boards.
2. Analyze software: To analyze whether the elements and components are on the latest release and to identify whether a new software is available for the inventory that you collected.
3. Download files: To download files that are required for upgrading elements and components.

   You can download a new release from Avaya PLDS to the software file library and use the release to upgrade the device software.
4. Preupgrade check: To ensure that conditions for successful upgrade are met. For example, if the new release supports the hardware, the RAID battery is sufficient, the bandwidth is sufficient, and if the files are downloaded.
5. Install software patches and service packs.

Upgrades of all other Avaya Aura® applications that Solution Deployment Manager supports can automatically deploy OVAs, but involve some manual operations for creating backup and restoring the backup data for all other applications manual process. The upgrade of Communication Manager, Session Manager, Branch Session Manager and Utility Services to Release 7.0 is automated. The upgrade process includes creating backup, deploying OVA, upgrading, and restoring the backup.

Upgrade job capacity

System Manager Solution Deployment Manager supports simultaneous upgrades or updates of Avaya Aura® applications. Solution Deployment Manager supports the following upgrade capacity:

- 5 upgrade or update job groups: Multiple elements combined together in an upgrade or update job is considered as a group.
- 20 elements in a job group: Maximum elements that can be combined in an upgrade or update group is 20. You can combine any element type for upgrade in a group.

Elements in paused state are also included in the capacity. If 5 upgrade job groups are running or in a paused state, you cannot upgrade the sixth group.

Avaya Aura® applications upgrade

With System Manager Solution Deployment Manager, you can upgrade the following Avaya Aura® applications to Release 7.0:

- Communication Manager
- Session Manager
- Branch Session Manager
- Utility Services

Note:

You must upgrade System Manager to Release 7.0 by using the Solution Deployment Manager client before you upgrade the Avaya Aura® applications to Release 7.0.

Upgrade target release selection

For backward compatibility, System Manager supports upgrading Communication Manager to Release 6.3.6 or later. By default, the target version is set to Release 7.0. Based on entitlements, to upgrade Communication Manager and the associated applications to Release 6.3.6, you must select Release 6.3.8 as the upgrade target release.

Related links

Selecting the target release for upgrade on page 1206

Selecting the target release for upgrade

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade version** field, select one of the following:
    - **SMGR 7.0**: To upgrade Avaya applications to Release 7.0 from the Upgrade Management page.
    - **SMGR 6.3.8**: To upgrade Communication Manager and the associated applications to Release 6.3.8 from the **Upgrade Management** > **Software Inventory** page.

    Important:

    By default, the target version is set to Release 7.0.
4. Click **Commit**.
5. Click **OK**.
6. To perform the upgrade, click **Upgrade Management**.

Related links

Upgrade target release selection on page 1206

Upgrading Avaya Aura® applications

Checklist for upgrading Avaya Aura® applications to Release 7.0

No.	Task	References	✔
1	Install Solution Deployment Manager client on your computer.	Installing the Solution Deployment Manager client on your computer on page 1142	
2	To upgrade on an Avaya-provided server, install Appliance Virtualization Platform.		
3	If System Manager is: • Unavailable: On Appliance Virtualization Platform, deploy the System Manager Release 7.0 OVA file by using the Solution Deployment Manager client • Available: Upgrade System Manager to Release 7.0		
4	Discover the applications and associated devices that you want to upgrade by enabling SNMP or manually add the elements from **Manage Elements** > **Discovery**.	"Discovering elements" in *Administering Avaya Aura® System Manager*	
5	Configure user settings.	"User settings" in *Administering Avaya Aura® System Manager*	
6	Use a local System Manager library or create a remote software library. **Note:** For local, the software local library for TN Boards and media gateway upgrades is not supported.	"User settings" in *Administering Avaya Aura® System Manager*	
7	Refresh the elements in the inventory.	"Refreshing elements" in *Administering Avaya Aura® System Manager*	
8	Analyze the software.	"Analyzing software" in *Administering Avaya Aura® System Manager*	
9	Download the required firmware for the Avaya Aura® application upgrade.	"Downloading the software" in *Administering Avaya Aura® System Manager*	
10	Analyze the software.	"Solution deployment and upgrades" in *Administering Avaya Aura® System Manager*	

Table continues…

No.	Task	References	✔
11	Perform the preupgrade check.	“Performing the preupgrade check” in *Administering Avaya Aura® System Manager*	
12	Perform the upgrade.	Upgrading Avaya Aura applications from 6.0, 6.1, 6.2, or 6.3 to Release 7.0 on page 1208	
13	Verify that the upgrade is successful.	-	

Upgrading Avaya Aura® applications from 6.0, 6.1, 6.2, or 6.3 to Release 7.0

About this task

Use the procedure to upgrade Communication Manager, Session Manager, Branch Session Manager, Utility Services to Release 7.0. The procedure covers upgrades on the same server and on a different server.

Before you begin

- From the Roles page, ensure that you set permissions that are required to perform all upgrade-related operations.
- Configure user settings.
- Complete all required operations up to the preupgrade check.
- If you are migrating from old server to ESXi host, add the new host in to VM Management.
- If migrating the Avaya Aura® application to a different server, add the Appliance Virtualization Platform host from the VM Management page.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click Upgrade Management.
3. To view and select the dependent elements:
    a. Click the element.
    b. On the Displaying Communication Manager Hierarchy page, select an element in the hierarchy.

       When you select an element, the system selects the parent of the element and all child elements of the element in the hierarchy. The page displays TN boards and media modules details in a table.
    c. Click **Done**.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, select the **Override preupgrade check** check box.

   When you select the check box, the upgrade process continues even when the recommended checks fail in preupgrade check.

6. To provide the upgrade configuration details, click **Edit**.
7. On the Edit Upgrade Configuration page, complete the details and click **Save**.
8. Ensure that the **Configuration Status** field displays ✅.

   If the field displays ❌, review the information on the Edit Upgrade Configuration page.
9. Click **Save**.
10. On the Upgrade Configuration page, click **Upgrade**.
11. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
12. Click **Schedule**.
13. Click **Upgrade**.
14. On the Upgrade Management page, click 🔄.

    Last Action column displays **Upgrade**, and **Last Action Status** column displays ✅.
15. To view the upgrade status, perform the following:
    1. In the navigation pane, click **Upgrade Job Status**.
    2. In the **Job Type** field, click **Upgrade**.
    3. Click the upgrade job that you want to view.
16. Verify that the upgrade of the application is successful.

    For upgrades on the same server, system goes to the pause state.
17. For upgrades on the same server, perform the following:
    1. Install the Appliance Virtualization Platform host.
    2. From the VM Management page, add the Appliance Virtualization Platform host.
    3. To continue with the upgrade, click **Upgrade Actions** > **Resume**.
    4. On the Resume Configuration page, select the target Appliance Virtualization Platform host and the datastore.
    5. Continue with the upgrade process.

Related links

Preupgrade Configuration field descriptions on page 1171
Upgrade Configuration field descriptions on page 1215
Edit Upgrade Configuration field descriptions on page 1215

Installing software patches

About this task

Use the procedure to install the software patches and service packs that are entitled for an Avaya Aura® application, and commit the software patches that you installed.

Before you begin

- Perform the preupgrade check.
- If you upgrade an application that was not deployed from Solution Deployment Manager, perform the following:
  1. Select the virtual machine.
  2. To establish trust, click **More Actions** > **Re-establish Connection**.
  3. Click **Refresh VM**.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click Upgrade Management.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In the **Upgrade Source** field, select the software library where you have downloaded the patch.

   In the Select patches for update section, the page displays the available patches.
8. Select the patch that you want to install.
9. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.
10. In the Upgrade Configuration Details section, select the software patch that you want to install.
11. Click **Save**.
12. Ensure that the **Configuration Status** field displays ✓.
13. Click **Upgrade**.
14. On the Job Schedule page, click one of the following:
    - **Run Immediately**: To perform the job.
    - **Schedule later**: To perform the job at a scheduled time.
15. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display ✓.

16. To view the update status, click ✓.

    The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.

    When the update is complete, the **Update status** and **Last Action Status** fields displays ✓.
17. Click **Upgrade Actions** > **Installed Patches**.
18. On the Installed Patches page, in the Patch Operation section, click **Commit**.

    The page displays all software patches that you can commit.

    You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.
19. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

    You can schedule to commit the patch at a latter time by using the **Schedule later** option.
20. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.
21. Ensure that the **Update status** and **Last Action Status** fields display ✓.

Related links

Preupgrade Configuration field descriptions on page 1171
Upgrade Configuration field descriptions on page 1215
Edit Upgrade Configuration field descriptions on page 1215
Installed Patches field descriptions on page 1211

Installed Patches field descriptions

Name	Description
Commit	The option to select the patches that you can commit.
Uninstall	The option to select the patches that you can uninstall.
Rollback	The option to select the patches that you can rollback.
Show All	The option to display all the available options.

Name	Description
Name	The name of the software patch.
Element Name	The element on which the software patch is installed.
Patch Version	The version of the software patch.

Table continues…

Name	Description
Patch Type	The type of the software patch. The options are: • service pack or software patch • Kernel
Patch State	The state of the software patch. The options are: • Installed • Activated • Deactivated • Removed • Uninstall • Pending

Name	Description
Schedule Job	The option to schedule a job: • **Run immediately**: To run the upgrade job immediately. • **Schedule later**: To run the upgrade job at the specified date and time.
Date	The date on which you want to run the job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date. This field is available when you select the **Schedule later** option for scheduling a job.
Time	The time when you want to run the 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 **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Name	Description
Schedule	Runs the job or schedules to run at the time that you configured in Job Schedule.

Upgrade Management field descriptions

You can apply filters and sort each column in the devices list.

Name	Description
Name	The name of the device that you want to upgrade.
Parent	The name of the parent of the device. For example, CommunicationManager_123.
Type	The device type. For example, TN board.
Sub-Type	The sub type of the device. For example, TN2302AP.
IP Address	The IP address of the device.
Release Status	The release status of the device. The upgrade status can be: For upgrade: • ✓: Upgraded successfully • ⚠: Ready for upgrade • 🕒: Pending execution • ?: Status unknown • ⏸: Upgrade process paused • ⊗: Nonupgradable • ✖: Operation failed
Update Status	The update status of the device. The upgrade status can be: • ✓: Upgraded successfully • ⚠: Ready for upgrade • 🕒: Pending execution • ?: Status unknown • ⏸: Upgrade process paused • ⊗: Nonupgradable • ✖: Operation failed
Last Action	The last action performed on the device.
Last Action Status	The status of the last action that was performed on the device.

Table continues…

Name	Description
Pre-upgrade Check Status	The status of preupgrade check of the device. The options are: • ✓: Mandatory checks and recommended checks passed • ⚠: Mandatory checks are successful, but recommended checks failed. • ✗: Mandatory checks and recommended checks failed You can click the icon to view the details on the Element Check Status dialog box.
Current Version	The software release status of the device.
Entitled Upgrade Version	The latest software release to which the device is entitled.
Entitled Update Version	The latest software patch or service pack to which the device is entitled.
Location	The location of the device.

Button	Description
Pre-upgrade Actions > **Refresh Elements**	Refreshes the fields that includes the status and version of the device.
Pre-upgrade Actions > **Analyze**	Finds if the latest entitled product release is available for a device and displays the report.
Pre-upgrade Actions > **Pre-upgrade Check**	Displays the Pre-upgrade Configuration page where you can configure to run the job or schedule the job to run later.
Upgrade Actions > **Upgrade**	Displays the Upgrade Configuration page where you can configure the upgrade.
Upgrade Actions > **Install Patches**	Displays the software patches for the element and the operations that you can perform. The operations are: install, activate, uninstall, and rollback.
Upgrade Actions > **Commit**	Commits the changes that you made.
Upgrade Actions > **Rollback**	Resets the system to the previous state.
Upgrade Actions > **Resume**	Resumes the upgrade process after you complete the required configuration. For example, adding the Appliance Virtualization Platformhost.
Download	Displays the File Download Manager page with the list of downloaded software required for upgrade or update.
Show Selected Elements	Displays only the elements that you selected for preupgrade or update.

Upgrade Configuration field descriptions

Name	Description
Element Name	The name of the device.
Parent Name	The parent of the device. For example, CommunicationManager_123.
Type	The device type.
IP Address	The IP Address of the device.
Release Version	The release status of the device.
Override preupgrade check	The option to override preupgrade check recommendations. When you select this option, the system ignores any recommendations during preupgrade check, and continues with the upgrade operation. The system enables this option only when the system displays the upgrade status as **Partial_Failure**.
Edit	Displays the Edit Upgrade Configuration page where you can provide the upgrade configuration details.
Configuration Status	An icon that defines the configuration status. • ✖: Configuration incomplete. • ✓: Configuration complete.

Button	Description
Upgrade	Commits the upgrade operation.

Edit Upgrade Configuration field descriptions

General Configuration Details

Name	Description
System	The system name.
IP Address	The IP address of the device.
Operation	The operation that you want to perform on the device. The options are: • Upgrade • Update
ESXI Host	The ESXi host on which you want to run the device. The options are: • Same host • List of hosts that you added from VM Management

Table continues…

Name	Description
VM Name	The name of the virtual machine.
Upgrade Source	The source where the installation files are available. The options are: • Local machine • Software library
Upgrade To	The Release 7.0 OVA file to which you want to upgrade. When you select the local System Manager library, the system displays the fields and populates most of the data in the Upgrade Configuration Details section.

Upgrade Configuration Details

The page displays the following fields when you upgrade Communication Manager and the associated devices. The page displays all values from the existing system. If the system does not populate the values, manually add the values in the mandatory fields.

Name	Description
Auto Commit	The option to automatically commit the upgrade.
Existing Administrative User	The Communication Manager user name with appropriate privileges.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway. For Communication Manager Messaging, the button is unavailable and you must fill in all details. For Communication Manager Messaging you must provide a new IP address.
CM IPv4 Address	The IP address of the Communication Managervirtual machine.
CM IPv4 Netmask	The network mask of the Communication Managervirtual machine.
CM IPv4 Gateway	The default gateway of the Communication Managervirtual machine.
Out of Band Management IPv4 Address	The IP address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.

Table continues…

Name	Description
Out of Band Management Netmask	The subnetwork mask of the virtual machine for out of band management.
CM Hostname	The hostname of the Communication Manager virtual machine.
NTP Servers	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).
DNS Servers	The DNS IP address of the virtual machine.
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
WebLM Server IPv4 Address	The IP address of WebLM. The field is mandatory.
CM Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time.
CM Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time.
Flexi Footprint	The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.
Public	The port number that you must assign to public port group.
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.
Private	Tan exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.
Services	The port number that is assigned to the services port. The system displays this field when Utility Services is available.
Duplication link	The port number assigned to a dedicated HA sync links. For example, Communication Manager duplex crossover that is assigned to an exclusive physical NIC. The installer selects free server NIC during the deployment process.

Table continues…

Name	Description
	The field is available only for the Communication Manager duplex configuration and when you select a different host.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

The page displays the following fields when you upgrade Session Manager.

Name	Description
Existing Administrative User	The user name of the administrator.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields.
IP Address	The IP address of the virtual machine.
Short Hostname	The hostname of the virtual machine. The hostname of the server and is often aligned with the DNS name of the server.
Network Domain	The domain name of the virtual machine.
Netmask	The network mask of the virtual machine.
Default Gateway	The default gateway of the virtual machine.
DNS Servers	The DNS IP address of the virtual machine.
Timezone	The timezone of the virtual machine.
Login Name	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
Enter Customer Account Password	Password to log on to the system.
Primary System Manager IP	The IP address of System Manager.
Enrollment Password	The password that is required to establish trust between System Manager and Session Manager.
Flexi Footprint	The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.
Public	The port number that you must assign to public port group.
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.

Table continues…

Name	Description
Private	The port number that is assigned to an exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

Button	Description
End User License Agreement	The end user license agreement. You must select the check box to accept the license agreement.

Button	Description
Save	Saves the changes that you made to the Edit Upgrade Configuration page.

System Manager upgrade management

Upgrading System Manager on a different server by using Solution Deployment Manager client

About this task

You can upgrade System Manager on the same server or a different server.

The procedure describes the steps to upgrade System Platform-based System Manager on a different server.

Before you begin

- Add a location.
- Install the Appliance Virtualization Platform host.
- Add the Appliance Virtualization Platform host from the VM Management page.
- Install the Solution Deployment Manager client.
- Obtain the following System Manager software:
  - OVA file, `SMGR-7.0.0.0.16266-e55-43-29-II.ova`
  - Data migration utility, `Data_Migration_Utility_7.0.0.0_r91.bin`

- Create the System Manager backup and copy the file to the same computer where Solution Deployment Manager client is installed.

Procedure

1. To start the Solution Deployment Manager client, perform one of the following:
    - On the desktop, click the SDM icon (SDM CLIENT).
    - Click **Start** > **All Programs** > **Avaya**, and click **SDM Client** > **Avaya SDM Client**.
2. Click **VM Management**.
3. In the lower pane, click **Upgrade Management**.
4. Click **Add Elements**, add the details of System Manager such as IP address, login credentials of System Manager and login credentials of the console domain.
5. Click **Save**.
6. On the Upgrade Elements page, select the System Manager that you added.
7. Click **Upgrade**.

    The system displays the Upgrade Management page.
8. Clear the **Install on Same ESXi** check box.
9. In **Host FQDN**, select the host that you added.

    The system populates details such as resources and memory.
10. Select the datastore on the host.
11. In the **Deploy OVA** section, perform the following:

    a. In **Select OVA** file, type the absolute path to the System Manager OVA file, and click **Submit File**.

    The system populates the network parameters and configuration parameters from the System Platform-based virtual machine.

    b. Select the flexi footprint.

    c. Provide the absolute path to the data migration utility.

    d. Provide absolute path to the System Manager backup file.
12. In the Configuration Parameters section, provide FQDN, Timezone, and SNMP passwords.
13. In the Network Parameters section, provide the Public and Out of Band Management details.
14. Click **Upgrade** and accept the license terms.

    The existing virtual machine shuts down, deploys OVA, and restores the data on the new virtual machine.
15. To view the status, in the Upgrade Status column, click **Status Details**.

    The complete process takes about 3 hours depending on the data on System Manager.

Related links

Installing the Solution Deployment Manager client on your computer on page 1142
Upgrade Management field descriptions on page 1224
Add Element field descriptions on page 1224
Install on Same ESXi field descriptions on page 1230

Upgrading System Manager on the same server by using Solution Deployment Manager client

About this task

You can upgrade System Manager on the same server or a different server.

The procedure describes the steps to upgrade System Platform-based System Manager on the same server.

Before you begin

- Add a location.
- Install the Solution Deployment Manager client.
- Obtain the following System Manager software:
  - OVA file, `SMGR-7.0.0.0.16266-e55-43-29-II.ova`
  - Data migration utility, `Data_Migration_Utility_7.0.0.0_r91.bin`
- Create the System Manager backup and copy the file to the same computer where Solution Deployment Manager client is installed.

Procedure

1. To start the Solution Deployment Manager client, perform one of the following:
   - On the desktop, click the SDM icon (SDM CLIENT).
   - Click **Start** > **All Programs** > **Avaya**, and click **SDM Client** > **Avaya SDM Client**.
2. Click **VM Management**.
3. In the lower pane, click **Upgrade Management**.
4. Click **Add Elements**, add the details of System Manager such as IP address, login credentials of System Manager and login credentials of the console domain.
5. Click **Save**.
6. On the Upgrade Elements page, select the System Manager that you added.
7. Click **Upgrade**.

   The system displays the Upgrade Management page.
8. Select the **Install on Same ESXi** check box.

9. Click **Continue**.

   The system shuts down the virtual machine and reaches a paused state.

   You must add the Appliance Virtualization Platform host from VM Management.

10. Install the Appliance Virtualization Platform host on the server on which System Platform was running.
11. To resume the upgrade operation, click **Upgrade Elements** > **Resume from Upgrade elements** list.
12. In **Host FQDN**, select the host that you added.

    The system populates details such as resources and memory.

13. Select the datastore on the host.
14. In the **Deploy OVA** section, perform the following:
    1. In **Select OVA** file, type the absolute path to the System Manager OVA file, and click **Submit File**.

       The system populates the network parameters and configuration parameters from the System Platform-based virtual machine.

    2. Select the flexi footprint.
    3. Provide the absolute path to the data migration utility.
    4. Provide absolute path to the System Manager backup file.
15. In the Configuration Parameters section, provide FQDN, Timezone, and SNMP passwords.
16. In the Network Parameters section, provide the Public and Out of Band Management details.
17. Click **Upgrade** and accept the license terms.

    The existing virtual machine shuts down, deploys OVA, and restores the data on the new virtual machine.

18. To view the status, in the Upgrade Status column, click **Status Details**.

    The complete process takes about 3 hours depending on the data on System Manager.

Related links

Installing the Solution Deployment Manager client on your computer on page 1142
Upgrade Management field descriptions on page 1224
Add Element field descriptions on page 1224
Install on Same ESXi field descriptions on page 1230

Installing service packs and software patches on System Manager by using the Solution Deployment Manager client

About this task

Use this procedure for updating System Manager that was deployed using the same Solution Deployment Manager client.

Before you begin

Install the Solution Deployment Manager client.

Procedure

1. To start the Solution Deployment Manager client, perform one of the following:
    - On the desktop, click the SDM icon (SDM CLIENT).
    - Click **Start** > **All Programs** > **Avaya**, and click **SDM Client** > **Avaya SDM Client**.
2. Click **VM Management**.
3. In VM Management Tree, select a location.
4. On the Virtual Machines tab, in the VMs for Selected Host <host name> section, select System Manager on which you want to install the patch.
5. **(Optional)** If updating from a different client, perform the following:
    a. Click **More Actions** > **Re-establish connection**.
    b. Click on **Refresh VM**.
    c. To view the status, in the **Current Action** column, click **Status Details**.
    d. Proceed with the next step.
6. Click **More Actions** > **Update VM**.

    The system displays the System Manager Update dialog box.
7. In **Select bin file from Local SMGR**, provide the absolute path to the software patch or service pack.

    Note:

    The absolute path is the path on the computer on which the Solution Deployment Manager client is running. The patch is uploaded to System Manager.
8. Click the **Auto commit the patch** check box.

    To install the patches manually, click **More Actions** > **Installed Patches**.
9. Click **Install**.

    In the VMs for Selected Host <host name> section, the system displays the status.

10. To view the details, in the **Current Action** column, click **Status Details**.

    SMGR Patching Status window displays the details. The patch installation takes some time.

Upgrade Management field descriptions

Upgrade Elements

Name	Description
IP/FQDN	The IP address or the FQDN of System Manager virtual machine.
SMGR Name	System Manager name.
Upgrade Status	The status of the upgrade process. The status can be **Upgrading**, **Completed**, or **Failed**. The **Status Details** link provides more information about the System Manager upgrade.
Last Action	The last upgrade action.

Button	Description
Add Elements	Displays the Add Element page where you add System Manager.
Upgrade	Displays the Upgrade Management page where you upgrade the System Manager virtual machine.
Edit	Displays the Edit Element page where you can change the details of System Manager that you added.
Delete	Deletes the System Manager virtual machine.

Add Element field descriptions

Required Element information

Name	Description
SMGR IP	The IP address of System Manager
SMGR NAME	The name of the System Manager virtual machine.
SMGR SSH User Name	The SSH user name of System Manager
SMGR SSH Password	The SSH password of System Manager

Required C-DOM information

Name	Description
C-DOM IP/FQDN	The C-DOM IP/FQDN
C-DOM SSH User Name	The C-DOM SSH user name
C-DOM SSH Password	The C-DOM SSH password
C-DOM Root User Name	The C-DOm root user name
C-DOM Root password	The C-DOM root password

Button	Description
Save	Saves the element that you added.

Edit Elements field descriptions

Required Element information

Name	Description
SMGR IP	The IP address of System Manager
SMGR NAME	The name of System Manager virtual machine.
SMGR SSH User Name	The SSH user name of System Manager
SMGR SSH Password	The SSH password of System Manager

Required C-DOM information

Name	Description
C-DOM IP/FQDN	The C-DOM IP/FQDN
C-DOM SSH User Name	The C-DOM SSH user name
C-DOM SSH Password	The C-DOM SSH password
C-DOM Root User Name	The C-DOm root user name
C-DOM Root password	The C-DOM root password

Button	Description
Update	Updates the changes to the element.

Upgrade Management field descriptions

Name	Description
Install on Same ESXi	The option to select the same or a different server. The options are: • Select: To upgrade on the same server. • Clear: To upgrade to a different server. If you do not select the check box, you must add a new server or select a server from the list to which you want to update.
Host FQDN	The Host FQDN to which you want to update. The system displays the CPU and memory details of the host in the Capacity Details section.
VM Name	The virtual machine name displayed on the Add Element page.

Select Resource Pool and Data Store

Button	Description
Resource Pool	The login to the resources. The field is display-only.
Datacentre/Cluster	The data centre or the cluster. The field is display-only.
AVP host	The host type. The values are: • **Yes**: An Appliance Virtualization Platform host • **No**: An ESXi host The field is display-only.
Model	The server model. For example, ProLiant DL360 G8 and PowerEdge™ R620.
Data Store	The data store with the available size.

Capacity Details

The system displays the CPU and memory details of the host in this section. The fields are read-only.

Name	Description
Name	The name
Full Capacity	The maximum capacity
Free Capacity	The available capacity
Reserved Capacity	The reserved capacity
Status	The status

Deploy OVA

Name	Description
Select the OVA	The option to select a `.ova` file of the virtual machine that is available on System Manager.
Select OVA file	The absolute path to the `.ova` file of the virtual machine. The field is available only when you click **Select the OVA from Local SMGR**.
Submit File	Selects the `.ova` file of the virtual machine that you want to deploy. The field is available only when you click **Select the OVA from Local SMGR**. The system displays the network configuration details in the Network Parameters section based on the System Manager virtual machine.
Select Flexi Footprint	The footprint size supported for the selected server. The system validates for the CPU, memory, and other parameters in the Capacity Details section. You must ensure that the status is ✓.
Select bin file	The absolute path to the System Manager data migration bin file.
Select backup file	The absolute path to the backup of System Manager virtual machine.

Configuration Parameters

The system populates most of the fields depending on the OVA file. You must provide information, such as password, FQDN, and timezone.

Name	Description
Management IP Address (Out of Band Management IP Address)	The IP address of the System Manager virtual machine for Out of Band Management. The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network.
Management Netmask	The Out of Band Management subnetwork mask to assign to the System Manager virtual machine.
Management Gateway	The gateway IP address to assign to the System Manager virtual machine. For example, 172.16.1.1.
IP Address of DNS Server	The DNS IP addresses to assign to the primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,). For example, 172.16.1.2, 172.16.1.4.

Table continues…

Name	Description
Management Hostname	The hostname to assign to the System Manager virtual machine. For example, bouldervm2.
Default Search List	The search list of domain names. The field is optional.
NTP Server IP or FQDN	The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).
Time Zone	The timezone where the System Manager virtual machine is located. A list is available where you can select the continent and the country.

Public Network Settings

Name	Description
Public IP Address	The IP address to enable public access to different interfaces.
Public Netmask	The subnetwork mask to assign to System Manager virtual machine.
Public Gateway	The gateway IP address to assign to the System Manager virtual machine. For example, 172.16.1.1.
Public Hostname	The hostname to assign to the System Manager virtual machine. For example, bouldervm2.

Virtual FQDN

Name	Description
Virtual Hostname	The virtual hostname of the System Manager virtual machine. For example, grsmgr.
Virtual Domain	The virtual domain name of the System Manager virtual machine. For example, dev.com.

SNMPv3 Parameters

Name	Description
SNMPv3 User Name Prefix	The prefix for SNMPv3 user.
SNMPv3 User Authentication Protocol Password	The password for SNMPv3 user authentication.
Confirm Password	The password that you retype to confirm the SNMPv3 user authentication protocol.
SNMPv3 User Privacy Protocol Password	The password for SNMPv3 user privacy.
Confirm Password	The password that you must provide to confirm the SNMPv3 user privacy protocol.

Backup Definition

Name	Description
Schedule Backup?	• **Yes**: To schedule the backup jobs during the System Manager installation. • **No**: To schedule the backup jobs later. **Note:** If you select No, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server. **Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id	The login ID of the backup server to log in through the command line interface.
Backup Server Login Password	The SSH login password to log in to the backup server from System Manager through the command line interface.
Confirm Password	The password that you reenter to log in to the backup server through the command line interface.
Backup Directory Location	The location on the remote backup server.
File Transfer Protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.
Repeat Type	The type of the backup. The possible values are: • `Hourly` • `Daily` • `Weekly` • `Monthly`
Backup Frequency	The frequency of the backup taken for the selected backup type.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.

Table continues…

Name	Description
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be 6 hours later than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

Network Parameters

Name	Description
Out of Band Management IP Address	The port number that you must assign to the Out of Band Management port group. The field is mandatory.
Public	The port number that you must assign to public port group. The field is optional.

Button	Description
Upgrade	Displays the EULA acceptance screen where you must click **Accept** to start the upgrade.

Install on Same ESXi field descriptions

Name	Description
Install on Same ESXi	The option to select the same or a different server during the upgrade. The options are: • Select: To upgrade on same server. • Clear: To upgrade on a different server.
HOST FQDN	The fully qualified domain name. For example, platform.mydomain.com.

Upgrade job status

Upgrade job status

The Upgrade Job Status page displays the status of completion of every upgrade job that you performed. Every step that you perform to upgrade an application by using Solution Deployment Manager is an upgrade job. You must complete the following jobs to complete the upgrade:

1. **Refresh Element(s)**: To get the latest data like version data for the applications in the system.
2. **Analyze**: To evaluate an application that completed the Refresh Element(s) job.
3. **Pre-Upgrade Check**: To evaluate an application that completed the Analyze job.
4. **Upgrade**: To upgrade applications that completed the Pre-upgrade Check job.
5. **Commit**: To view commit jobs.
6. **Rollback**: To view rollback jobs.
7. **Uninstall**: To view uninstall jobs.

Viewing the Upgrade job status

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Job Status**.
3. On the Status of Upgrade Management Jobs page, in the **Job Type** field, click a job type.
4. Select one or more jobs.
5. Click **View**.

   The system displays the Upgrade Job Status page.

Deleting the Upgrade jobs

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Job Status**.
3. On the Upgrade Job Status page, in the **Job Type** field, click a job type.
4. Select one or more jobs.
5. Click **Delete**.

   The system updates the Upgrade Job Status page.

Upgrade Job Status field descriptions

Name	Description
Job Type	The upgrade job type. The options are: • **Refresh Element(s)**: To view refresh elements jobs. • **Analyze**: To view analyze jobs. • **Pre-Upgrade Check**: To view preupgrade check jobs. • **Upgrade**: To view upgrade jobs. • **Commit**: To view commit jobs. • **Rollback**: To view rollback jobs. • **Uninstall**: To view uninstall jobs.
Job Name	The upgrade job name.
Start Time	The time when the system started the job.
End Time	The time when the system ended the job.
Status	The status of the upgrade job. The status can be: SUCCESSFUL, PENDING_EXECUTION, PARTIAL_FAILURE, FAILED.
% Complete	The percentage of completion of the upgrade job.
Element Records	The total number of elements in the upgrade job.
Successful Records	The total number of times that the upgrade job ran successfully.
Failed Records	The total number of times that the upgrade job failed.

Button	Description
Stop	Stops the upgrade job.
Delete	Deletes the upgrade job.
Re-run Checks	Performs the upgrade job again.

Upgrades to Communication Manager Release 6.3.100

Communication Manager upgrades

System Manager provides the user interface to upgrade Communication Manager and the associated devices to Release 6.3.100. However, you must select the target release 6.3.8 from **Solution Deployment Manager** > **Upgrade Release Selection**.

The Software Inventory page in Upgrade Management consists of a collective inventory of different devices arranged in a hierarchy.

When you select more than one element in a hierarchy, the system creates a scheduler job for the upgrade. Each hierarchy can have only one job scheduled. The system determines the sequence in which the elements must be upgraded. The devices might include:

- Communication Manager
- Communication Manager Messaging
- Utility Server
- Branch Session Manager
- Gateways
- TN Boards
- Media modules

If one of the devices fails to upgrade within the hierarchy, the system might proceed or process the job as failed based on the compatibility of the failed device with the subsequent device.

Important:

You cannot select Communication Manager Release 5.2.1 and Avaya Virtualization Platform-based Communication Manager Release 6.x together. You can only upgrade Communication Manager Release 5.2.1 systems together or all Appliance Virtualization Platform-based Communication Manager Release 6.x systems at a time.

You can perform the following operations by using the **Upgrade Management** > **Software Inventory**:

- Get Inventory
- Analyze software
- Download
- Perform a preupgrade check
- Reset or backup Communication Manager
- Sequence upgrades
- Upgrade the following:
  - System Platform-based Communication Manager Release 6.x to Release 6.3.100
  - Linux-based Communication Manager Release 5.x to Release 5.2.1

    Note:

    Install System Platform on the supported server before you upgrade Communication Manager
  - All devices and components that run on Communication Manager
- Commit, rollback, or cancel the template upgrade
- Update Communication Manager, SAMP firmware, and MPC firmware
- Upgrade gateways, TN boards, and media modules

Checklist for upgrading Communication Manager to Release 6.3.100

Performing the initial setup

Task	Notes
1. Install the physical or virtual servers that support the Avaya Aura® applications that you want to deploy. 2. Deploy System Manager, Communication Manager, and Session Manager.	You require the working knowledge of the following Avaya Aura®applications: Communication Manager, System Manager, Session Manager, and Branch Session Manager. You require the working knowledge of the following processes: • Setting up PLDS. • Downloading Avaya Aura® applications from PLDS • Configuring a standalone FTP, SCP, HTTP, or SFTP server to host Avaya Aura® applications. You require the administrator credentials for the Avaya Aura® applications that you are upgrading.

Performing the preconfiguration steps

Task	Notes
Click **Save Trans** to save the changes that you have made.	
Ensure that you have sufficient disk space for the server that you have attached with the software library.	
Create a user with administrator credentials to gain access for the elements using HTTP, FTP, SCP or SFTP services.	Protocol requirements to configure a remote server on page 1154
For the Communication Manager instance that you have created, create a user and user profile.	Creating a new user account on page 175
Configure SNMP for the user.	Creating an SNMPv3 user profile on page 883
Create the EPW file for the Communication Manager instance by using the following templates: • Embedded CM Main • Embedded Survivable Remote	
Add the following files: 1. System Platform authentication file 2. Communication Manager 6.x license file	

Table continues…

Task	Notes
Ensure that you have the PLDS access credentials and Company ID.	
Administer Branch Session Manager in System Manager.	

Managing elements inventory

Task	Notes
Configure Communication Manager for administration and SNMP access.	Creating an SNMP target profile on page 886
Configure the access to the H.248 gateway device.	Adding a G430 or G450 gateway to System Manager on page 862

Performing the software management configuration settings

Task	Notes
Option 1: Set up PLDS access through the Avaya Support site at https://support.avaya.com.	Log in to the PLDS website at http://plds.avaya.com. Use your PLDS account to get your Company ID. On the System Manager web console, go to **Services** > **Solution Deployment Manager** > **User Settings**. Enter the following details to get entitlements for analyze and artifacts for download: 1. SSO user name 2. SSO password 3. Company ID
Option 2: Set up the PLDS access through an alternate source.	
Set up the software library.	Creating a software library on page 1160

Performing the upgrade process

Task	Notes
Collect the software inventory.	Perform the Get Inventory operation when you modify the PLDS access or alternate source. For more information, see Software inventory on page 1232
Perform the Analyze Software operation for the Communication Manager element that you selected.	Analyzing the software on page 1238
Download the software.	Downloading the software on page 774
Run the preupgrade check for the selected Communication Manager device.	Performing a preupgrade check on page 1240

Table continues…

Task	Notes
Run the upgrade operation.	Upgrading a Communication Manager on page 1275 Upgrading a Communication Manager Release 5x on page 1266 Upgrading communication manager 6x on page 1246 **Note:** The upgrade process takes about 2.5 hours to complete.

Installing the service packs

Task	Notes
Installing the service pack or software patches on Communication Manager.	Updating Communication Manager on page 1276
Updating the **H.248 Media Gateway** device.	1. In the alternate source location, download the patch file `g450_sw_36_9_0.bin`. 2. For the gateway that you have selected, perform the Analyze job. 3. On the Select Gateway (G) panel, select **Library and download protocol** . 4. Click **Download**. 5. Click the active status link to observe the progress of upgrade.

Getting inventory

About this task

Before you perform any operation on Communication Manager 6.3.x or earlier, perform the get inventory operation to ensure that the system reflects the exact state of the device in Software Inventory.

Do not perform the following during an upgrade:

- The get inventory operation when the upgrade is in progress.
- The analyze operation when the upgrade is in progress.
- The analyze operation during the get inventory operation.
- Log on the Dom0, Cdom, or virtual machine.

Before you begin

- Configure the SNMP parameters on the device before you configure the same device in System Manager from Manage Elements.

> **Note:**
>
> Use the same SNMP credentials for the device in System Manager.

- To upgrade a Communication Manager device, you must configure a profile 18 user on Communication Manager. You cannot use init and craft user profiles while configuring a profile 18 user.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select the device or devices for which you want to obtain the inventory, and perform the following:
   - To get the inventory now, click **Get Inventory** > **Now**.
   - To get the inventory later, click **Get Inventory** > **Schedule**.

   > **Note:**
   >
   > If you click **Get Inventory**, the system automatically analyzes the devices. You need not analyze the devices again.

Analyze software

The analyze software operation finds and displays the latest release of a device in the **Available Software** column. This operation changes the icon in the **State** column after comparing the current software version of the device with the latest version. To get the latest version, use **Get Inventory**.

> **Note:**

Icon	State	Description
?	Unknown	Indicates that the device is yet to be analyzed.
⊗	Update Required	Indicates that a new version of the software is available and the device must be upgraded. Also indicates that the software file is not downloaded to the System Manager software file library.
⚠	Ready to Update	Indicates that an upgrade is required for the device and the new version of the software is downloaded to the software file library. Also indicates that the device is ready for upgrade. .
✓	Updated	Indicates that the device is on the latest version.

Table continues…

Icon	State	Description
ℹ	Non Upgradable	Indicates that you cannot upgrade the component, and the component is only listed as part of the inventory.
Ⓔ	Unentitled	Indicates that the new version of the software is available, but you are not entitled to the new version.

Analyzing the software

About this task

Using the analyze feature, you can identify whether a new software is available for the inventory that you collected, and whether you have permissions to download the software.

Before you begin

- Get the inventory. If multiple sites work on the same survivable remote server, get the inventory before you perform the analyze operation.
- Configure user settings.
- Ensure that the inventory is populated.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select one or more devices, and perform one of the following:
    - To analyze all devices, click **Analyze** > **Analyze All Now**.
    - To analyze all devices at a later time, click **Analyze** > **Analyze All Scheduled**.
    - To analyze selected devices, click **Analyze** > **Analyze Selected Now**.
    - To analyze selected devices at a later time, click **Analyze** > **Analyze Selected Scheduled**.

Downloading the software

Before you begin

- Analyze the software.
- Create a software library.

- Ensure that 9 GB disk space is available on System Manager.

  To view the available disk space, log in to the System Manager command line interface, and type `df -h /opt/Avaya/`.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select the devices, and click **Download**.

   The system displays the File Download Manager page.
6. For Branch Session Manager, perform the following:
   a. In the **Select Software/Hardware Types.** section, select Branch Session Manager and click **Show files**.
   b. Select `asm-patch-6.3.2.1.632006.sh`.
7. In the **Select Files Download Details** section, select **Source** and the files that you want to download.

   Note:

   Do not select the redundant `6.3.0.0.1105.iso` file.

   Based on the type of the software or hardware, select the required `6.3.0.0.1105.iso` file.
8. Click **Download**.

   The system displays the Files Download Manager — Library and Protocol Selection page.
9. Select the **Library** and **Protocol**, and click **Download**.
10. On the End User Licensing Agreement page, read the License Agreement, and if you agree to its terms, click **I Agree to the above end user license agreement** and do one of the following:
    - Click **Now** to begin the download immediately.
    - Click **Schedule** to schedule the download for a later time.

    The system displays the Files Download Manager page, where the **File Download Status** section displays the download details.

Result

After you download the recommended files, on the Software Inventory page the state of the device changes to ⚠ that is “ready to update”.

Performing a preupgrade check

Before you begin

For Communication Manager 5.2.1:

- Create the authorization file for System Platform, and store the file in a local folder.

  For more information, contact Avaya support team.
- Create the new EPW file for the Communication Manager to be upgraded, and provide all credentials to the EPW file including System Platform details. Store the EPW file on the HTTP or HTTPS server.

  For more information, contact Avaya support team.
- Get the WebLM server IP address for licensing.

  For more information contact the Avaya support team.
- Get the inventory for Communication Manager 5.2.1.
- Analyze the software.
- Download the related firmware for Communication Manager 5.2.1 upgrade.

For Communication Manager 6.x:

- Get the inventory.
- Analyze the software.
- Download the related firmware for the Communication Manager upgrade.
- Run the preupgrade check for the supported servers, compatible template, and the memory requirement in System Manager.

  For more information, see Hardware requirement checks during preupgrade check.

About this task

Install the latest System Platform on the server. You can stop the preupgrade check for elements that are in queue.

Note:

- System Platform must be on the same subnetwork as Communication Manager 5.2.1.
- During preupgrade, if the mandatory check fails, the **Upgrade** button becomes unavailable.
- If you fail to perform preupgrade, the **Upgrade**, **Commit**, **Rollback**, **Cancel Template Upgrade**, **Backup CM/CMM**, and **More Actions** buttons become unavailable.
- You can select about four templates to perform the preupgrade check.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.

4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select the templates that you want to upgrade.

   You can select only templates.
6. Click **Pre-Upgrade Check**.

   The system displays the status with the icons. For more information, see Preupgrade status.
7. To run the preupgrade check for templates again, on the Pre-upgrade Check Running Status page, select one or more templates and click **Run**.
8. **(Optional)** To stop the committed preupgrade check for the template, click **Cancel**.
9. On the Software Inventory page, view the status of the preupgrade check for an element in the **Pre-Upgrade Check Status** column.

Related links

Preupgrade status on page 1244
Preupgrade checks on page 1241

Preupgrade checks

The system runs the following preupgrade checks for Communication Manager 5.2.1:

- Mandatory checks:
  - Hardware compatibility check
  - Required files download check
- Recommended check:
  - Sufficient memory check

The system runs the following preupgrade checks for System Platform-based Communication Manager 6.x:

- Mandatory checks:
  - RAID battery check
  - Hardware compatibility check
  - Required files download check
  - CDOM credentials check
  - Disk space check
- Recommended check:
  - Sufficient memory check
  - Version compatibility check
  - Bandwidth is sufficient check

- Informational check:
  - Sufficient memory check

Note:

Do not perform any jboss operations while upgrade is in progress.

Preupgrade checklist for Linux® Operating System upgrades

Perform the following checks before you start upgrading elements that you have deployed on System Manager on Linux® Operating System to System Manager on Appliance Virtualization Platform, on the same server or a different server:

Note:

No.	Task	✔
1	Ensure that you assign a different IP address for the ESXi host	
2	After you perform the **Refresh Element(s)** operation, ensure that your system contains the latest version of all elements.	
3	On the User Settings page, ensure that PLDS or the alternate source are configured correctly.	
4	After you perform the **Analyze** operation, verify on the Upgrade Job status page that the operation you performed is successful.	
5	Download the OVA file for the element that you want to upgrade.	
6	After you have performed the **Analyze** job, verify that the element that you want to upgrade displays the **Ready for Upgrade** status.	
7	On the Pre-upgrade Check Job Details page, ensure that the status of the element that you want to upgrade displays **Successful**.	
8	In the **Upgrade Job** status, in the Pre-upgrade Configuration page, verify the configuration values are correct.	

Pre-upgrade checklist for System Platform upgrades

Perform the following checks before you start upgrading elements on System Manager that you have deployed on System Platform to System Manager on System Platform, on the same server or a different server:

Note:

No.	Task	✔
1	Ensure that you assign a different IP address for the ESXi host.	

Table continues…

No.	Task	✔
2	Ensure that you have added all the elements on the System Platform and you have established a structural relationship among all those elements.	
3	After you perform the **Refresh Element(s)** operation, ensure that your system contains the latest version of all the elements.	
4	On the User Settings page, ensure that the PLDS or the Alternate source are configured correctly.	
5	After you perform the **Analyze** operation, verify on the Upgrade Job Status page that the operation that you performed is successful.	
6	Download the OVA file for the element that you want to upgrade.	
7	After you have performed the **Analyze** job, verify that the element that you want to upgrade displays the **Ready for Upgrade** status.	
8	On the Pre-upgrade Check Job Details page, ensure that the element that you want to upgrade displays status as **Successful**.	
9	In the **Upgrade Job Status** section, on the Pre-upgrade Configuration page, verify the configuration values are correct.	

Hardware requirement checks during a preupgrade check

During the preupgrade check, the system checks the supported servers, template compatibility, and memory requirement in System Manager.

Template	Server type	Minimum memory requirement
CM_Duplex	Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, HP ProLiant DL360 G7, and HP ProLiant DL360p G8	12 GB
CM_Simplex	Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, HP ProLiant DL360 G7, and HP ProLiant DL360p G8	8 GB
CM_SurvRemote	Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, HP ProLiant DL360 G7, and HP ProLiant DL360p G8	8 GB
CM_SurvRemoteEmbed	S8300D	8 GB
CM_onlyEmbed	S8300D	8 GB

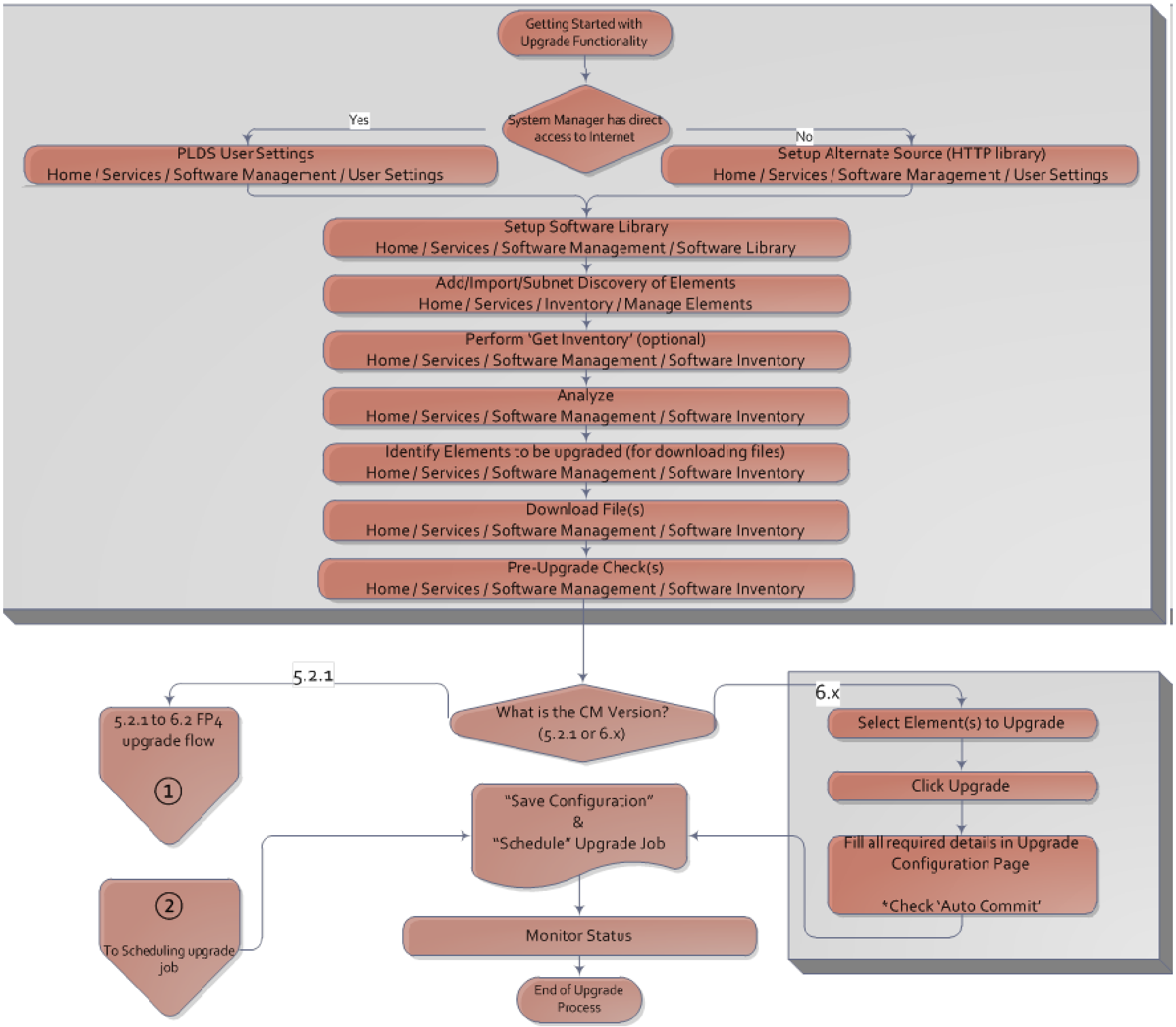
Preupgrade status

Icon	State	Description
?	Unknown or Not-Started	Indicates that the preupgrade check has not started, or was not run earlier.
⊗	Failed	Indicates that one or more mandatory preupgrade checks failed, and the failed elements are unavailable for upgrade as the probability of upgrade failure is high.
⚠	Success with recommended check failure	Indicates that mandatory preupgrade checks are successful, but one or more recommended checks failed. The elements are available for upgrade as the probability of upgrade failure is less.
✓	Successful	Indicates that all preupgrade checks are successful, and the probability of successful upgrade is high.

Upgrading Communication Manager 6.0, 6.1, or 6.2 to 6.3

Communication Manager upgrade workflow

Procedure


Getting Started with Upgrade Functionality
System Manager has direct access to Internet
Yes
No
PLDS User Settings
Home / Services / Software Management / User Settings
Setup Alternate Source (HTTP library)
Home / Services / Software Management / User Settings
Setup Software Library
Home / Services / Software Management / Software Library
Add/Import/Subnet Discovery of Elements
Home / Services / Inventory / Manage Elements
Perform 'Get Inventory' (optional)
Home / Services / Software Management / Software Inventory
Analyze
Home / Services / Software Management / Software Inventory
Identify Elements to be upgraded (for downloading files)
Home / Services / Software Management / Software Inventory
Download File(s)
Home / Services / Software Management / Software Inventory
Pre-Upgrade Check(s)
Home / Services / Software Management / Software Inventory
5.2.1
What is the CM Version? (5.2.1 or 6.x)
6.x
5.2.1 to 6.2 FP4 upgrade flow
1
2
To Scheduling upgrade job
Select Element(s) to Upgrade
Click Upgrade
Fill all required details in Upgrade Configuration Page
*Check 'Auto Commit'
"Save Configuration" & "Schedule" Upgrade Job
Monitor Status
End of Upgrade Process

Related links

- Analyze software on page 1237
- CM Upgrade Configuration field descriptions on page 1260
- Analyzing the software on page 1238
- Performing a preupgrade check on page 1240
- Preupgrade checks on page 1241
- System Platform Templates Upgrade Configuration field descriptions on page 1250
- Software Inventory field descriptions on page 1253
- Device list on page 835

Communication Manager 6.x upgrade checklist

For upgrades to Communication Manager 6.3.100, customer must reconfigure the SNMP alarming on the upgraded system.

No.	Task	References	✔
1.	Install System Platform and the required patch on the supported server.	—	
2.	Discover the devices that you want to upgrade by enabling SNMP or adding from Discovery on the Manage Elements page.	Creating discovery profiles and discovering elements on page 834	
3.	Configure user settings.	Establishing PLDS connection to Avaya on page 1148	
4.	Create a remote software library.	Creating a software library on page 1160	
5.	Get the inventory for Communication Manager 6.x.	Getting inventory on page 1236	
6.	Analyze the software.	Analyzing the software on page 1238	
7.	Download the related firmware for the Communication Manager upgrade.	Downloading the software on page 1238	
8.	Run the preupgrade check.	Performing a preupgrade check on page 1240	
9.	Perform the upgrade.	Upgrading Communication Manager 6.0, 6.1, or 6.2 to 6.3.100 on page 1246	
10.	Verify that the upgrade is successful.	Verifying the upgrade on page 1248.	

Related links

Device list on page 835

Upgrading Communication Manager 6.0, 6.1, or 6.2 to 6.3.100

About this task

Use the procedure to upgrade Communication Manager 6.0, 6.1, or 6.2 that is running on System Platform to Release 6.3.100.

For the supported upgrade paths of System Platform, see *Upgrading Avaya Aura® System Platform*.

Important:

For duplex system, first upgrade the standby Communication Manager. When the standby Communication Manager upgrade is complete, upgrade the active Communication Manager.

For more information about postupgrade steps for duplex templates, see *Upgrading Avaya Aura® Communication Manager*.

When you upgrade a System Platform-based Communication Manager with:

- Branch Session Manager, the system upgrades Branch Session Manager

- Communication Manager Messaging, the system upgrades Communication Manager Messaging

Before you begin

- Get the inventory.
- Analyze the software.
- Download the software.
- Run the preupgrade check.
- Run the hardware requirement checks during the preupgrade check.

  During the preupgrade check, the system checks the supported servers, template compatibility, and the memory requirement in System Manager.

  For more information, see Hardware requirement checks during a preupgrade check.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select the templates that you want to upgrade.
6. Click **Upgrade**.
7. On the System Platform Template(s) Upgrade Configuration page, select one or more templates of the same type.
8. In the **Upgrade Configuration** section, select the templates that you want to upgrade and complete the fields.

   For more information, see System Platform Template(s) Upgrade Configuration field descriptions.
9. Perform one of the following actions:
   - To upgrade the solution template automatically, select **Auto Commit Upgrade**.

     Important:

     You cannot perform rollback if you select **Auto Commit Upgrade**.
   - To commit the upgrade of the Communication Manager template manually, perform the following:
     a. Clear the **Auto Commit Upgrade** check box.
     b. On the Software Inventory page, click **More Actions** > **Commit Template Upgrade**.
10. **(Optional)** If you find any errors or issues, click **More Actions** > **Rollback Template Upgrade**.

    The system rolls back the software to the original version.

11. **(Optional)** To stop the upgrade during template installation, click **More Actions** > **Cancel Template Upgrade**.
12. Click **Save the configuration**.
    - To cancel the operation, click **Clear configuration**.
13. In the **Job Schedule** section, perform one of the following:
    - To upgrade the device, click **Now**.
    - To upgrade the device at a later time, click **Later**.
14. Click **Upgrade**.

Next steps

Verify that the upgrade is successful.

For more information, see “Verifying the upgrade”.

Related links

Analyze software on page 1237
Analyzing the software on page 1238
Performing a preupgrade check on page 1240
Preupgrade checks on page 1241
Device list on page 835

Verifying the upgrade

Before you begin

Complete the upgrade of Communication Manager and devices.

About this task

Important:

For more information about postupgrade steps for a duplex template, see *Upgrading Avaya Aura® Communication Manager*.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, click the status of the Communication Manager device to view the logs and the description of the upgrade operation.

   The system displays the status of the upgrade in **Status** column.
6. To verify that the upgrade is successful, check the following on the Software Inventory page:
    - The **Release** column displays the updated icon ✓.

- The **Update** column displays the updated icon ✓.
- The **Sw Release** changed from the previous release to the latest upgraded release.
- The **Status** changed from **Upgrade Scheduled** to **IDLE**.

7. Validate that the Communication Manager 5.2.1 server data that is restored on Release 7.0. If the server data on the Release 7.0 system is incomplete, complete the required fields.

   Important:

   This validation applies only to Communication Manager Release 5.2.1.

   For more information about the following, see *Upgrading Avaya Aura® Communication Manager*:

   - Recording the configuration screens.
   - Worksheet for upgrading Communication Manager to simplex and embedded templates.

Sample scenario to upgrade Communication Manager Release 6.x to 6.3.100

To upgrade Communication Manager Release 6.x to 6.3.100, do the following:

1. Perform the Preupgrade tasks on page 1249
2. Perform the Upgrading Communication Manager 6.x to 6.3.100 on page 1250
3. Perform Verifying the upgrade on page 1248

Preupgrade tasks

No.	Task	References	✔
1.	Discover the devices that you want to upgrade by enabling SNMP or adding from Discovery on the Manage Elements page.	Discovering elements on page 834	
2.	Configure user settings.	Configuring user settings on page 1148	
3.	Create a remote software library.	Creating a software library on page 1160	
4.	Get the inventory for Communication Manager 6.x.	Get inventory software inventory on page 1236	
5.	Analyze the software.	Analyzing the software for software inventory on page 1238	
6.	Download the related firmware for the Communication Manager upgrade.	Downloading the software for software inventory on page 1238	
7.	Run the preupgrade check.	Performing the preupgrade check on page 1240	

Upgrading Communication Manager 6.x to 6.3.100

Before you begin

Complete the preupgrade tasks.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select the Communication Manager 6.x device that you want to upgrade.
6. Click **Upgrade**.
7. On the System Platform Template(s) Upgrade Configuration page, select **CM_Simplex**.
8. In the **Upgrade Configuration** section, select one or more templates that you want to upgrade and complete the fields.

   For more information, see System Platform Template(s) Upgrade Configuration field descriptions.
9. Click **Save the configuration**.
10. In the **Job Schedule** section, click **Now**.
11. Click **Upgrade**.

    On the Software Inventory page, the system displays the status of the upgrade in **Status**. Click the status of the Communication Manager device to view the logs and the description of the upgrade operation.

Related links

Upgrading Communication Manager 6.0, 6.1, or 6.2 to 6.3.100 on page 1246
System Platform Templates Upgrade Configuration field descriptions on page 1250
Software Inventory field descriptions on page 1253

System Platform Templates Upgrade Configuration field descriptions

Name	Description
Upgrade Source	The source where you have the installation file. The source can be the remote server software library.
Available System Platform	The available System Platform for the upgrade. The field applies only for Communication Manager Release 5.2.1 upgrade.
EPW file	The EPW file available for the upgrade.

Table continues…

Name	Description
	The field applies only for Communication Manager Release 5.2.1 upgrade.
Template Name	The Communication Manager template available for the upgrade: • CM_Simplex • CM_SurvRemoteEmbed • CM_SurvRemote • CM_onlyEmbed • CM_Duplex The field applies only for Communication Manager Release 5.2.1 upgrade. For Communication Manager Release 6.x, the field is read-only.
CM/CMM Backup/Restore File Server	The file server used for storing backup data during the upgrade. The field applies only for Communication Manager Release 5.2.1 upgrade.
Authentication File	The link to authenticate the file. The field applies only for Communication Manager Release 5.2.1 upgrade.
WebLM Server IP Address	The WebLM server IP address. The field applies only for Communication Manager Release 5.2.1 upgrade.
Communication Manager IP Address	The Communication Manager IP address. The Communication Manager IP address must be the same as the selected Communication Manager to be upgraded. The field applies only for Communication Manager Release 5.2.1 upgrade.
Upgrade To	The Communication Manager template version that you want to upgrade to.
Branch Session Manager	The Branch Session Manager available for the upgrade. The **Branch Session Manager** IP address must be of the same name as mentioned in the **EPW** file.
Branch Session Manager Login	The Branch Session Manager login name.
Branch Session Manager Password	The Branch Session Manager password. The password must not exceed nine letters.

Table continues…

Name	Description
Branch Session Manager Enrollment Password	The Branch Session Manager enrollment password. The password must not exceed nine letters.
Utility Server	The Utility Services virtual application.
Communication Manager	The version of Communication Manager that you want to upgrade to.
System Platform Upgrade Version	The System Platform release upgrade that you want to upgrade to.
System Platform Update Version	The System Platform patch upgrade version that you want to update the version to.
Utility Server IP Address	The Utility Services IP address. The name of **Utility Server IP Address** must be the same as mentioned in the **EPW file**. The field applies only for Communication Manager Release 5.2.1 upgrade.
Auto Commit Upgrade	The option to automatically commit the template upgrade. • If you select **Auto Commit Upgrade**, the system automatically upgrades System Platform. **Important:** If you select **Auto Commit Upgrade**, you cannot roll back the template upgrade. • If you do not select **Automatic Commit Upgrade**, the system displays **Waiting** or **RollBack** for **Commit** on the Software Inventory page. On the System Inventory page, click **More Actions** > **Commit Template Upgrade**.
CM VM Kernel,Platform Patching	The kernel patch or platform patch for the Communication Manager virtual machine. **Note:** • If selected, the kernel and platform patching must be performed implicitly on the Communication Manager virtual machine. • If not selected, the kernel and platform patching must be performed manually on the Communication Manager virtual machine. For more information, see *Deploying Avaya Aura® Communication Manager on System Platform*.
CM VM Platform Patch	The platform patch for the Communication Manager virtual machine.

Table continues…

Name	Description
CM VM Kernel Patch	The kernel patch for the Communication Manager virtual machine.
Override Recommended Failure	The checkbox that specifies whether the system must override any recommended preupgrade check failure that occurs during the element upgrade. When you select this checkbox, the system tries to upgrade the element. **Note:** You must select **Override Recommended Failure** if one or more of the earlier recommended preupgrade checks have failed.

Note:

If a version is unavailable in the library, the system displays a warning for the following fields:

- **Upgrade To**
- **Communication Manager**
- **System Platform Upgrade Version**
- **System Platform Update Version**

Button	Description
Done	To save the information that you enter.
Reset	To clear the values that you enter.
Now	To begin the upgrade.
Schedule	To schedule the upgrade for later.
Cancel	To cancels the upgrade.

Software Inventory field descriptions

Name Adjust column width	Description
Select	The option to select a group.
Name	The name of the device.
Release	The release state.
Update	The update state.
Pre-Upgrade Check Status	The status of the preupgrade check.
IP Address	The IP address.
Type	The device type.
Sw Release	The software release.
Status	The status of the device for upgrade.

Table continues…

Name Adjust column width	Description
Location	The location of the device.
Family	The family of the device.

Button	Description
Get inventory > **Now**	To get the components of the device software.
Get inventory > **Schedule**	To get the components of the device software at a later time.
Analyze > **Analyze All Now**	To analyze whether any new firmware for all device software is available.
Analyze > **Analyze All Scheduled**	To analyze at a later time whether any new firmware for all device software is available.
Analyze > **Analyze Selected Now**	To analyze whether any new firmware for the selected device is available.
Analyze > **Analyze Selected Schedule**	To analyze at a later time whether any new firmware for the selected device is available.
Download	To download the required files for one or more devices.
Pre-upgrade Check	To display the system requirement for an upgrade as follows: • The required bandwidth of the selected device. • The required entitlements downloaded by the System Manager and the selected device.
Upgrade	To upgrade the device template.
More Actions > **Commit**	Prompts you to save the changes you made to the selected Communication Manager, Gateway, or the loads the previous release on the selected Communication Manager, System Platform template, Gateway template. Do one on the following actions; • **Now**: To commit the upgrades to the latest release on the selected Communication Manager, Gateway, or the System Platform template. • **Later**: To commit the upgrades to the latest release on the selected Communication Manager, Gateway, or the System Platform template at a later time. • **Cancel**: To cancel the upgrades to the latest release on the selected Communication Manager, Gateway, or the System Platform template.

Table continues…

Button	Description
More Actions > **Rollback**	Loads the previous release on the selected Communication Manager, System Platform template, gateway. The options are: • **Now**: To rollback the upgrades to the previous release on the selected Communication Manager, Gateway, or the System Platform template. • **Later**: To rollback the upgrades to the previous release on the selected Communication Manager, gateway, or the System Platform template at a later time. • **Cancel**: To cancel the rollback of the upgrades to the previous release on the selected Communication Manager, gateway, or the System Platform template.
More Actions > **Reset**	Restarts the selected Communication Manager, or Gateway. The options are: • **Now**: To restart the selected Communication Manager or Gateway. • **Later**: To restart the selected Communication Manager or Gateway. • **Cancel**: To cancel the restart on the selected Communication Manager or Gateway. Reset operation is service affecting, with higher levels being increasingly destructive that can close the SAT login. Certain conditions can result in a higher reset level than the reset requested.
More Actions > **Cancel Template Upgrade**	Cancels the System Manager template upgrade. The options are: • **Now**: To cancel the template upgrade on the selected System Platform solution template. • **Later**: To cancel the template upgrade on the selected System Platform solution template at a later time. • **Cancel**: To cancel the cancel template upgrade on the selected System Platform solution template.
More Actions > **Backup CM/CMM**	Displays the Backup Configuration page where you can create a backup of Communication Manager 5.2.1 that you want to upgrade. For more information see, Backing up Communication Manager.

Table continues…

Button	Description
	The field applies only for Communication Manager Release 5.2.1 upgrade.
Advanced Search	Displays fields where you can specify the criteria for searching a group.
Filter: Enable	Displays fields where you can set the filter criteria. This button is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This button is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters groups based on the criteria.
Select: None	Clears all check boxes.

Icon	Description
🔄	Refreshes the group information.

Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link in the upper-right corner of the page.

Field	Description
Criteria	The criteria for search operation. The page displays the following fields: • **Field 1:** The list of criteria to search groups. • **Field 2:** The list of operators for evaluating the expression. This list of operators depends on the criterion that you selected in **Field 1**. • **Field 3:** The value of the search criterion. The Software Inventory service retrieves and displays the devices that match this value.

Icon	Description
+	Adds a row after **Field 1**, **Field 2**, and **Field 3** to add more search conditions.
-	Deletes the row with the search conditions.

Button	Description
Clear	Clears the search value that you entered in **Field 3**.
Search	Searches the group based on the specified search conditions, and displays the results in the **Groups** section.
Close	Cancels the search operation, and hides the **Criteria** section.

Upgrading Communication Manager 5.2.1

Communication Manager Release 5.2.1 upgrade

You can upgrade Communication Manager Release 5.2.1 to Release 6.3.100 on a different server. For example:

- You can upgrade Communication Manager Release 5.2.1 running on a different server. On the CM Upgrade Configuration page, you must click **Upgrade** for the system to perform the upgrade. For more information, see “Upgrading to Communication Manager on a different server”.
- You must perform **Get Inventory** to get the latest state of System Platform before you upgrade Communication Manager Release 5.2.1 to Release 6.3.100 on a different server. You must perform the step in the following scenario:
  1. On your system, you have added System Platform to the inventory
  2. After adding System Platform, you have applied latest software patch from the System Platform web console.

Related links

Upgrading Communication Manager 5.2.1 to Release 6.3.100 on a different server on page 1266

Communication Manager 5.2.1 upgrade checklist

No.	Task	References	✔
1.	Install System Platform and the required patch on the supported server.	—	
2.	Discover the devices that you want to upgrade by enabling SNMP or adding from Discovery on the Manage Elements page.	Discovering elements on page 834	
3.	Configure user settings.	Configuring user settings on page 1148	
4.	Create a remote software library.	Creating a software library on page 1160	
5.	Record the server data for Communication Manager 5.2.1 in the worksheet.	For more information about the following, see *Upgrading Avaya Aura® Communication Manager*: • Recording the configuration screens. • Worksheet for upgrading Communication Manager to simplex and embedded templates.	

Table continues…

No.	Task	References	✔
6.	Create the authorization file for System Platform, and store the file in **My Computer**.	For more information, contact the Avaya support team.	
7.	Create the new EPW file for the Communication Manager selected for upgrade, and provide all credentials to the EPW file including System Platform details. Store the EPW file on the HTTP or HTTPS server.	For more information, contact the Avaya support team.	
8.	Get the WebLM server IP address for licensing.	For more information, contact the Avaya support team.	
9.	Get the inventory for Communication Manager 5.2.1.	Get inventory software inventory on page 1236	
10.	Analyze the software.	Analyzing the software for software inventory on page 1238	
11.	Download the related firmware for the Communication Manager upgrade.	Downloading the software for software inventory on page 1238	
12.	Perform a preupgrade check.	Performing the preupgrade check on page 1240	
13.	Perform the upgrade.	Upgrading Communication Manager 5.2.1 on page 1266	
14.	Verify that the upgrade is successful.	Verifying the upgrade on page 1248	
15.	Validate that the Communication Manager 5.2.1 server data that is restored on 6.3.100 is complete.	Verifying the upgrade on page 1248	

Related links

Device list on page 835

Backing up Communication Manager or Communication Manager Messaging

Before you begin

- Get the inventory.
- Analyze the software.
- Download the software.

About this task

Perform the routine backup of Communication Manager 5.2.1 and Communication Manager Messaging. You also need to take a backup before you upgrade Communication Manager in the semi-automated mode.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select the template that you want to upgrade and click **More Actions** > **Backup CM/CMM**.
6. On the Backup Configuration page, do the following:
    a. From the list of available elements, select the element that you want to upgrade.
    b. In the Upgrade Operations section, in **CM/CMM Backup/Restore File Server**, click the appropriate file server where you want to take the backup.
    c. Select the **Ready for Upgrade** check box.

       The system marks the Communication Manager device used for upgrade. Communication Manager becomes unavailable for any administrative operations such as incremental synchronization.
7. In the **Job Schedule** > **Schedule Job** section, do one of the following:
    - To perform the backup immediately, click **Now**.
    - To perform the backup later, click **Later**.
8. Click **Backup CM/CMM**.

Result

On successful completion of the backup, if you have selected the **Ready for Upgrade** check box, Communication Manager:

- Shuts down, except when running on the S8300D server
- Becomes nonoperational until the upgrade is complete

Next steps

You can start the upgrade after successful completion of the backup.

To start the upgrade, on the CM Upgrade Configuration page, click **Upgrade**.

Backup Configuration field descriptions

Upgrade Operations

Name	Description
CM/CMM Backup/Restore File Server	The backup file server address for backup.
Ready for Upgrade	The option to select the Communication Manager device for upgrade.

Table continues…

Name	Description
	Communication Manager becomes unavailable for any administrative operations such as incremental synchronization. On successful completion of the backup, Communication Manager shuts down, except when running on the S8300D server, and becomes nonoperational until the upgrade is complete. **Note:** When you select the check box, system does not refresh this Communication Manager when you perform the get inventory operation. You must clear the check box to refresh Communication Manager during the get inventory operation.

Button	Description
Save the configuration	Saves the backup configuration with the latest modifications.
Clear configuration	Resets the backup configuration page to the default settings.
Backup CM/CMM	Creates a backup copy of the selected Communication Manager or Communication Manager Messaging element.
Cancel	Cancels the backup operation and returns to the CM Backup Configuration page.

CM Upgrade Configuration field descriptions

The following table is updated when you choose the upgrade, update, or license authentication operations for Communication Manager. You can upgrade or update multiple Communication Manager devices simultaneously.

Name	Description
Element Name	The name of Communication Manager.
IP Address	The IP address of the Communication Manager device.
Software Version	The software version of Communication Manager that you selected.
Server Status	Specifies whether Communication Manager is active or standby. The **Server Status** field is applicable only to the duplex Communication Manager.
Operation	The upgrade operation that you want to perform for the Communication Manager devices that you choose.

Table continues…

Release	The current version of Communication Manager.
SAMP/MPC	The SAMP firmware that is available.
CM Service Pack	The Communication Manager service pack available.
SES Service Pack	The SES service pack available.
Kernel Update	The kernel update available.
Platform/Security Update	The platform or security update available.
License File	The license file that you downloaded for the upgrade operation.
Authentication File	The authentication file that you downloaded for the upgrade operation.

Upgrade operations

The system displays the following fields for upgrading Communication Manager 5.x to Communication Manager 5.2.1.

Field	Description
Operation	The operation that you want to perform. The options are: • **Copy Release**: To copy the release file from a CD-ROM or a URL. • **Install Release**: To install the Communication Manager release that you selected. • **Copy & Install Release**: To copy the installation file and install the Communication Manager release using the file.
Source	The source the installation file is made available. The source can be a remote server or CD-ROM on Communication Manager.
Method	The remote server protocol. The **Method** field applies only for a remote server. For SCP, FTP, and SFTP, provide the user name, password, host name, and directory name. For HTTP and HTTPS, provide the URL and proxy details.
Auto Commit Upgrade	The option to specify if a backup of the current release is available. The options are: • **Yes**: A backup of the current release is available. Rollback is not possible if you select yes. • **No**: A backup of the current release is unavailable. Rollback is possible if you select no.

The system displays the following fields for upgrading the Communication Manager 5.2.1. to Communication Manager 6.x and later.

Field	Description
Upgrade Source	The source where the installation file is available. The can be Software Library that can be used for semi-automated upgrade. You must install System Platform and the latest software patch and click **Upgrade** for the system to perform the upgrade. ✱ **Note:** Based on the **Upgrade Source** you select, the system displays different sets of templates in the **Select Templates** field.
Available System Platform	System Platform that is available for the upgrade. The field applies only for Communication Manager Release 5.2.1 upgrade.
EPW file	The complete path of EPW file that is available for upgrade. For example, `http://<file-server>/epw.zip`. This valid file server must support HTTP or HTTPS protocol. You must copy the EPW file on the server and the EPW file must be made available on the server before you begin the upgrade. You require the EPW file for the solution template upgrade. The file consists of the IP address and network details of System Platform and virtual machines. Ensure that you gain access to the EPW file from System Manager and System Platform at the http url that is specified in the field. You can create the EPW file by using EPW installer tool available with System Platform.
Select Template	The Communication Manager template available for the upgrade. The options are: • CM_Simplex • CM_SurvRemoteEmbed • CM_SurvRemote • CM_onlyEmbed • CM_Duplex The field applies only for Communication Manager Release 5.2.1 upgrade.

Table continues…

Field	Description
	Note: The system displays different sets of templates in the **Select Template** field based on the **Upgrade Source** that you select. For Communication Manager Release 6.x, the field is read-only. **Note:** Based on the template that you select, the system displays appropriate fields.
CM/CMM Backup/Restore File Server	The file server that is used to store the backup data during the upgrade. The field applies only for Communication Manager Release 5.2.1 upgrade. On the Backup Configuration page, if you select **Ready For Upgrade**, the system displays the file server address where the backup data is saved.
Authentication File	The link to authenticate the file. The field applies only for Communication Manager Release 5.2.1 upgrade.
WebLM Server IP Address	The IP address of the WebLM server. The field applies only for Communication Manager Release 5.2.1 upgrade.
Vlan Id	The IP address of the VLAN circuit pack. **Note:** The system displays the field only when you select **Flash Drive** in the **Upgrade Source** field.
Dom0 Hostname	The host name of the Domain-0 virtual machine. **Note:** The system displays the field only when you select **Flash Drive** in the **Upgrade Source** field.
Cdom Hostname	The host name of the System Platform console domain virtual machine. **Note:** The system displays the field only when you select **Flash Drive** in the **Upgrade Source** field.

Table continues…

Field	Description
Services Hostname	The host name of the Services virtual machine. **Note:** The system displays the field only when you select **Flash Drive** in the **Upgrade Source** field.
SP Root Password	The password for the System Platform root user. **Note:** The system displays the field only when you select **Flash Drive** in the **Upgrade Source** field.
Ldap Root Password	The password for the root user of the LDAP directory server. **Note:** The system displays the field only when you select **Flash Drive** in the **Upgrade Source** field.
Communication Manager IP Address	The Communication Manager IP address. The Communication Manager IP address must be the same as the Communication Manager system that you selected for upgrade. The field applies only for Communication Manager Release 5.2.1 upgrade.
Upgrade To	The device to which you want to upgrade.
Branch Session Manager	The Branch Session Manager available for the upgrade. The Branch Session Manager IP address must be the same that is mentioned in the **EPW** file.
Branch Session Manager Login	The Branch Session Manager login.
Branch Session Manager Password	The Branch Session Manager password. The password must not exceed nine letters.
Branch Session Manager Enrollment Password	The Branch Session Manager enrollment password. The password must not exceed nine letters.
Utility Server	The Utility Services available for the upgrade.
Communication Manager	The available Communication Manager.
System Platform Upgrade Version	The available System Platform upgrade version for the upgrade.
System Platform Update Version	The available System Platform update version for the upgrade.

Table continues…

Field	Description
Utility Server IP Address	The Utility Services IP address. The IP address must be the same as the IP address mentioned in the EPW file. The field applies only for Communication Manager Release 5.2.1 upgrade.
Auto Commit Upgrade	The field to specify if a backup of the current release is available. The options are: • **Yes**: If you do not require a backup of the current release. Rollback is not possible if you select Yes. • **No**: If you require a backup of the current release. You can perform a rollback operation if you select No.
CM VM Kernel,Platform Patching	The kernel patch or platform patch for the Communication Manager virtual machine. ✱ **Note:** • If selected, the kernel and platform patching must be performed implicitly on the Communication Manager virtual machine. • If not selected, the kernel and platform patching must be performed manually on the Communication Manager virtual machine. For more information, see *Deploying Avaya Aura® Communication Manager on System Platform*.
CM VM Platform Patch	The platform patch for the Communication Manager virtual machine.
CM VM Kernel Patch	The kernel patch for the Communication Manager virtual machine.
Override Recommended Failure	The option that specifies whether the system must override any recommended preupgrade check failure that occurs during the element upgrade. When you select this option, the system continues with upgrade even when a recommended preupgrade check fails. ✱ **Note:** Select **Override Recommended Failure** if one or more of the earlier recommended preupgrade checks have failed.

Update Operations

Name	Description
CM Service Pack	The Communication Manager service pack version to which you are entitled.
SES Service Pack	The SES service pack update to which you are entitled.
Kernel Update	The kernel update to which you are entitled.
Platform/Security Update	The platform or security update to which you are entitled.

License Authentication Operations

Name	Description
Import License File	The license file that you must select for the upgrade.
Import Authentication File	The authentication file that you must select for the upgrade.

Button	Description
Save Configuration	To save the configuration. You can save the configuration details for multiple Communication Manager devices before upgrading.
Clear Configuration	To clear the configuration that you have chosen.
Proceed to Job Summary	To view the summary of the configuration that you have chosen.
Commit	To perform the upgrade operation.
Cancel	To cancel your current operation, and go to the previous page.

Upgrading Communication Manager 5.2.1 to Release 6.3.100 on a different server

Before you begin

- Install the latest System Platform release and the latest service pack on the supported server.

  For more information, see Hardware requirement checks during preupgrade check.

- The recommended System Platform must be on the same subnetwork as Communication Manager 5.2.1.
- Record the server data for Communication Manager 5.2.1 in the worksheet for upgrading Communication Manager to simplex and embedded templates.

  For more information, see Recording the configuration screens, and Worksheet for upgrading Communication Manager to simplex and embedded templates, see *Upgrading to Avaya Aura® Communication Manager*.

  The system backs up most of the server data and restores the data after the upgrade. You must verify and complete the configuration after the upgrade is complete.

- Create the authorization file for System Platform, and store the file in **My Computer**.

  For more information, contact the Avaya support team.

- Create the EPW file for the Communication Manager selected for upgrade, and provide all credentials to the EPW file including System Platform details. Store the EPW file on the HTTP or HTTPS server.

  For more information, contact the Avaya support team.

- Get the WebLM server IP address that is mandatory for licensing.

  For more information, contact the Avaya support team.

- Get the inventory for Communication Manager 5.2.1.

  The get inventory operation ensures that the system reflects the exact state of the device in Software Inventory.

- Analyze the software.
- Download the related firmware for the Communication Manager upgrade.
- Run the preupgrade check.

About this task

Use the procedure to upgrade Communication Manager 5.2.1 to Release 6.3.100 on a different server.

Important:

For a duplex, first upgrade the standby Communication Manager and then the active Communication Manager.

When you select a Communication Manager on which Communication Manager Messaging is enabled , the Communication Manager Messaging device updates to the latest version after the upgrade.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select the Communication Manager 5.2.1 device that you want to upgrade.
6. **(Optional)** For a semiautomated upgrade, perform the following:
   a. Create a backup.
   b. To upgrade on a different server, clear the **Ready for Upgrade** check box.

   For more information, see Backing up Communication Manager or Communication Manager Messaging on page 1258
7. Click **Upgrade**.

8. On the CM Upgrade Configuration page, perform the following:
    1. Select the Communication Manager 5.2.1 device to which you want to upgrade.
    2. Provide the HTTP or HTTPS path for the EPW file.
    3. Browse and select the authentication file.
    4. In the Upgrade Operations section, complete the fields.
        1. For semi automated upgrade, in the **Upgrade Source** field, select **Software Library**.
        2. In the **Available System Platform** field, select the System Platform device that you manually installed and added to System Manager.

            For more information, see Add Communication Manager field descriptions on page 876.
        3. In the **Select Template** field, select a template.

        For more information, see CM Upgrade Configuration field descriptions on page 1260.
    5. Click **Save the configuration**.
9. In the Job Schedule section, perform one of the following:
    - To upgrade the device, click **Now**.
    - To upgrade the device at a later time, click **Later**.
10. Click **Upgrade**.

    The Software Inventory page displays the status of the upgrade in **Status**.
11. To view the logs and the description of the upgrade operation, click the status of the Communication Manager device.

Next steps

- Verify that the upgrade is successful.
- Validate that the Communication Manager 5.2.1 server data that is restored on the new system is complete.

For more information, see Verifying the upgrade on page 1248.

Related links

Analyze software on page 1237
CM Upgrade Configuration field descriptions on page 1260
Analyzing the software on page 1238
Getting inventory on page 1236
Creating a software library on page 1160
Performing a preupgrade check on page 1240
Preupgrade checks on page 1241
Sample scenario to upgrade Communication Manager Release 5.2.1 to 6.3.100 on a different server on page 1269
Hardware requirement checks during a preupgrade check on page 1243

Communication Manager 5.2.1 upgrade checklist on page 1257
Device list on page 835

Sample scenario to upgrade Communication Manager Release 5.2.1 to 6.3.100 on a different server

To upgrade Communication Manager Release 5.2.1 to 6.3.100 on a different server, do the following:

1. Perform the Preupgrade tasks on page 1269.
2. Perform the Upgrading Communication Manager 5.2.1 to 6.3.100 on page 1270.
3. Perform Verifying the upgrade on page 1248.

Preupgrade tasks

No.	Task	References	✔
1.	Discover the devices that you want to upgrade by enabling SNMP or adding from Discovery on the Manage Elements page.	Discovering elements on page 834	
2.	Configure user settings.	Configuring user settings on page 1148	
3.	Create a remote software library.	Creating a software library on page 1160	
4.	Install the latest System Platform software on the supported server. Visit the Avaya support site for the latest availabe software.	Hardware requirement checks during preupgrade check on page 1243	
5.	Record the server data for Communication Manager 5.2.1 in the worksheet for upgrading Communication Manager to simplex and embedded templates.	For more information about the following, see *Upgrading Avaya Aura® Communication Manager*: • Recording the configuration screens. • Worksheet for upgrading Communication Manager to simplex and embedded templates.	
6.	Create the authorization file for System Platform, and store the file in **My Computer**.	For more information, contact the Avaya support team.	
7.	Create a new EPW file for the Communication Manager instance selected for upgrade, and provide all credentials to the EPW file including System Platform details. Store the EPW file on the HTTP or HTTPS server.	For more information, contact the Avaya support team.	

Table continues…

No.	Task	References	✔
8.	Get the WebLM server IP address for licensing.	For more information, contact the Avaya support team.	
9.	Get the inventory for Communication Manager 5.2.1.	Get inventory software inventory on page 1236	
10.	Analyze the software.	Analyzing the software for software inventory on page 1238	
11.	Download the related firmware for the Communication Manager upgrade.	Downloading the software for software inventory on page 1238	
12.	Perform the preupgrade check.	Performing the preupgrade check on page 1240	

Upgrading Communication Manager 5.2.1 to 6.3.100

Before you begin

Complete the preupgrade tasks.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select the Communication Manager 5.2.1 device that you want to upgrade.
6. Click **Upgrade**.
7. On the CM Upgrade Configuration page, perform the following:
    a. Provide the HTTP or HTTPS path for the EPW file.
    b. Browse and select the authentication file on **My Computer** in the field required.
    c. In the Upgrade Operations section, complete the fields.

       For more information, see CM Upgrade Configuration field description.
    d. Click **Save the configuration**.
    e. In the **Job Schedule** section, click **Now**.
8. Click **Upgrade**.

   The Software Inventory page displays the status of the upgrade in **Status**.
9. To view the logs and the upgrade details, click the status of the Communication Manager device.

Server support for Communication Manager Release 5.2.1 to 6.3.100 upgrades

Existing CM 5.2.1 server	Possible CM 6.3.100 templates during software and hardware upgrades	Servers compatible for upgrade to CM 6.3.100
HP DL360 G7	CM_Simplex CM_Duplex CM_SurvRemote	Yes
HP DL360 G8	CM_Simplex CM_Duplex CM_SurvRemote	Yes
S8300D	CM_onlyEmbed CM_SurvRemoteEmbed	Yes
S8510	CM_Simplex CM_SurvRemote	Yes
S8800	CM_Simplex CM_Duplex CM_SurvRemote	Yes
S8300C	CM_Simplex CM_Duplex CM_SurvRemote	No
S8300B	CM_Simplex CM_Duplex CM_SurvRemote	No
S8400	CM_Simplex	No
S8400B	CM_Simplex	No
S8500	CM_Simplex CM_SurvRemote	No
S8500A	CM_Simplex CM_SurvRemote	No
S8500B	CM_Simplex CM_SurvRemote	No
S8500C	CM_Simplex	No

Table continues…

Existing CM 5.2.1 server	Possible CM 6.3.100 templates during software and hardware upgrades	Servers compatible for upgrade to CM 6.3.100
	CM_SurvRemote	
S8710	CM_Duplex CM_SurvRemote	No
S8720	CM_Duplex CM_SurvRemote	No
S8730	CM_Duplex CM_SurvRemote	No

Upgrading TN boards

Before you begin

For TN boards, perform the following:

- Get the inventory.
- Analyze the firmware.
- Download the firmware.

You cannot upgrade the TN board if the TN board:

- Is in the nonupgradable ℹ **State**
- Has a Virtual IP address

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select the Communication Manager devices that you want to upgrade.
6. Click **Upgrade**.
7. On the CM Upgrade Configuration page, click the TN Boards tab.
8. Select the TN board that you want to upgrade.
9. Download the upgrade file to the software library.

   The state of the TN board changes to ⚠.
10. Click **Upgrade**.

    The system displays the status of the upgrade operation as RUNNING.

11. Click the status to view the description of the upgrade operation.

Related links

Analyze software on page 1237

Upgrading media gateways and media modules

Before you begin

- Obtain the inventory for the media gateways.
- Analyze the software.
- Download the software.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select the Communication Manager devices that you want to upgrade.
6. Click **Upgrade**.
7. On the CM Upgrade Configuration page, click the Gateway tab.
8. Download the upgrade file to the software library.

   The **Upgrade** is enabled only if the **State** of the media gateway state changes to ready to update ⚠.

   The device state changes to ready to update ⚠.
9. Select the media gateway that you want to upgrade.
10. Click **Upgrade**.
11. On the Gateway Upgrade Configuration page, click **Now**.

    The system displays the status of the upgrade job as RUNNING.
12. Click the status to view the description of the upgrade job.

Related links

Protocol matrix for upgrades on page 1277

Downloading a file

About this task

Using **Download Manager**, you can download the software releases you are entitled from Avaya PLDS, or from an alternate source. You can upload a file from your local system to the software library using **Download Manager**.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Download Manager**.
3. From **Select Software/Hardware Types**, select the firmware you want to download.

   You can choose either **Tree View** or **List View** to view the software, hardware types.
4. Click **Show Files**.

   The system displays the upgrade files available for download. The system displays all the files for the category you selected. You can select only those files which you are entitled to.
5. Select a **Source** from where you want to download a software or firmware.
6. Select the files you want to download, and click **Download**.

   The system displays the End User License Agreement page.
7. On the Library and Protocol Selection page, select a **Library** where you want to download the software or firmware.
8. On the Library and Protocol Selection page, select a **Protocol** through which you want to upload the downloaded software to the software library from System Manager. This scenario is applicable when the software library is on an external server.
9. Select the **I Agree** checkbox to download the software.
10. Perform one of the following actions:
    - Click **Now** to download the software immediately.
    - Click **Schedule** to schedule the download at a specified time.

    To view the status of the download, click **Services** > **Scheduler** on the System Manager console.

    To view the progress of the download, refresh the **File Download Status** section on the Download Manager page.

    Note:

    For IP Office upgrades, you must download the file to a remote HTTP software library. You can schedule an upgrade job only for a software library configured with an http URL.

    The IP Office executable files are downloaded to the local System Manager repository and are available in the `$ABG_HOME/tools` folder.

Upgrading Communication Manager 5.x

Upgrading Communication Manager 5.x

Before you begin

Get the inventory for Communication Manager.

Analyze the software.

Download the software.

About this task

Use the procedure to upgrade Communication Manager 5.x to 5.2.1.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select the Communication Manager 5.x device that you want to upgrade.
6. Click **Upgrade**.
7. On the CM Upgrade Configuration page, perform the following:
    a. Select the Communication Manager 5.2.1 device to which you want to upgrade.
    b. Provide the HTTP or HTTPS path for the EPW file.
    c. Browse and select the authentication file.
    d. In the Upgrade Operations section, complete the fields.
        a. For semi automated upgrade, in the **Upgrade Source** field, select **Software Library**.
        b. In the **Select Template** field, select a template.

    For more information, see CM Upgrade Configuration field descriptions on page 1260.

    e. Click **Save the configuration**.
8. In the Job Schedule section, click **Now** or **Later**.
9. Click **Upgrade**.

    The Software Inventory page displays the status of the upgrade in **Status**.
10. To view the logs and the description of the upgrade operation, click the status of the Communication Manager device.

Related links

Analyze software on page 1237

Updating Communication Manager

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. On the Software Inventory page, select the Communication Manager you want to update.
6. Click **Upgrade**.
7. On the CM Upgrade Configuration page, select **Update** and fill in the required fields.
8. From the table, select the file you want to activate, deactivate, or remove.
9. In the Job Schedule section, click **Now** or **Later**.
10. Click **Upgrade**.

    The Software Inventory page displays the status of the update in **Status**.
11. To view the logs and the description of the uppdate, click the status of the Communication Manager device.

Related links

Analyze software on page 1237

Updating the SAMP/MPC firmware

Before you begin

- Add a Communication Manager system with the SAMP/MPC firmware to the System Manager inventory.
- Obtain the inventory and perform the analyze operation for Communication Manager.
- Download the appropriate SAMP/MPC firmware to the software library.

About this task

You can only update SAMP/MPC firmware through the **Install (Copy and Unpack)/Update SAMP, MPC** option.

Note:

The procedure applies only to upgrading Communication Manager Release 5.x to 5.2.1.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Release Selection**.
3. In the **Select Upgrade Version** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the left navigation pane, click **Upgrade Management** > **Software Inventory**.
5. Click the Communication Manager that you want to update.
6. Perform the analyze operation.
7. Click **Upgrade**.
8. On the Patch Configuration page, click **Update**, and complete required fields.
9. Select the appropriate SAMP/MPC firmware from the table.
10. Click **Now** or **Schedule**.

Protocol matrix for upgrades

Table 11: Protocols supported by devices in Software Management

Product	Supported protocols	Notes
G350	FTP, USB	Media modules associated with the gateway support the same protocols as the gateway.
G700	FTP	Media modules associated with the gateway support the same protocols as the gateway.
G430	FTP, SCP (gateway versions later than 31.17.XX), USB	G430 supports the SCP protocol only if the current versions of the gateway are 31.17.X and later.
G450	FTP, SCP (gateway versions later than 31.17.XX), USB	G450 supports the SCP protocol only if the current versions of the gateway are 31.17.X and later.
G250	FTP, USB	Media modules associated with the gateway support the same protocols as the gateway.
TN Boards	SCP	TN Boards support only the SCP protocol.
Communication Manager	HTTP, HTTPS, SCP, FTP, SFTP	When you perform upgrades, use the protocols to copy the Communication Manager release files from the remote server.
System Manager	HTTP, HTTPS, SCP, FTP, SFTP	When you perform upgrades, use the protocols to copy the System Manager release files from the remote server.

When you perform gateway upgrades by using the Library Server Details for **Local Survivable Processor(LSP)**, the system supports only SCP and FTP protocols.

Related links

Analyze software on page 1237

Chapter 26: Communication Manager Notify Sync

Overview of the CM notify sync feature

When you perform an administrative task from System Manager, the local database is immediately updated. If you execute the action through a Communication Manager SAT screen, or through a phone, or from any of the several management applications such as Site Administration, MultiSite Administration, Native Configuration Manager, or MyPhone, it is not immediately reflected in System Manager. This scenario creates an out-of-sync condition between the Communication Manager and System Manager.

The CM notify sync feature provides near-real time notifications from Communication Manager to System Manager whenever you execute certain tasks against a Communication Manager object from a system other than System Manager. The CM notify sync feature also provides notifications whenever the tti-m, tti-s, psa-u, psa-a, or psa-d logins perform their predefined actions against a Communication Manager station object.

After a Communication Manager sends notifications to System Manager, System Manager discovers the complete details of the task you preformed. The transmission of notifications in the form of event messages from Communication Manager to System Manager is based on the Communication Manager's existing rsyslog capability. The Communication Manager's rsyslog uses UDP or TCP to send event messages from the originating Communication Manager to the System Manager.

Note:

The existing daily default synchronization and any other scheduled synchronization operations are unaffected by the CM notify sync feature.

You need Communication Manager with version 6.2 or above for to enable the CM notify sync feature. System Manager 6.3 supports both one-way and two-way TLS.

Enabling the CM notify sync feature

You can enable and disable the CM notify sync feature on a per Communication Manager basis. You can activate the CM notify sync feature from a new System Manager using **Manage Elements**. Select Communication Manager 6.2 or a higher version, and select **Enable Notifications** in the Attributes section.

As a system administrator, you must specify the IPs of one or two System Managers to which the Communication Managers send the event data using rsyslog. If your configuration includes two

System Managers, the standby System Manager ignores the syslog messages until it becomes active.

Configuring one-way and two-way TLS

You must configure either one-way or two-way TLS for the CM notify sync feature.

To configure one-way TLS, perform the following actions:

- Downloading the certificate on page 1280
- Downloading the pem file to on page 1281
- Adding a trusted certificate to on page 1282
- Configuring notify sync on on page 1283

> **Note:**
>
> You must add the Communication Manager in **Inventory** > **Manage Elements** before enabling the notify sync feature on the Communication Manager. If you add the Communication Manager in the System Manager **Inventory**, and enable notify sync before adding the certificate, add the trusted certificate to the Communication Manager. Then edit the Communication Manager through **Manage Elements**, and re-enable the Communication Manager notify sync feature.

To configure two-way TLS, perform the following actions:

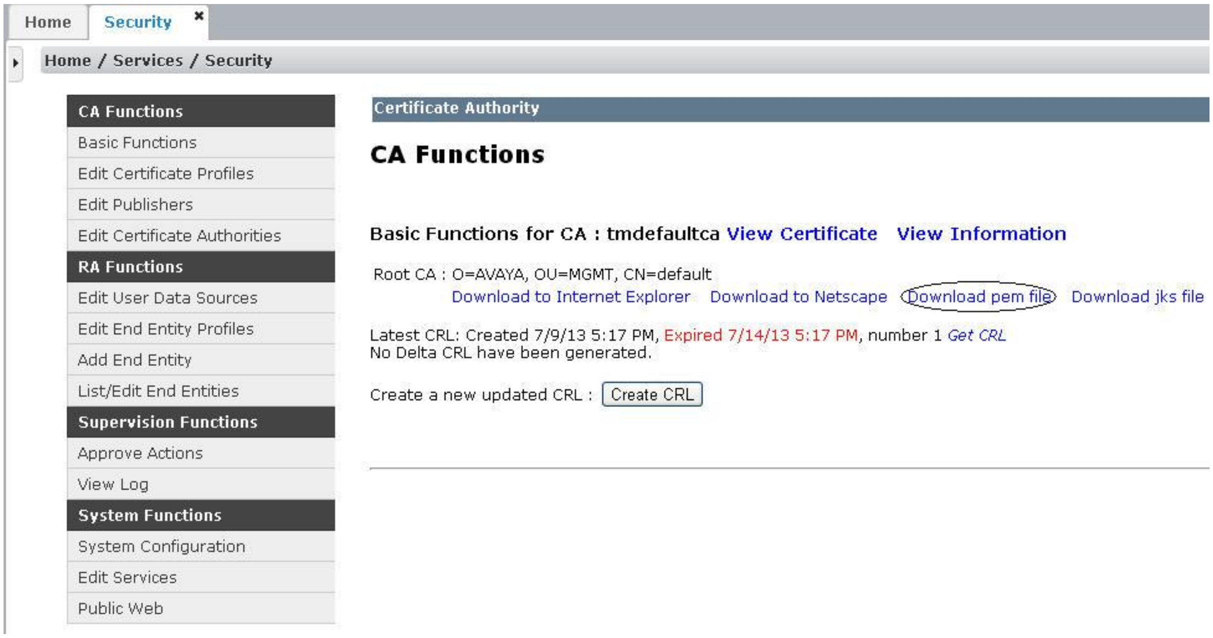
- Adding the certificate to the trust on page 1285
- Enabling two-way TLS in on page 1286

Downloading the System Manager certificate

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.

3. On the CA Functions page, click **Download pem file**.



CA Functions

Basic Functions for CA : tmdefaultca View Certificate View Information

Root CA : O=AVAYA, OU=MGMT, CN=default
Download to Internet Explorer Download to Netscape Download pem file Download jks file

Latest CRL: Created 7/9/13 5:17 PM, Expired 7/14/13 5:17 PM, number 1 *Get CRL*
No Delta CRL have been generated.

Create a new updated CRL : Create CRL

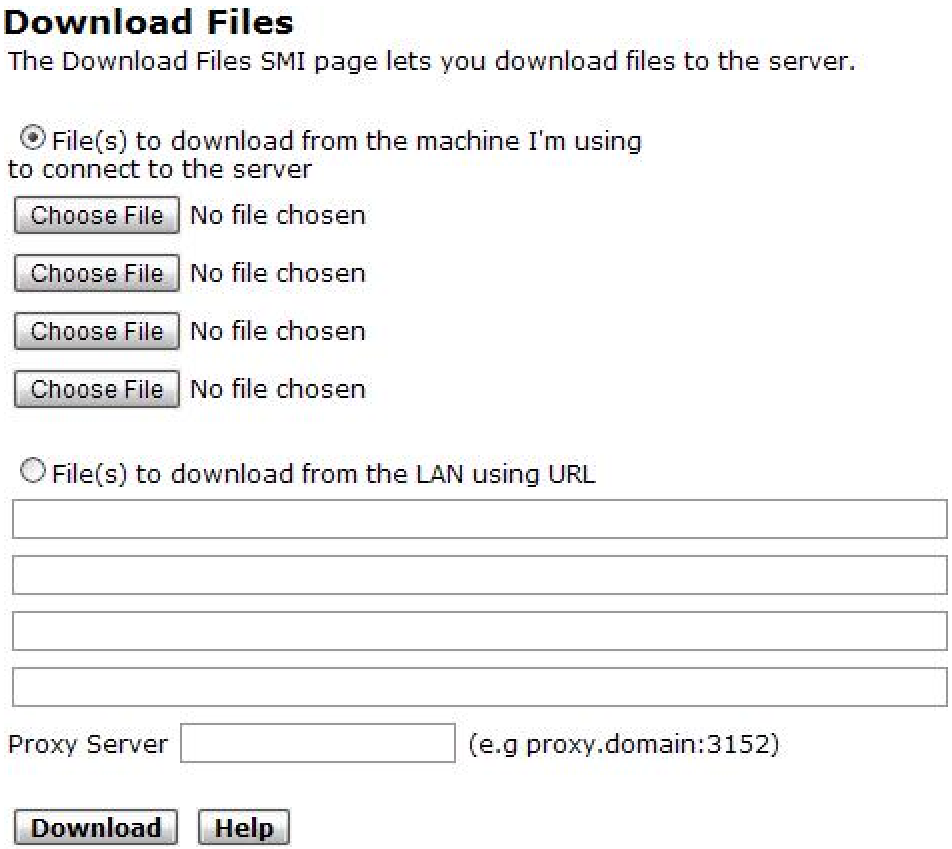
4. After you download the .pem file, save the file to your system.

Downloading the pem file to Communication Manager

Procedure

1. Log in to a Communication Manager web console.
2. Click **Administrator** > **Server (Maintenance)**.
3. In the left navigation pane, click **Miscellaneous** > **Download Files**.
4. Select the **Files to download from the machine I'm using to connect to the server** option.
5. Click **Choose File** to browse to the downloaded certificate.
6. Click **Download**.

   The system displays the Download Files Results page with a message that the download is successful.


Download Files

The Download Files SMI page lets you download files to the server.

● File(s) to download from the machine I'm using to connect to the server

Choose File No file chosen

Choose File No file chosen

Choose File No file chosen

Choose File No file chosen

○ File(s) to download from the LAN using URL

Proxy Server (e.g proxy.domain:3152)

Adding a trusted certificate to Communication Manager

Procedure

1. Log in to a Communication Manager Web console.
2. Click **Administration** > **Server (Maintenance)**
3. Click **Security** > **Trusted Certificates**.
4. Click **Add**.
5. On the Trusted Certificate – Add page enter the file name for the certificate you want to add. The certificate must be a .pem file. The name of the certificate must be the same as the one used in the ***Downloading the pem file to Communication Manager*** section.
6. To validate the certificate, click **Open**.

   After a successful validation, the Trusted Certificates – Add page displays the **issued-to**, **issued by**, and **expiration date** information for the certificate you are adding.

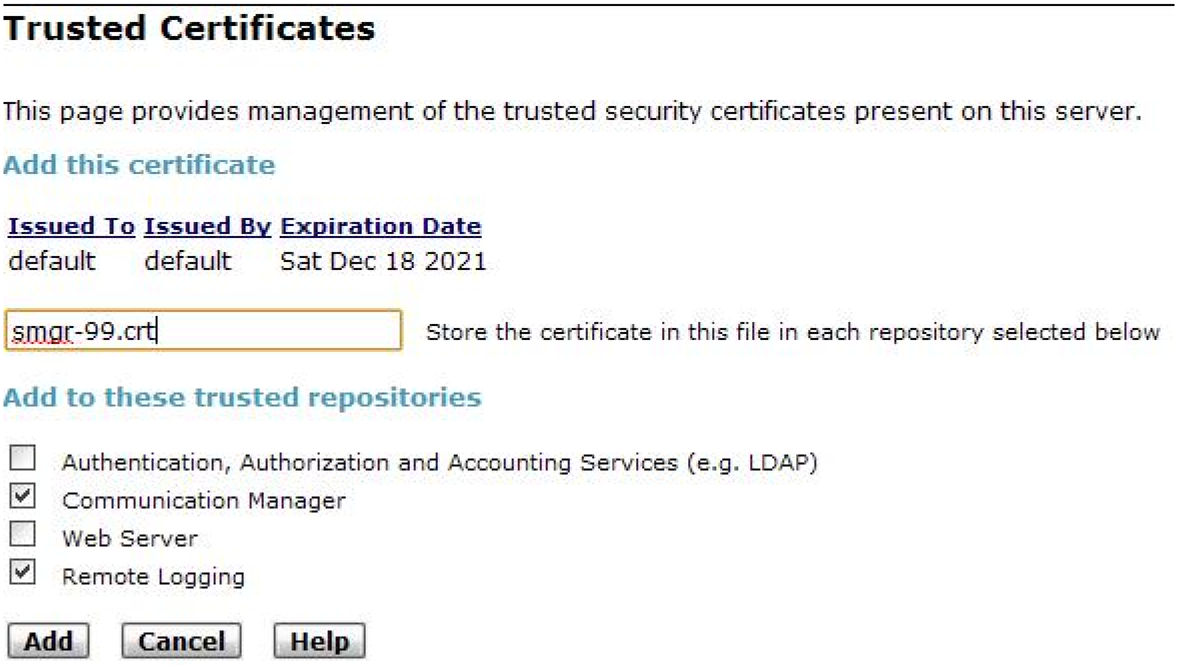
Note:

The system displays an error message if the certificate is not a valid certificate.

7. Select the **Communication Manager**, **Remote Logging** repositories from the list of trusted repositories.
8. Click **Add**.

   The system verifies the following:

   - The certificate name has a .crt extension. If the certificate name has a different extension, the system deletes it and replaces it with a .crt extension.
   - The certificate name is unique and does not already exist.
   - The certificate is not a duplicate certificate with a new name.



Trusted Certificates

This page provides management of the trusted security certificates present on this server.

Add this certificate

Issued To	Issued By	Expiration Date
default	default	Sat Dec 18 2021

smgr-99.crt Store the certificate in this file in each repository selected below

Add to these trusted repositories

☐ Authentication, Authorization and Accounting Services (e.g. LDAP)
☑ Communication Manager
☐ Web Server
☑ Remote Logging

Configuring notify sync on Communication Manager

About this task

The `/etc/syslog.conf` file contains the following two IPTCM entries:

```
#iptcm_log local6.*
$DefaultNetstreamDriverCAFile /etc/opt/ecs/certs/rsyslog/CA/all-ca.crt
$ActionSendStreamDriver gtls
$ActionSendStreamDriverMode 1
$ActionSendStreamDriverAuthMode x509/certvalid
local6.*   @@[148.147.162.35]:9000
```

```
$ActionSendStreamDriver gtls
$ActionSendStreamDriverMode 1
$ActionSendStreamDriverAuthMode x509/certvalid
local6.*   @@[148.147.162.36]:9000
```

The first local6 entry contains the primary System Manager IP address. For example, 148.147.162.35, and the second local6 entry contains the secondary System Manager IP address. For example, 148.147.162.36.

Before you begin

- Register both the IP addresses, Server 1 IP and Server 2 IP, of the duplex Communication Manager pair for System Manager to handle the notify sync messages.
- In the **Alternate IP Address** field, edit the existing Communication Manager and add the Server 2 IP address.

Note:

The virtual IP address cannot be used on Communication Manager systems in a duplex configuration.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Select a Communication Manager with version 6.2 or later.
4. In the Attributes section, select **Enable Notifications**.

   When you enable the notify sync feature, the system sends a register command to Communication Manager for registering the IP address of System Manager as a syslog server. After you enable notify sync, all administrative changes made on Communication Manager are sent to System Manager asynchronously.
5. To verify that the notify sync feature is successfully enabled, perform the following:
   a. Open ssh and log in as `sroot`.
   b. Type `cmSyslogConfig --iptcmquery`.

   The system displays the details of the registration.
6. If the notify sync feature does not function and if Geographic Redundancy is set up on System Manager, complete the following:
   a. Open the `/etc/syslog.conf` file.
   b. Remove the following secondary System Manager related entries from the file:

   ```
   $ActionSendStreamDriver gtls
   $ActionSendStreamDriverMode 1
   $ActionSendStreamDriverAuthMode x509/certvalid
   local6.*   @@[148.147.162.36]:9000
   ```

7. **(Optional)** If the primary System Manager becomes nonoperational, and you want to manage Communication Manager by using the secondary System Manager, complete the following:

   a. In the `/etc/syslog.conf` file, replace the primary System Manager IP address with secondary System Manager IP address.

   ```
   #iptcm_log local6.*
   $DefaultNetstreamDriverCAFile /etc/opt/ecs/certs/rsyslog/CA/all-ca.crt
   $ActionSendStreamDriver gtls
   $ActionSendStreamDriverMode 1
   $ActionSendStreamDriverAuthMode x509/certvalid
   local6.*   @@[148.147.162.36]:9000
   ```

   b. Remove the following secondary System Manager related entries from the file:

   ```
   $ActionSendStreamDriver gtls
   $ActionSendStreamDriverMode 1
   $ActionSendStreamDriverAuthMode x509/certvalid
   local6.*   @@[148.147.162.35]:9000
   ```

8. To restart the rsyslog service on Communication Manager, type `service rsyslog restart`.

   Notify sync becomes operational.

Configure two-way TLS

You must configure either one-way or two-way TLS to enable the CM notification service. To configure two-way TLS, perform the following procedures:

- Downloading the certificate on page 1280
- Downloading the pem file to on page 1281
- Adding a trusted certificate to on page 1282
- Configuring notify sync on on page 1283
- Adding the certificate to the trust on page 1285
- Enabling two-way TLS in on page 1286

Adding the Communication Manager certificate to the System Manager trust

Before you begin

1. Download the System Manager certificate.
2. Download the pem file to Communication Manager.

3. Add a trusted certificate to the Communication Manager.
4. Configure notify sync on the Communication Manager.

Procedure

1. Download the Communication Manager certificate to your computer from `/etc/opt/ecs/certs/rsyslog/CA/sip_product_root.crt`.
2. Login to the System Manager Web Console.
3. On the System Manager web console, click **Services** > **Inventory**.
4. In the left navigation pane, click **Manage Elements**.
5. Select **System Manager** from the elements list.
6. Click **More Options** > **Configure Trusted Certificates**.
7. Click **Add**.
8. In the **Select Store Type to add trusted certificate** field, select **TM_INBOUND_TLS** as the store type.
9. Click **Import from file**.
10. Click **Choose File**.
11. Browse to the certificate that you have downloaded, and click **Open**.
12. Click **Retrieve certificate** to check the contents of the certificate.
13. Review the certificate details, and click **Commit**.

Enabling two-way TLS in System Manager

Before you begin

Add the Communication Manager certificate to the System Manager trust.

About this task

Perform the following procedure during off peak hours or during a planned outage since you have to restart the JBoss service after enabling two-way TLS.

Procedure

1. Login to the System Manager CLI using the admin credentials.
2. Browse to the `$IPTCM_HOME/config/workflow` folder and open the `notify-sync.properties` file for editing.
3. In the iptcm.authtype.twowaytls property, change the value to **iptcm.authtype.twowaytls=true**.

   The default value is **iptcm.authtype.twowaytls=false**.

4. Restart the System Manager JBoss service using the **`service jboss restart`** command.

Chapter 27: Changing the IP address and FQDN in System Manager

Verifying the deployment of extension packs

Before you begin

- Install System Manager.
- Log on to System Manager web console as admin.

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. Click **Extension Packs**.
3. In the **Extension pack data** section, verify that the status of all extension pack data is `success(confirmed)`.
4. Create a remote backup using the **Services** > **Backup and Restore** service in System Manager.

Related links

Changing the IP address or FQDN in System Manager on page 1290
Changing the network parameters for an ESXi host on page 1181

Impact of change in FQDN and IP address on the Geographic Redundancy feature

In a Geographic Redundancy configuration, the system automatically communicates any change in the IP address or FQDN of the primary or the secondary System Manager to the elements.

Impact of the change in IP address or FQDN on the primary System Manager

- The system changes the identity certificates of the primary System Manager. Therefore, reinitialize trust on the primary System Manager.
- The secondary System Manager does not require any trust changes.
- System Manager notifies the change to the elements. If the event notification fails due to temporary disconnect, the system sends the event when the elements resume the network connectivity.

Impact of the change in IP address or FQDN on the secondary System Manager in the active and stand-by mode

- The system changes the identity certificates of the secondary System Manager. Therefore, reinitialize trust on the secondary System Manager.
- The primary System Manager does not require any trust changes.
- System Manager notifies the change to the elements. If the event notification fails due to temporary disconnect, the system sends the event when the elements resume the network connectivity.

Impact of the change in IP address or FQDN during a network split

When the split network heals, run the IPFQDN pair.

SSO login to remote machine fails

For System Manager deployments that involve remote machines such as CS 1000 Servers and solutions based on the System Manager Single Sign On (SSO) client, the Web-based Single Sign On between System Manager and the remote machine fails.

During the data migration or IP-FQDN change, the system does not import the LDAP attribute that contains the SSO cookie domain value back to the directory. Therefore, the System Manager SSO login to the remote machine fails. Enable SSO after the data migration or the IP-FQDN change.

Related links

Reimporting the SSO cookie domain value on page 1289

Reimporting the SSO cookie domain value

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Security** > **Policies**.
3. In the section **Single Sign-on Cookie Domain** section, click **Edit**.
4. In the **Single Sign-on Cookie Domain** field, select an appropriate domain based on the FQDN of the servers that you deployed.
5. Click **Save**.

Changing the IP address or FQDN in System Manager

Before you begin

Verify that the deployment of the extension packs are successful.

About this task

After you install System Manager, you can change the IP address, host name, or the general network settings of the system running System Manager.

Procedure

1. On the System Manager we console, click **Services** > **Solution Deployment Manager**.
2. On the left navigation pane, click **VM Management**.
3. Change the hostname and FQDN as appropriate.

   For more information, see Changing the network parameters.

Related links

Verifying the deployment of extension packs on page 1288
Changing the network parameters for an ESXi host on page 1181

Changing IP address or FQDN of managed elements on System Manager

About this task

Use the procedure to change the IP address or FQDN of Communication Manager.

For instructions to change the IP address or FQDN of managed elements, see the appropriate guide. For example, for Session Manager, see *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Select the registered element from the table.
4. Click **Edit**.
5. In the **General** section, in the **Node** field, update the value.
6. In the **Access Profile** section, in the **Host** field update the value.

Changing the System Manager IP address in managed elements

About this task

When the IP address or FQDN of System Manager changes:

- If the managed elements use JNDI lookup to communicate with System Manager, the elements must point to the new System Manager IP address.
- The adopting element must recreate the License Manager object with the new IP address.
- Data replication on managed elements, such as Session Manager and Presence can have an impact because both elements use the System Manager host name to communicate with System Manager.

Therefore, you must change the references of System Manager IP address and FQDN on the managed elements, such as Session Manager, Presence, and AES so the elements can continue to connect and communicate with System Manager.

Procedure

To change the IP address or FQDN of System Manager on the managed elements, see the documentation of the element.

For example, to change the IP address or FQDN of System Manager on Session Manager, see *Maintaining and Troubleshooting Avaya Aura® Session Manager* on the Avaya support site.

Changing the IP address and FQDN on the System Manager servers in Geographic Redundancy

Change in IP address and FQDN on the primary and secondary System Manager servers

The sections provide various scenarios for changing the IP address and FQDN on System Manager configured with Geographic Redundancy. The section also provides the procedure to run the pair IP-FQDN script.

Ensure that the IP address and FQDN meets the following requirements:

- For the IP address change: Map the new IP address of the FQDN of System Manager in DNS.

  Ensure that the new IP address is unique.
- For the FQDN change: Map the new FQDN to the IP address of System Manager in DNS.

  Ensure that the new FQDN is unique and different from the virtual FQDN.

- For the IP address and FQDN change: Ensure that the new IP address and FQDN is valid and mapped in DNS.

Note:

Entering an invalid IP address and FQDN might affect the behavior of the system.

Changing the IP address and FQDN on the primary System Manager when the secondary is in the standby or active mode

Procedure

1. Disable the Geographic Redundancy replication if not already disabled.
2. On the primary System Manager server, change the IP address or FQDN or both. For instructions, see Changing the IP address and FQDN in System Manager.

   Wait for about 30–40 minutes before you perform the next step.
3. Log on to the web console of the primary System Manager server, and verify that System Manager is up and running.
4. If System Manager is running on System Platform, log in to the CLI of the secondary System Manager server as `root` and perform one of the following:
   - If you changed both the IP address and FQDN, type the following:

     ```
     #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old
     IP of the primary server> -NEWIP <New IP of the primary server> -
     OLDFQDN <Old FQDN of the primary server> -NEWFQDN <New FQDN of the
     primary server>
     ```
   - If you changed the IP address, type the following:

     ```
     #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old
     IP of the primary server> -NEWIP <New IP of the primary server>
     ```
   - If you changed FQDN, type the following:

     ```
     #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDFQDN
     <Old FQDN of the primary server> -NEWFQDN <New FQDN of the primary
     server>
     ```
5. On the secondary System Manager server, verify that the Geographic Redundancy page displays the new IP address or FQDN of the primary System Manager server.
6. Enable the Geographic Redundancy replication.

Related links

Enabling the Geographic Redundancy replication on page 75
Disabling the Geographic Redundancy replication on page 76
Changing the IP address or FQDN in System Manager on page 1290

Changing the IP address and FQDN on the primary System Manager server when the secondary is nonoperational

Procedure

1. Disable the Geographic Redundancy replication if not already disabled.
2. On the primary System Manager server, change the IP address or FQDN or both. For instructions, see Changing the IP address and FQDN in System Manager.

   Wait for about 30–40 minutes before you perform the next step.
3. Log on to the web console of the primary System Manager server, and verify that System Manager is up and running.
4. Bring the secondary System Manager server to operation.
5. If System Manager is running on System Platform, log in to the CLI of the secondary System Manager server as `root` and perform one of the following:
   - If you changed both the IP address and FQDN, type the following:

     ```
     #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old
     IP of the primary server> -NEWIP <New IP of the primary server> -
     OLDFQDN <Old FQDN of the primary server> -NEWFQDN <New FQDN of the
     primary server>
     ```
   - If you changed the IP address, type the following:

     ```
     #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old
     IP of the primary server> -NEWIP <New IP of the primary server>
     ```
   - If you changed FQDN, type the following:

     ```
     #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDFQDN
     <Old FQDN of the primary server> -NEWFQDN <New FQDN of the primary
     server>
     ```
6. On the secondary System Manager server, verify that the Geographic Redundancy page displays the new IP address or FQDN of the primary System Manager server.
7. Enable the Geographic Redundancy replication.

Related links

Enabling the Geographic Redundancy replication on page 75
Disabling the Geographic Redundancy replication on page 76
Changing the IP address or FQDN in System Manager on page 1290

Changing the IP address and FQDN on the secondary System Manager server when the secondary is in the standby or active mode

Procedure

1. Disable the Geographic Redundancy replication if not already disabled.
2. On the secondary System Manager server, change the IP address or FQDN or both. For instructions, see Changing the IP address and FQDN in System Manager.

   Wait for about 30–40 minutes before you perform the next step.
3. Log on to the web console of the secondary System Manager server, and verify that System Manager is running.
4. If System Manager is running on System Platform, log in to the CLI of the primary System Manager server as `root` and perform one of the following:
   - If you changed both the IP address and FQDN, type the following:

     ```
     #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old
     IP of the secondary server> -NEWIP <New IP of the secondary
     server> -OLDFQDN <Old FQDN of the secondary server> -NEWFQDN <New
     FQDN of the secondary server>
     ```
   - If you changed the IP address, type the following:

     ```
     #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old
     IP of the secondary server> -NEWIP <New IP of the secondary
     server>
     ```
   - If you changed FQDN, type the following:

     ```
     #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDFQDN
     <Old FQDN of the secondary server> -NEWFQDN <New FQDN of the
     secondary server>
     ```
5. On the primary System Manager server, verify that the Geographic Redundancy page displays the new IP address or FQDN of the secondary System Manager server.
6. Enable the Geographic Redundancy replication.

Related links

Enabling the Geographic Redundancy replication on page 75
Disabling the Geographic Redundancy replication on page 76
Changing the IP address or FQDN in System Manager on page 1290

Changing the IP address and FQDN on the secondary System Manager server when the primary is nonoperational

Procedure

1. On the secondary System Manager server, change the IP address or FQDN or both. For instructions, see Changing the IP address and FQDN in System Manager.

   Wait for about 30–40 minutes before you perform the next step.

2. Log on to the web console of the secondary System Manager server, and verify that System Manager is running.
3. Bring the primary System Manager server to operation.
4. Log on to the primary System Manager server and disable the Geographic Redundancy replication if not already disabled.
5. On the primary System Manager server, verify that the Geographic Redundancy page displays the new IP address or FQDN of the secondary System Manager server.
6. If System Manager is running on System Platform, log in to the CLI of the primary System Manager server as `root` and perform one of the following:
   - If you changed both the IP address and FQDN, type the following:

     ```
     #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old
     IP of the secondary server> -NEWIP <New IP of the secondary
     server> -OLDFQDN <Old FQDN of the secondary server> -NEWFQDN <New
     FQDN of the secondary server>
     ```

   - If you changed the IP address, type the following:

     ```
     #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old
     IP of the secondary server> -NEWIP <New IP of the secondary
     server>
     ```

   - If you changed FQDN, type the following:

     ```
     #sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDFQDN
     <Old FQDN of the secondary server> -NEWFQDN <New FQDN of the
     secondary server>
     ```

Related links

Changing the IP address or FQDN in System Manager on page 1290

Changing network parameters on System Manager running on VMware

Changing the IP address, FQDN, DNS, Gateway, or Netmask address from CLI

About this task

Use this procedure to change the network configuration parameters for Public interface and Management interface when OOBM is enabled.

Important:

- Do not change the network settings from vSphere Client when the virtual machine is in the power off state.
- FQDN value must be unique and different from the virtual FQDN value of System Manager.
- After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:
  1. Log in to the System Manager virtual machine as root user.
  2. Run the following command, `#sh /opt/Avaya/vsp/SMGRVirtualFqdnUtility.sh`.

Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Client and click on the **Console** tab or the 🖥 icon.
  - Start an SSH on System Manager.
- Log in to the System Manager virtual machine as admin.
- Create the System Manager virtual machine snapshot.

  Note:

  Delete the snapshot after the System Manager operation is complete.

Procedure

1. To configure Management network parameters, type `changeIPFQDN -IP <IP address> -FQDN <FQDN> -GATEWAY <Gateway address> -NETMASK <Netmask address> -DNS <DNS address> -SEARCH <search list of domain names>`.

   For information, see changeIPFQDN command.

2. To configure Public network parameters, type `changePublicIPFQDN -IP <IP address> -PublicFQDN <FQDN> -PublicGATEWAY <Gateway address> -PublicNETMASK <Netmask address>`.

For information, see changePublicIPFQDN command.

Next steps

Get new licenses from PLDS containing the new host ID and install the new licenses.

After you change the IP address of System Manager, the system generates a new host ID for WebLM server that System Manager hosts. Therefore, all previously installed licenses become invalid.

For instructions to install a license file, see Managing Licenses in *Administering Avaya Aura® System Manager*.

Related links

System Manager command line interface operations on page 1298

changeIPFQDN command on page 1297

changeIPFQDN command

Use the **changeIPFQDN** command to change the Management IP address when Out of Band Management is enabled. With this command you can change the IP address, FQDN, DNS address, Gateway, Netmask address for Management network configuration of System Manager, and the search list for the DNS address.

To change the Public IP address when Out of Band Management is enabled, use the **changePublicIPFQDN** command

Syntax

```
changeIPFQDN -IP < >  -FQDN < > -GATEWAY < >-NETMASK < > -DNS < > -SEARCH < >
```

#	Option	Description	Usage
1	IP	The new Management IP address of System Manager.	`changeIPFQDN -IP 10.11.12.13`
2	FQDN	The new Management FQDN of System Manager.	`changeIPFQDN -FQDN a.mydomain.smgr.com`
3	GATEWAY	The new Management Gateway address of System Manager.	`changeIPFQDN -GATEWAY 10.11.1.1`
4	NETMASK	The new Management netmask address of System Manager.	`changeIPFQDN -NETMASK 255.255.203.0`

5	DNS	The new Management DNS address of System Manager.
		You an provide multiple DNS addresses. Separate each address by a comma.
			`changeIPFQDN -DNS 10.11.1.2`
			`changeIPFQDN -DNS 10.11.12.5,10.11.12.3`

6	SEARCH	The new search list of domain names.	`changeIPFQDN -SEARCH smgr.com`

Example

You can provide options in any combination that the system supports:

```
changeIPFQDN -IP 10.11.y.z -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1 -NETMASK
255.255.255.0 -DNS 10.11.1.2 -SEARCH platform.avaya.com
```

```
changeIPFQDN -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1
```

```
changeIPFQDN -IP 10.11.y.z
```

System Manager command line interface operations

#	Command	Parameters	Description	Usage
1	**changeIPFQDN**	• **-IP <new Management interface or Out of Bound Management IP address for System Manager>** • **-FQDN <new Management or Out of Bound Management fully qualified domain name for System Manager>** • **-GATEWAY <new Management interface or Out of Bound Management Gateway address for System Manager>** • **-NETMASK <new Management interface or Out of Bound Management netmask address for System Manager>** • **-DNS <new DNS address for System Manager>** • **-SEARCH <new search list for DNS address>**	Updates the existing Management interface or Out of Bound Management IP address, FQDN, Gateway, Netmask, DNS, and the search list with the new value.	• **changeIPFQDN -IP <new IP address>** • **changeIPFQDN -FQDN <new fully qualified domain name>** • **changeIPFQDN -IP <new IP address> -GATEWAY <new Gateway address for System Manager> -SEARCH <new search list for DNS address>**
1	**changePublicIPFQDN**	• **-publicIP <new IP address for System Manager>** • **-publicFQDN <new fully qualified**	Updates the existing Public IP address, FQDN, Gateway, and Netmask with the new value.	• **changePublicIPFQDN -publicIP <new Public IP address>** • **changePublicIPFQDN -publicFQDN <new fully qualified**

Table continues…

#	Command	Parameters	Description	Usage
		domain name for System Manager> • -publicGATEWAY <new Gateway address for System Manager> • -publicNETMASK <new netmask address for System Manage>		domain name for public interface> • changePublicIPFQDN -publicIP <new Public IP address> -publicGATEWAY <new Public Gateway address for System Manager>
2	upgradeSMGR	<absolute path to the dmutility.bin> -m -v -V -H	Upgrades System Manager using the data migration utility.	upgradeSMGR dmutility *.bin -m -v -V -H
3	SMGRPatchdeploy	<absolute path to the System Manager service pack or the software patch>	Installs the software patch or the service pack for System Manager.	SMGRPatchdeploy <absolute path to /home/admin/<SMGRservicepackName> ✱ **Note:** Copy the System Manager service pack or patches that you must install to `/home/admin/`.
4	updateASG	<absolute path to the ASG XML file>	Updates the ASG XML file.	updateASG <absolute path to the ASG XML file>
5	configureTimeZone	Time zone that you select	Configures the time zone with the value that you select.	configureTimeZone Select a time zone. For example, America/Denver
6	configureNTP	<IP address of NTP server>	Configures the NTP server details.	configureNTP <IP address of NTP server> Separate IP addresses or hostnames of NTP servers with commas (,).
7	createCA		Creates a new Certificate Authority by using SHA2 signing algorithm and 2048 key size.	createCA You must provide the desired Common Name (CN)

Table continues…

#	Comma nd	Parameters	Description	Usage
			For more information, see, Creating a new Certificate Authority by using SHA2 signing algorithm and 2048 key size.	

Chapter 28: Configuring the date and time

Verifying changes to the date and time configuration

Procedure

1. Log in to System Manager from the command line.
2. Type the date, and press `Enter`.

   The system displays the updated date, time, and time zone values. Verify the values.
3. Type `exit` and press `Enter`.

Configuring System Manager logs for Syslog server

You can direct System Manager security logs to remote Syslog server. Also, you can configure general and security logs for the Syslog server.

About this task

Perform the following procedure to configure security audit logs for the Syslog server.

Procedure

1. Log on to System Manager web console.
2. Click **Services** > **Events**.
3. Click **Logs** > **Log Settings**.
4. On the Log Settings page, in the **Logger** column, select `com.avaya.security.iam.audit`.
5. Click **Edit**.
6. On the Edit Logger page, click **Attach**.
7. On the Attach Appender page, in the **Select Appender** field, select **SYSLOG**.
8. Click **Commit**.

   Add SYSLOG as an appender for the audit log.

Note:

To modify the Syslog configuration, select the SYSLOG appender and click **Edit**.

Changing date and time on System Manager running on VMware

Configuring the NTP server

Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Client and click on the **Console** tab or the 🖥 icon.
  - Start an SSH on System Manager.
- Log in to the System Manager virtual machine as admin.

Procedure

Type `configureNTP <IP address of NTP server>`.

Related links

System Manager command line interface operations on page 1298

Configuring the time zone

Procedure

1. Type `configureTimeZone`.
2. Select the time zone from the list.

   For example, America/Denver.

Related links

System Manager command line interface operations on page 1298

Appendix A: Firewall implementation in System Manager

Firewall basics

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources. The firewall controls what outside resources its own users can have access to. Simply put, a firewall is a program or a hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters it is not allowed through.

Firewalls use one or more of three methods to control traffic flowing in and out of the network:

- Packet filtering - Packets or small chunks of data are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded.
- Proxy service - Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.
- Stateful inspection - A newer method that does not examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match the information is allowed through. Else, it is discarded.

Firewall implementation in System Manager

The System Manager firewall implementation uses packet filtering and stateful inspection techniques. The System Manager firewall provides the following:

- Supports unlimited access to loop back address through packet filtering.
- Drops all inbound packets by default, allows all outbound packets, and allows all packets that are to be forwarded through packet filtering.
- For TCP packets, the firewall checks for various combinations of the TCP flags to ascertain whether a packet is valid or not. The System Manager firewall implementation includes a set of standard rules for identifying valid TCP packets.

- Supports stateful inspection of packets. The firewall checks the state of all inbound and outbound packets for secure communication. For inbound packets the state must be either Established or Related. For outbound packets the state must be either New, Established or Related.
- Disables ICMP timestamp responses as this allows an attacker to know the date which is set on your machine. This defeats all the time based authentication protocols.
- Allows inbound communication on ports that are exposed for interactions with various Avaya Aura® products.

Appendix B: Communication Manager reports available through System Manager

List reports

- aar analysis
- aar digit-conversion
- aar route-chosen
- abbreviated-dialing group
- abbreviated-dialing personal
- aca-parameters
- access-endpoint
- administered-connection
- agent-loginid
- announcements
- ars analysis
- ars digit-conversion
- ars route-chosen
- asq-history
- attendant
- audio-group
- authorization-code
- bcms agent
- bcms skill
- bcms split
- bcms summary agent
- bcms summary skill
- bcms summary split

- bcms summary trunk
- bcms summary vdn
- bcms trunk
- bcms vdn
- bcms-vustats loginIDs
- best-service-routing
- bridged-extensions
- cabinet
- call-forwarding
- calltype
- configuration all
- configuration board
- configuration carrier
- configuration control
- configuration ds1
- configuration firmware-versions
- configuration media-gateway
- configuration port-network
- configuration power-supply
- configuration radio-controller
- configuration software-versions
- configuration stations
- configuration trunks
- configuration wt-stations
- cor
- coverage answer-group
- coverage path
- coverage time-of-day
- crm-features
- cti-link
- data-module
- directory board
- disabled-mos
- do-not-disturb group

- do-not-disturb station
- eda-external-device-alrm
- emergency
- extended-pickup-group
- extension-type
- group-page
- groups-of-extension
- history
- holiday-table
- hunt-group
- internal-data loginID
- integrated-annc-boards
- intercom-group
- intra-switch-cdr
- ip-codec-set
- ip-interface
- ip-network-map
- ip-network-region monitor
- ip-network-region qos
- ip-route
- ipserver-interface
- isdnpri-testcall
- logins
- marked-ports
- mct-history
- media-gateway
- meet-me-vdn
- members hunt-group
- members trunk-group
- mmi
- modem-pool
- moh-analog-group
- monitored-station
- mst

- multimedia endpoints
- multimedia h.320-stations
- multimedia ip-stations
- multimedia ip-unregistered
- node-routing
- node-names
- off-pbx-telephone station-mapping
- partition-route-table
- partitioned-group
- personal-co-line
- pickup-group
- pms-down
- policy-routing-table
- precedence-routing analysis
- precedence-routing digit-conversion
- precedence-routing route-chosen
- pri-endpoint
- private-numbering
- public-unknown-numbering
- registered-ip-stations
- remote-office
- report-scheduler
- route-pattern
- service-hours-table
- set-data
- signaling-group
- sip-station
- skill-status
- station
- stn-firmware
- survivable-processor
- suspend-alm-orig
- synchronization
- sys-link

- term-ext-group
- toll all
- toll restricted-call
- toll toll-list
- toll unrestricted-call
- trace
- trunk-group
- tti-ip-stations
- uniform-dialplan
- usage button-type crss-alert
- usage button-type hunt-ns
- usage button-type night-serv
- usage button-type trunk-ns
- usage cti-link
- usage digit-string
- usage extension
- usage holiday-table
- usage hunt-group
- usage ip-address
- usage node-name
- usage variables
- usage vector
- user-profiles
- vdn
- vector
- video-bridge
- vrt
- vustats-display-format
- wakeup incomplete
- wakeup requests
- wakeup station
- xmobile mapping

Display reports

- aar analysis
- aar digit-conversion
- abbreviated-dialing 7103A-buttons
- abbreviated-dialing enhanced
- abbreviated-dialing group
- abbreviated-dialing personal
- abbreviated-dialing system
- access-endpoint
- adjunct-names
- administered-connection
- agent-loginid
- alarms
- alias station
- alphanumeric-dial-table
- alternate-frl
- announcement
- ars analysis
- ars digit-conversion
- ars toll
- attendant
- audio-group
- authorization-code
- bcms-vustats loginIDs
- best-service-routing
- bp
- bri-trunk-board
- bulletin-board
- button-labels
- button-location-aca
- cabinet
- call-screening
- call-type

- cama-numbering
- capacity
- carrier-frequencies
- circuit-packs
- communication-interface links
- communication-interface processor-channels
- console-parameters
- cor
- cos
- cos-group
- coverage answer-group
- coverage path
- coverage remote
- coverage sender-group
- coverage time-of-day
- cti-link
- data-module
- daylight-savings-rules
- dialplan analysis
- dialplan parameters
- digit-absorption
- display-messages ad-programming
- display-messages auto-wakeup-dn-dst
- display-messages button-labels
- display-messages call-identifiers
- display-messages date-time
- display-messages leave-word-calling
- display-messages malicious-call-trace
- display-messages miscellaneous-features
- display-messages posted-message
- display-messages property-management
- display-messages self-administration
- display-messages softkey-labels
- display-messages time-of-day-routing

- display-messages transfer-conference
- display-messages view-buttons
- display-messages vustats
- ds1
- eda-external-device-alrm
- enp-number-plan
- errors
- ethernet-options
- events
- extended-pickup-group
- failed-ip-network-region
- feature-access-codes
- firmware download
- firmware station-download
- group-page
- holiday-table
- hunt-group
- inc-call-handling-trmt
- initcauses
- integrated-annc-boards
- intercom-group
- intra-switch-cdr
- ip-codec-set
- ip-interface
- ip-network-map
- ip-network-region
- ip-parameters
- ip-route
- ip-services
- ipserver-interface
- isdn dcs-qsig-tsc-gateway
- isdn mwi-prefixes
- isdn network-facilities
- isdn private-numbering

- isdn public-unknown-numbering
- isdn qsig-dcs-tsc-gateway
- isdn tsc-gateway
- ixc-codes
- listed-directory-numbers
- location-parameters
- locations
- login
- lsp
- mct-group-extensions
- meas-selection coverage
- meas-selection principal
- meas-selection route-pattern
- meas-selection trunk-group
- meas-selection wideband-trunk-group
- media-gateway
- modem-pool
- mst
- multifrequency-signaling
- node-names audix
- node-names ip
- node-routing
- off-pbx-telephone configuration-set
- off-pbx-telephone feature-name-extensions
- off-pbx-telephone station-mapping
- paging code-calling-ids
- paging loudspeaker
- partition-route-table
- permissions
- personal-CO-line
- pickup-group
- port
- precedence-routing analysis
- precedence-routing digit-conversion

- pri-endpoint
- private-numbering
- public-unknown-numbering
- radio-controller
- reason-code-names
- remote-access
- remote-office
- rhnpa
- route-pattern
- service-hours-table
- signaling-group
- sit-treatment
- site-data
- software
- station
- svn-button-location
- synchronization
- system-parameters cdr
- system-parameters country-options
- system-parameters coverage-forwarding
- system-parameters crisis-alert
- system-parameters customer-options
- system-parameters duplication
- system-parameters features
- system-parameters hospitality
- system-parameters ip-options
- system-parameters ipserver-interface
- system-parameters maintenance
- system-parameters mlpp
- system-parameters multifrequency-signaling
- system-parameters ocm-call-classification
- system-parameters offer-options
- system-parameters security
- system-parameters special-applications

- system-parameters wireless
- telecommuting-access
- tenant
- term-ext-group
- terminal-parameters
- tftp-server
- time
- time-of-day
- toll
- tone-generation
- trunk-group
- uniform-dialplan
- variables
- vdn
- vector
- video-bridge
- vrt
- vustats-display-format
- xmobile configuration-set

List reports available in Avaya Aura® System Manager 7.0

- measurements aca
- measurements announcements board last-hour
- measurements announcements board today-peak
- measurements announcements board yesterday-peak
- measurements announcements all last-hour
- measurements announcements all today-peak
- measurements announcements all yesterday-peak
- measurements attendant group
- measurements attendant positions
- measurements blockage pn last-hour
- measurements blockage pn today-peak

- measurements blockage pn yesterday-peak
- measurements call-rate data
- measurements call-rate multimedia
- measurements call-rate service-link
- measurements call-rate total
- measurements call-rate voice
- measurements call-summary
- measurements cbc-trunk-group last-hour
- measurements cell-traffic cell-addr last-hour
- measurements cell-traffic cell-addr today-peak
- measurements cell-traffic cell-addr yesterday-peak
- measurements cell-traffic summary last-hour
- measurements cell-traffic summary today-peak
- measurements cell-traffic summary yesterday-peak
- measurements clan ethernet
- measurements clan sockets detail last-hour
- measurements clan sockets detail today-peak
- measurements clan sockets detail yesterday-peak
- measurements clan sockets hourly
- measurements clan sockets summary last-hour
- measurements clan sockets summary today-peak
- measurements clan sockets summary yesterday-peak
- measurements communications-links 1-8
- measurements communications-links 9-16
- measurements communications-links 17-24
- measurements communications-links 25-32
- measurements communications-links 33
- measurements coverage-path last-hour
- measurements coverage-path today-peak
- measurements coverage-path yesterday-peak
- measurements ds1 log
- measurements ds1 summary
- measurements ds1-facility log
- measurements ds1-facility summary

- measurements expansion-services-mod hourly
- measurements expansion-services-mod summary last-hour
- measurements expansion-services-mod summary today-peak
- measurements expansion-services-mod summary yesterday-peak
- measurements hunt-group last-hour
- measurements hunt-group today-peak
- measurements hunt-group yesterday-peak
- measurements ip codec detail last-hour
- measurements ip codec detail today-peak
- measurements ip codec detail yesterday-peak
- measurements ip codec hourly
- measurements ip codec summary last-hour
- measurements ip codec summary today-peak
- measurements ip codec summary yesterday-peak
- measurements ip dsp-resource detail last-hour
- measurements ip dsp-resource detail today-peak
- measurements ip dsp-resource detail yesterday-peak
- measurements ip dsp-resource hourly
- measurements ip dsp-resource summary last-hour
- measurements ip dsp-resource summary today-peak
- measurements ip dsp-resource summary yesterday-peak
- measurements ip signaling-groups current-hour
- measurements ip signaling-groups last-hour
- measurements ip signaling-groups today
- measurements ip signaling-groups yesterday
- measurements lar-route-pattern last-hour
- measurements lar-route-pattern today
- measurements lar-route-pattern yesterday
- measurements lightly-used-trunk last-hour
- measurements lightly-used-trunk today
- measurements lightly-used-trunk yesterday
- measurements load-balance incoming last-hour
- measurements load-balance incoming today-peak
- measurements load-balance incoming yesterday-peak

- measurements load-balance intercom last-hour
- measurements load-balance intercom today-peak
- measurements load-balance intercom yesterday-peak
- measurements load-balance outgoing last-hour
- measurements load-balance outgoing today-peak
- measurements load-balance outgoing yesterday-peak
- measurements load-balance tandem last-hour
- measurements load-balance tandem today-peak
- measurements load-balance tandem yesterday-peak
- measurements load-balance total last-hour
- measurements load-balance total today-peak
- measurements load-balance total yesterday-peak
- measurements modem-pool last-hour
- measurements modem-pool today-peak
- measurements modem-pool yesterday-peak
- measurements multimedia-interface hourly
- measurements multimedia-interface last-hour
- measurements multimedia-interface today-peak
- measurements multimedia-interface yesterday-peak
- measurements occupancy busiest-intervals
- measurements occupancy last-hour
- measurements occupancy summary
- measurements outage-trunk last-hour
- measurements outage-trunk today
- measurements outage-trunk yesterday
- measurements principal last-hour
- measurements principal today-peak
- measurements principal yesterday-peak
- measurements route-pattern last-hour
- measurements route-pattern today
- measurements route-pattern yesterday
- measurements security-violations detail
- measurements security-violations summary
- measurements summary

- measurements tone-receiver detail last-hour
- measurements tone-receiver detail today-peak
- measurements tone-receiver detail yesterday-peak
- measurements tone-receiver summary last-hour
- measurements tone-receiver summary today-peak
- measurements tone-receiver summary yesterday-peak
- measurements trunk-group hourly
- measurements trunk-group summary last-hour
- measurements trunk-group summary today-peak
- measurements trunk-group summary yesterday-peak
- measurements voice-conditioners hourly
- measurements voice-conditioners summary last-hour
- measurements voice-conditioners summary today-peak
- measurements voice-conditioners summary yesterday-peak
- measurements wideband-trunk-group hourly
- measurements wideband-trunk-group summary last-hour
- measurements wideband-trunk-group summary today-peak
- measurements wideband-trunk-group summary yesterday-peak
- performance attendant today
- performance attendant yesterday
- performance hunt-group today
- performance hunt-group yesterday
- performance summary today
- performance summary yesterday
- performance trunk-group today
- performance trunk-group yesterday

Status reports available in Avaya Aura® System Manager 7.0

- access-endpoint
- administered-connection
- aesvcs (cti-link, interface, link)

- attendant
- audits
- bri-port
- cabinet
- cdr-link
- clan-al
- clan-ip
- clan-port
- clan-usage
- data-module
- environment
- esm
- ess
- firmware
- hardware-group
- health
- ip-board
- ip-network-region
- ip-synchronization
- isdnpri-testcall
- journal-link
- link
- logins
- media-gateways
- media-processor
- mg-announcements
- meet-me-vdn
- mst
- nr-registration
- off-pbx-telephone
- packet-interface
- periodic-scheduled
- pms-link
- pnc

- port-network
- pri-endpoint
- processor-channels
- processor-ip-interface
- psa
- qos-parameters
- remote-access
- remote-office
- signaling-group
- sp-link
- socket-usage
- station
- switch-node
- synchronization
- sys-link
- trace-analyzer
- trunk
- tsc-administered
- tti
- val-ip
- video-bridge

Commands that does not generates CSV reports

- integrated-annc-boards
- measurements attendant positions
- measurements cell-traffic cell-addr last-hour
- measurements cell-traffic summary last-hour
- measurements cell-traffic summary today-peak
- measurements cell-traffic summary yesterday-peak
- measurements tone-receiver summary last-hour
- members hunt-group
- members trunk-group

Migration

The migration process includes changing the server hardware, change the operating system, and reinstallation of software that includes hypervisor.

During migration, you might need to perform backup and restore operations outside the normal upgrade process. You cannot rollback the upgrade easily.

Related links

Upgrade on page 1322
Update on page 1322

Upgrade

The upgrade process includes upgrading a product from earlier release to the latest release without the need to change the server hardware or hypervisor.

The process is triggered through the normal process without requiring additional backup and restore operations. You can rollback an upgrade.

Related links

Migration on page 1322

Update

The update process includes installing patches of an application. For example, kernel patches, security patches, hotfixes, service packs, and feature packs.

Related links

Migration on page 1322

Index

Special Characters

.CADF xml file to MIB and trapd file 881, 882

Numerics

2048 key size 1101
7.0 .... 1212, 1215

A

AAR/ARS Digit Conversion field descriptions
  AAR/ARS Digit Conversion; field description 691, 694
Abbreviated Dialing
  Enhanced List 661
Abbreviated Dialing List 1, List 2, List 3 660
abbreviated dialing lists 660
abort
  global user settings import job on first error 345
abort a user import job 336
abort global user settings import job on first error 345
about audio files 1063
about CM aduit 902
about IP Office element manager 733
about reports 998
about security configuration 743
about system configuration 740
Access Control 143
Accessing Element Cut-Through 631
accessing log harvest 923
accessing resources 136
accessing scheduler 1011
accessing the Backup and Restore service 779
accessing the Data Retention Rules service 796
accessing the Log Settings service 936
accessing WebLM 951
access log harvesting 923
access profile 865
  create 855
  delete 856
  modify 856
  new 855
  remove 856
access Solution Deployment Manager client 1144
Access to Administrative Users 172
access to PLDS 1148
account operations
  CS1000 907
account synchronization 903
activate
  secondary server 76
activating agent 894
activating serviceability agent 894
Active
  Coverage Path 624
Active Station Ringing 648
Act Time 630
actual license usage 953
add
  Appliance Virtualization Platform host 1179
  AVP host 1179
  Communication Manager 860
  communication profile for user 204
  custom role 148
  custom tenant administrator role 149
  endpoints 633
  ESXi host 1179, 1201
  G430 gateway 862
  G450 gateway 862
  location 1174
  new role 148
  new tenant administrator role 149
  role 148
  virtual machine 1192, 1196
add a contact address of a private contact 233
add a contact address of a public contact 523
add address 200
Add Address page 202, 239, 533
add a postal address to public contact 521
add a public contact 519
Add Communication Manager
  field descriptions 876
Add Communication Manager field descriptions 876
add element access profile 845
add element instances 961
Add elements
  bulk 833
  manual 832
Add elements in bulk 833
Add End Entity 1098
add endpoints
  field descriptions 644
add endpoints in bulk 670
add endpoint templates
  field descriptions 644
add ESXi host 1179
add ESXi host in vCenter 1201
Adding
  CallPilot 553
  listen-only 676
  Service Observe 676
  so-coach 676
  VOA Repeat 677
adding a CM Endpoint profile 209
adding a contact in contact list 222
adding a CS 1000 or CallPilot profile 216

adding a CS 1000 profile 217
Adding a data module
  data modules; adding 699
adding agent
  agents; add 592
adding agents in bulk
  agents; bulk add 593
adding a local WebLM server 965
adding a messaging profile 213
adding an announcement 603
adding an audio group 612
adding an element access profile 845
adding an IP Office endpoint profile 219
adding announcements 603
adding an SNMP Access profile 839
adding an SNMP target profile 886
adding a postal address of a private contact 231
adding a private contact 229
adding a shared address 532
adding a trusted certificate to Communication Manager . 1282
Adding a UCM and Application Server Configuration template
....1066
adding audio groups 612
adding a vector routing table 618
Adding a VMPro Call Flow template 1074
Adding a VMPro System Configuration template 1070
adding CM Agent template 1030
adding CM Endpoint template 1032
Adding Communication Manager certificate to the System Manager 1285
adding communication profile for user 204
adding communication profiles
  IP Office endpoint 219
Adding corporate logo 45
adding coverage path
  coverage path; add 621
adding coverage time-of-day
  coverage time-of-day; add 628
adding custom role 148
adding dependencies to endpoints 728
adding endpoints 633
adding IP Office endpoint template 1056
adding IP Office system configuration templates 1060
Adding off PBX endpoint mapping 683
adding Remote Servers 1008
adding resources to a selected group 138
adding subnetworks 843, 844
adding subscribers CMM field description 574
adding subscribers MM field description 577
adding subscriber templates
  field descriptions 1048
adding subscriber templates; field description 1051
adding subscriber templates MM; field description 1053
adding synchronization datasources 51
adding templates; subscriber
  adding subscriber templates
    new subscriber templates 1035
adding UDP entries 724
adding udp group 719
adding uniform dial plan group 719
adding vector directory number
  vector directory number; add 616
Add IP Office
  field description 879
Add local WebLM page 975
add location 1174
add location to host 1202
Add Mapping 157, 159
Add New Role 156
Add Remote Server field descriptions 1009
add resources; selected groups 138
address
  add 200
Add service to user 542
add SNMP Access profile 839
Add Station Template 646
add subscribers
  Messaging field descriptions 569
add System Platform 859
Add Trusted Certificate page 1094
add trusted certificates 1085
add virtual machine 1192, 1196
admin
  logon information 38
administration
  Session Manager communication profile 207
Administrative Users 172
advanced search
  searching announcements 608
  searching endpoints 639
Advance Options Presence Integration 663
AES
  user management 112
agent
  adding dependencies 728
Agent editor
  permissions 165
Agent Management page 798
agents 591
agents; bulk delete 594
agents field descriptions
  agents ....
    field description 595
Agent Skill
  Adding 677
  SIP Phones 677
agents list 592
agent template
  field description 1041
agent template field description 1041
Alarming 909
Alarming UI 812
Alarm List page 917
Alarm Management 799

alarms
- CS 1000 96
- delete 911
- exclude 888
- forward to secondary System Manager 915
- include 888
- standby mode 915

alarms; export 910
alarms; search 912
Alarms for Conferencing 108
Alarms for IP Office 111
alarm throttling; configure 912
all announcements; backup 605
Allocations by Feature Page 982
Allocations by Local WebLM page 983
Allow access to Administrative Users Web UI 172
alternate source 1148
- upgrades 1149

Always Use
- Station 655

analyze inventory
- SDM 1168

analyze job status 1231
analyze software 1237
analyzing
- software 774, 1238

analyzing software inventory 1244
announcement 601
announcement; add 603
announcements 609
announcements; backup 605
announcements; broadcast 607
announcements; delete 604
announcements; download 606
announcements; edit 604
announcements; filter 608
announcements; move 607
announcements; restore 606
announcements; save 605
announcements; view 604
announcements list 602
anonymous communication profiles 906
anonymous profiles 904
- assign 904
- delete 905

answer 672
appender; modify 939
Appliance Virtualization Platform 31
Appliance Virtualization Platform host password
- change 1182

Appliance Virtualization Platform network parameters 1181
application instance
- create 833
- new 833

application instances 831
application management page 862
applications

applications *(continued)*
- preupgrade check 1171

Applying a Communication Manager patch 1276
Applying an IP Office system configuration template on an IP Office device 1062
Applying a UCM and Application Server Configuration template 1069
Applying a VMPro call flow template on a device 1076
Applying a VMPro System Configuration template on a device 1072
Architecture and deployment diagrams for Geographic Redundancy 66
Argument 662
Assertions 1114
assign
- shared address to user 202, 531
- tenant administrator 1125

assigned elements
- remove 855

assigned resources
- remove 127

assign groups
- multiple users 197, 198
- single user 197

Assign Groups 313
assign groups to user 312
assigning an appender to a logger 938
assigning anonymous profiles 904
assigning applications 855
assigning filter profile to serviceability agent 891
Assigning permissions
- CM templates 1034

assigning permissions in user management 164
assigning permissions through User Management 165
assigning permission to access UDP groups 726
assigning range for endpoints 164
assigning resources 137
assigning resources to group 123
assigning roles to
- multiple users 196

assigning users to role 152
assign permissions in Scheduler 1011
assign permissions in Solution Deployment Manager 150
Assign Role page 312
Assign Roles page 311
assign roles to
- single user 195

assign users 152, 199
Assign Users 158, 315
assign users to role 152
assign users to roles 199
association between IP Office endpoint profile and user
- remove 222

Attach Appender page 941
attach contacts page 224
attribute details defined in Delete user XSD 467
attribute details defined in Import User XSD 459

attribute details defined in the CM Endpoint profile XSD ... 468
attribute details defined in the Conferencing communication profile XSD ... 502
attribute details defined in the Messaging communication profile XSD ... 491
attribute details defined in the Session Manager communication profile XSD ... 499
Audible Message Waiting ... 655
audio files
  transfer ... 767
audio groups ... 612
audio groups; add ... 612
audio groups; delete ... 613
audio groups; edit ... 612
audio groups; more actions ... 613
audio groups; view ... 613
audio groups field description ... 614
audit reports ... 902
Audix Name ... 654
authentication
  Kerberos server ... 1111
authentication scheme
  edit ... 1109
authentication servers ... 1110
authorization code ... 712
authorization code field description
  authorization code; field description ... 714
authorization code list ... 713
auto ... 672
Auto activation of serviceability agents ... 894
Auto answer ... 672
  field descriptions ... 672
Auto Answer
  Station ... 648
automatic
  call routing ... 211
automatic alternate routing digit conversion ,
  aar digit conversion ... 690, 693
  ars digit conversion ... 690, 693
  automatic route selection digit conversion ... 690, 693
automatic route selection toll,
  ars toll ... 696
automatic route selection toll field descriptions ... 697
automatic route selection toll list ... 696
AutoRefresh Alarm List page ... 916
auto-refresh log list page ... 947
Auto Select Any Idle Appearance ... 655
Avaya appliance offer ... 31
Avaya Aura application
  deploy ... 1145
  upgrade ... 1145
Avaya Aura application upgrade ... 1205, 1212
Avaya Aura Conferencing configuration ... 105
Avaya Multimedia Messaging ... 112
Avaya SIP AST endpoints ... 1128

B

B5800 endpoint templates
  duplicate ... 1058
backing up all anouncements ... 605
backing up audio groups ... 613
backing up audio groups; field description ... 614
Backing up Communication Manager
  Backing up Communication Manager Messaging 1258
Backing up Communication Manager or Communication Manager Messaging ... 1258
backup ... 777, 778
  remote server ... 780
Backup ... 745, 751
backup and restore ... 777, 778
Backup and Restore page ... 789
backup and restore service; access ... 779
backup and restore time ... 787
backup field descriptions ... 747
backup files; view ... 779
backup file size ... 787
backup of announcements ... 605
Backup page ... 790
basic reports
  generate ... 1000
  new ... 1000
bidirectional synchronization ... 49
Bindings ... 1114
Branch Session Manager upgrade ... 1208
Bridged Appearance Origination Restriction ... 659
Bridged Call Alerting ... 648
Bridged Idle Line Preference ... 655
broadcasting an announcement ... 607
broadcasting anouncements ... 607
Building
  Station ... 660
built-in roles ... 143
Built-in roles ... 143
bulk add endpoint; field descriptions ... 670
bulk delete endpoints ... 638
bulk deleting agents ... 594
bulk deleting endpoints ... 638
bulk edit
  users ... 183, 185
bulk export ... 317, 323, 794
  key features ... 323
bulk export global settings ... 342
bulk export of global user settings ... 341
bulk export of users ... 328
bulk export of users partially ... 331
bulk export users ... 327
bulk export utility ... 853
bulk import ... 317, 323, 794
  global settings options ... 339
  global user settings ... 340
  key features ... 323
bulk import and export ... 317, 323, 794

bulk import and export of user by using Excel file 319
bulk import and export with Excel 317
BulkImportEncryptionUtil 333, 334
bulk import encryption utility 332
Bulk import of elements 833
bulk import of global user settings 339, 340
bulk import of partial user attributes 330
bulk import users 324
bulk import XML for users with SIP phone 516
bulk user
    delete 184
bulk user edit job
    view 183
Bulk User Editor 185
Busy
    Coverage Path 625
Button Assignment 662
Button Feature 662
Button Label 662

C

Cable 660
CA Generation utility 36
Call Appearance Display Format 654
Call Forwarding 661
CallPilot
    functionality limitations 98
Call Pilot
    configuration 101
CallPilot certificate 553
cancel
    global user settings import job 346
cancel a global user settings import job 346
cancel a user import job 338
capabilities
    Solution Deployment Manager client 1145
CDR Privacy 655
centralized licensing 957
    adding elements 959
    disable 962
    enable 958
    overview 957
centralized Solution Deployment Manager 1140
certificate
    generation capabilities 1079
    management capabilities 1079
    Microsoft Active Directory 1084
    view 1101
Certificate authorities 1093
Certificate Authority 1102
Certificate Enrollment 1100
certificate generation 1097
certificate keystore
    generate 1099
certificate response 1104
Certificate Signing Request
Certificate Signing Request *(continued)*
    create 1097
certificate using CSR
    create 1100
change
    DNS 1296, 1298
    ESXi host IP address 1181
    FQDN 1290, 1296
    FQDN from CLI 1298
    Gateway 1296, 1298
    IP address 1290, 1296
    IP address from CLI 1298
    Netmask 1296, 1298
    search list 1296, 1298
change abbreviated-dialing enhanced 661
Change Allocations page 984
Change communication profile password 173
change ESXi host password 1182
change FQDN
    primary System Manager 1292
change FQDN from CLI 1298
change FQDN in the primary System Manager 1292
change FQDN on primary System Manager 1293
change FQDN on secondary System Manager 1294, 1295
Change Gateway 1184
change H323 and SIP passwords 173
change IP address
    primary System Manager 1292
change IP address and FQDN on primary and secondary System Manager 1291
change IP address for ESXi host 1181
change IP address from CLI 1298
change IP address on primary System Manager 1292
Change IP address on primary System Manager 1293
change IP address on secondary System Manager 1294, 1295
changeIPFQDN 1298
Change IP FQDN 1190
changeIPFQDN command, ... 1297
change Netmask for Appliance Virtualization Platform host 1181
Change Network Params 1181
Change Password page 42
changePublicIPFQDN 1298
changing alarm status 910
changing allocations of a licensed feature 970
changing a managed element's FQDN in System Manager 1290
changing a managed element's IP address in System Manager 1290
changing compatibility view setting 36
changing FQDN in System Manager 1290
changing IP address in System Manager 1290
changing System Manager IP address in managed elements 1291
changing to classic view 591
Check 1241

checklist
    Branch Session Manager upgrade 1207
    Communication Manager 6.x upgrade 1207, 1246
    Session Manager upgrade 1207
choose
    shared address 202, 531
Choose Address page 204
choose a shared address for a private contact 522
Choose Group page 141
choose parent group 142
choosing a shared address for a private contact 232
class of service 708
    messaging; class of service
        COS 565
Class of Service
    COS List 566
class of service data; edit 708
class of service data; view 709
class of service field description 709
class of service group,
    cos group 714
    system; class of service group 714
class of service group field descriptions
    class of service group; field description 716
class of service group list 714
class of service list; field description 709
class of service list; filter 709
CleanUp 905
clean up communication profiles 905
client audit 988
Client node locking 952
client Solution Deployment Manager 1139
CM Agent template
    upgrade 1029
CM Agent template;
    add 1030
    copy 1031
    delete 1031
    edit 1030
CM audit 902
CM audit field description 902
CM audit report; field description 903
CM audit report field descriptions 903
CM Endpoint profile
    delete 212
CM Endpoint template
    upgrade 1029
CM Endpoint templates
    add 1032
    copy 1034
    delete 1033
    edit 1032
    view 1033
CM notify sync feature 1279
CM objetcs 587
CM station data
    export 317
CM station data *(continued)*
    import 317
CM templates
    permissions 1034
CM Upgrade Configuration
    field description
        CM Upgrade Configuration 1260
collecting inventory 773, 1236
command
    changeIPFQDN 1297
    configureTimeZone 1302
    exportUpmGlobalsettings 343
    runRTSCli.sh 853
command line restore 786
command runRTSCli.sh 853
communication address
    modify 206
Communication Manager
    6.3.100 1234
    add 860, 876
    Multi Tenancy 1129
    new features 34
    upgrade 1234
Communication Manager; adding a trusted certificate 1282
Communication Manager; update 1276
Communication Manager 5.2.1
    upgrade 1248, 1257, 1266, 1269, 1270
    upgrade on different server 1269
Communication Manager 5.2.1 to 6.3.100 upgrade 1271
Communication Manager 5.2.1 upgrade 1257
Communication Manager 5.x upgrade 1275
Communication Manager 6.x 1246
    upgrade 1249, 1250
Communication Manager audit 902
Communication Manager Backup Configuration field descriptions 1259
Communication Manager capabilities 583
Communication Manager configuration when primary System Manager is nonoperational 95
Communication Manager objects 587
Communication Manager objects; add
    adding Communication Manager objects 589
Communication Manager objects; changing to classic view 591
Communication Manager objects; delete
    deleting Communication Manager objects 590
Communication Manager objects; edit
    Communication Manager objects; edit 590
Communication Manager Session Manager correlation 731
Communication Manager templates
    permissions 1034
Communication Manager update 1210
Communication Manager upgrade 1208
Communication Manager upgrade from Software Management 1204
Communication Manager upgrade from System Manager 1204

Communication Manager upgrades 1232
communication profile
  add 204
  Presence 208
Communication profile 257
communication profile for user
  delete 205
communication profile password history policy 538
communication profile password policy
  edit 538
Communication Profile Password Policy field descriptions 539
communication profile password strength policy 538
communication profiles
  clean up 905
  delete 905
Communication profiles 204
communication profiles; synchronize 903
communication profiles for a user 209
communication profiles synchronization 903
communication profile worksheets
  communication profile hierarchy 321
  hierarchy 321
  parent-child communication profile 321
  relationship 321
  worksheets 321
Company ID 1149
compatibility mode 36
completed jobs
  view 1012
Completed Jobs Page 1019
Conf/Trans On Primary Appearance 656
Conferencing configuration 105
Conferencing GR configuration 105
configuration 326, 329
  Conferencing 105
  Meeting Exchange element 100
  Messaging 102
configuration management 798
configuration options for bulk import of users 329
configuration options for bulk import through Excel 326
Configuration Parameters 1196
configure
  Communication Manager when primary System Manager is nonoperational 95
  Geographical Redundancy 73, 81
  health monitoring timeout interval 84
  Hosted Service Provider on System Manager 1116
  Remote Identity Provider 1117
configure alarm throttling 912
Configure Call Pilot 101
configure centralized licensing 958
  field description 958
configure centralized licensing field description 958
configure Conferencing 108
configure CS 1000 SNMP alarms 96
configure customized interface
configure customized interface *(continued)*
  field descriptions 48
configure enterprise licensing 963
configure FTP server as remote server 1155
configureNTP 1298, 1302
Configure options 907
Configure Presence Server 100
configure remote server
  protocol support 1154
configureTimeZone 1298, 1302
configure two-way TLS 1285
configuring
  Multimedia Messaging 112
  periodic report cleanup 1007
  report properties 1007
Configuring
  GR-unaware elements 88
Configuring Communication Manager during GR failback 94
Configuring Communication Manager during GR failover 93
Configuring Communication Manager during GR failover when only the primary is reachable 95
configuring communication manager user profile settings 584
Configuring Conferencing to be managed by System Manager 105
Configuring CS 1000 96
Configuring DTLS for CS 1000 1107
configuring endpoints 727
configuringfor GR
  IP Office 109
configuring IP Office 800
  field description 801
configuring IP Office in Active-Active scenario 111
Configuring IP Office in normal operation with SCEP disabled 110
Configuring IP Office in normal operation with SCEP enabled 109
Configuring IP Office when primary is active 109, 110
configuring IP Office when primary nonfunctional 110
Configuring Linux-based CS1000 servers 97
Configuring Messaging during GR failback 103
Configuring Messaging during split network 104
Configuring Messaging in normal operational mode 102
Configuring Messaging when primary server is nonoperational 103
configuring notify sync 1283
configuring NTP server 1302
configuring periodic 1007
configuring periodic cleanup 1007
configuring periodic cleanup for reports 1007
Configuring Presence Server 100
configuring Remote Servers 1008
Configuring Remote Servers 1008
configuring report 1007
configuring report properties 1007
Configuring Session Manager Release 6.2 and earlier during failback 91

configuring Session Manager Release 6.2 and earlier during GR failover 91
Configuring SIP TLS for CS1000 1108
configuring Syslog server 1301
configuring System Manager security logs 1301
Configuring the http or https protocol for a remote server . 745
configuring time zone 1302
configuring trap listener 824
configuring two-way TLS 1285
Configuring user settings 1148
Configuring VxWorks-based CS1000 servers 97
confirming identity certificate updates 1107
connectivity status of the local WebLM servers 967
console
    Tenant Management 39
contact
    add in default contact list 222
    modify 223
Contact Center
    reconfiguring 112
contact list member
    edit 226
contacts
    attach 224
Continue on Error 647
convert
    to stand-alone 83
convert .CADF xml file to MIB and trapd 882
converting .CADF xml file to MIB and trapd 881
converting .wav audio files 1064
converting .wav to .c11 audio file format 1064
converting to .c11 audio files 1064
cookie domain value
    SSO 1289
copy
    permission 158
Copy All From 158
Copy from Role 158
copy group 121
copying CM Agent template 1031
copying CM Endpoint templates 1034
copying permission mapping for a role 153
COR 646
Cord Length 660
corporate logo
    add 45
Corporate logo 37
Corporate Logo 45
correlation 731
COS
    Station 646
courses 26
Coverage After Forwarding 649
Coverage Criteria 624
Coverage Msg Retrieval 656
Coverage Path 623
coverage path,
coverage path, *(continued)*
    coverage; coverage path 621
Coverage Path 1 or Coverage Path 2 646
coverage path list
    coverage; coverage path list 621
Coverage Path Number 623
COVERAGE POINTS 626
coverage time-of-day,
    coverage; coverage time-of-day 627
coverage time-of-day list 627
create
    log harvesting profile 923
    new user profile 175
    profiles 834
    site 1121
    team 1121
    tenant 1121
    tenant organization 1121
    user account 175
    user provisioning rule 542
    virtual machine 1188
createCA 1101, 1298
create certificate signing request 1097
Create Discovery Profile
    field descriptions 837
create discovery profiles 834
create duplicate groups 121
create filter profiles 892
create log harvesting profile 923
create new Certificate Authority with SHA2 and 2048 1101
create new instance 833
Create New Profile if it doesn't exist for the user 184
Create New Profile page 930
Create Tenant page 1132
create user
    user provisioning rule 176, 177
create using user provisioning rule
    user profile 176
Creating a backup of the IP Office device configuration 746
creating a backupUCM and Application Serverdevice configuration 752
creating access profile 855
Creating a Certificate Signing Request 1097
creating an end entity 1098
creating a new communication address for a profile 205
creating a new port 856
creating an SNMP target profile 886
creating an SNMPv3 user profile 883
Creating certificate using certificate signing request 1100
creating data backup on remote server 780
creating detailed reports 999
creating discovery profiles 834
creating duplicate groups 121
creating duplicate user provisioning rule 544
creating duplicate users 181
creating groups 120
creating new user account 175

creating notification filter profile 889
Creating NRP 729, 730
Creating NRP groups 729, 730
creating SCS profiles 847
creating software library 1160
creating SRS profiles 847
creating system data backup on a local server 780
creating use profile 563, 565
creating user profile using user provisioning rule 176
creating user provisioning rule 542
creating user synchronization job 60
CS 1000
functionality limitations 98
CS 1000 account operations 907
CS 1000 alarms
configure 96
CS 1000 and CallPilot profile administration 215
CS 1000 configuration 96
CS1000 Presence users 219
CS1000 server
configuration 97
CSR
create 1097
CSR create 1097
Customized
interface 45
logo 45
Customized interface 45
Customized Interface field descriptions 48
customizing 1004
customizing reports 1004
custom prompt files
transfer 761
custom reports 998
custom role
add 148
delete 155
edit 154
custom roles 147
Custom roles 143
custom templates 1028
custom tenant administrator role
add 149
Cvg Enabled for VDN Route-To Party 623
CVG Path 630

D

dashboard
login 38
Dashboard
System Manager 37
data backup
create 780
remote server 780
data backup; schedule 781, 782
data backup from local server 784
database replication 69
Database size 787
Data entry warning in Excel 323
Data entry warning in Microsoft Excel 323
Data link error in Excel 322
Data link error in Microsoft Excel 322
data module list 698
Data Modules 698
data modules field descriptions
data modules; field descriptions 700
data replication 987, 988
data replication service 987
Data Restriction 656
Data Retention page 797
data retention rules 796
data retention rules; edit 797
data retention rules; modify 797
data retention rules; view 796
data retention rules service; access 796
Data Transport Config field descriptions 807
Data Transport Static Config page 810
date and time configuration; verify 1301
deactivate
secondary server 78
Default ACL 536
default contact
add contact list 222
default end entities
use new CA 1105
default login password for day one configuration of an IP Office device 740
Default Policy rule 536
default templates 1028
delete
communication profile 205
element 872
ESXi host 1183, 1202
global user settings import job on first error 346
location 1175
role 155
tenant 1127
user provisioning rule 544
delete a global user settings import Job 346
delete alarms 911
Delete ALL 911
delete an address 201
delete a user import job 338
Delete Confirmation Page 1027
delete contact addresses of a public contact 524
delete custom role 155
Deleted Trusted Certificate Confirmation page 1096
deleted user
restore 199
Deleted Users page 314
delete element 852
delete element access profile 845
Delete Element Confirmation page 872

delete element instance mapping 961
delete element instances 961
delete ESXi host 1183
delete ESXi host in vCenter 1202
delete filter profiles 892
Delete Group Confirmation page 134
delete IP Office endpoint profile of a user 221
Delete IP Office field description 880
Delete local WebLM page 978
delete Local WebLM server 978
delete location 1175
delete mapping 961
delete postal addresses of a public contact 522
delete public contact of a user 520
Delete Selected 911
delete SNMP Access profile 840
delete SNMPv3 user profiles 884
delete users in bulk 184
deleting
    upgrade jobs 1231
deleting access profile 856
deleting a communication address 207
deleting a communication profile 205
deleting agent
    agents; delete 593
deleting agents in bulk 594
deleting an announcement 604
deleting an audio file in IP Office system configuration template 1065
deleting an audio group 613
deleting an CM Endpoint profile 212
deleting an element access profile 845
deleting an element instance 961
deleting announcements 604
deleting anonymous profiles 905
deleting an SNMP target profile 888
deleting an SNMPv3 user profile 884
deleting a port 857
deleting a profile 925
Deleting a Remote Server 1009
deleting a shared address 533
deleting a station profile 215
Deleting a UCM and Application Server System Configuration template 1068
deleting audio groups 613
Deleting a VMPro Call Flow template 1076
Deleting a VMPro System Configuration template 1072
deleting bulk user edit jobs 184
deleting CM Agent template 1031
deleting CM Endpoint templates 1033
deleting completed jobs 1014
deleting contact addresses of a private contact 234
deleting contacts from the contact list 224
deleting coverage path
    coverage path; delete 622
deleting coverage time-of-day
    coverage time-of-day; delete 629
deleting data modules
    data modules; delete 700
deleting element instances 961
deleting endpoints
    removing endpoints 636
deleting files from software library 1165
deleting groups 122
deleting instances 961
deleting IP Office endpoint templates 1058
deleting IP Office system configuration templates 1062
deleting jobs 1014
deleting notification filter profile 890
deleting pending jobs 1014
deleting postal addresses of a private contact 232
deleting private contact of a user 230
deleting reports 1007
deleting scheduled backup job 783
deleting SNMP Access profile 840
deleting SNMP target profiles 888
deleting software library 1161
deleting subnetworks 844
deleting synchronization datasource, 54
deleting udp group 720
deleting uniform dial plan group 720
deleting uploaded audio file 769
deleting uploaded greeting file 769
deleting user provisioning rule 544
deleting user synchronization jobs 61
deleting vector directory number
    vector directory number; delete 617
deleting vector routing tables
    vector routing table; delete 619
department
    create 1121
    editing 1126
    team
        viewing 1126
    viewing
        team 1126
deploy
    Branch Session Manager 1188
    Communication Manager 1188
    Session Manager 1188
    System Manager 1188
    Utility Services 1188
deploy application 1173
deploy Avaya Aura 7.0 application 1188
Deploying an OVA file
    utility services 1186
deploy OVA 1188
Desktop Video Conferencing 652
determine System Manager that manages GR-aware element 851
device configuration 751, 752
device configurationUCM and Application Server 753
device list 835
Direct IP-IP Audio Connections

Direct IP-IP Audio Connections *(continued)*
Attendant Console 656
directory synchronization 49
Disable Confirmation page 1024
disabling
Geo Redundancy replication 76
Disabling
pending jobs
completed jobs 1015
disabling centralized licensing 962
disaster recovery 116
discover
device 835
discover elements 834
discovering elements 834
discovering SCS servers 847
discovering SRS servers 847
Discover Now 836
Discover SCS server
field descriptions 849
discover SCS servers 847
Discover SRS server
field descriptions 849
discover SRS servers 847
discovery
profiles 834
Discovery Job Status 836
discovery profiles
create 834
Discovery Profiles 836
field descriptions 836
disk space for
System Manager backup 778
display 1088
Display Client Redirection 656
Display Language 650
DND/SAC/Go to Cover
All 625
Coverage Path 625
Don’t Answer 625
domain control 679
domain control SIP endpoints
enable reachability 679
download
harvested log files 927
downloading
software 774, 1238
Downloading 754
downloading an announcement 606
downloading announcements 606
downloading audio groups 613
Downloading Excel template 326
downloading harvested log files 927
Downloading IP Office System Configuration 741
downloading reports 1005
downloading the .pem file 1281
downloading the .pem file to Communication Manager 1281
downloading the system manager certificate 1280
downloading the voice mail call flow 764
downloading upgrade files 1274
download manager
downloading software releases 1274
download software 1169, 1186
DRS 987, 988
DRS client audit 988
DRS clients 988
duplicate
UPR 544
user provisioning rule 544
Duplicate Group page 134
duplicate groups; create 121
Duplicate User Provisioning Rule
field descriptions 545
duplicating an endpoint 635
Duplicating a VMPro call flow template 1077
Duplicating a VMPro System Configuration template 1073
duplicating CM Agent template 1031
duplicating CM Endpoint templates 1034
duplicating IP Office endpoint templates 1058
duration
backup and restore 787
CS 1000 account operations 907
DVC 652

E

edit
communication profile password policy 538
custom role 154
ESXi host 1180, 1202
grace period 815
location 1174
scheduled job 1022
site 1126
virtual machine 1190
Edit Address page 240, 534
edit agent data in bulk,
agents; bulk edit 594
Edit Appender page 940
edit assignment of a license file 960
edit authentication scheme 1109
Edit Common Console Profile page 814
edit Communication Profile Password Policy
field descriptions 539
edit contact in a contact list 223
edit contact list member page 226
Edit Discovery Profile
field descriptions 837
edit element access profile 845
edit element instances 961
Edit Element page 865
edit elements 1225
edit endpoint
field descriptions 644

edit endpoint extension
  field descriptions 669
edit endpoint templates
  field descriptions 644
edit ESXi host 1180
edit ESXi host in vCenter 1202
edit filter profiles 892
Edit Group page 132
Edit Host 1183
editing
  department 1126
  team 1126
  tenant 1126
Editing
  pending jobs
    completed jobs 782, 1014
editing a coverage path
  coverage path; edit 622
editing agent data
  agents; edit data 593
editing an announcement 604
editing an audio group 612
editing an element access profile 845
editing an IP Office endpoint profile 220
editing announcements 604
editing an SNMP target profile 887
editing an SNMPve user profile 883
Editing a Remote Server details 1008
editing a security configuration 744
editing a system configuration 741
Editing a UCM and Application Server Configuration template 1067
Editing a UCM and Application Server security configuration 759
Editing a UCM and Application Server system configuration 758
editing audio groups 612
editing authorization code
  authorization code; edit 713
Editing Automatic Alternate Routing Digit Conversion data
  Automatic Alternate Routing Digit Conversion; editing data 691
editing automatic route selection digit conversion data
  automatic route selection digit conversion; edit data 693
editing automatic route selection toll data
  automatic route selection toll; edit data 697
Editing a VMPro call flow template 1075
Editing a VMPro System Configuration template 1071
editing class of service data 708
editing class of service group
  class of service group; edit 715
editing CM Agent template 1030
editing CM Endpoint templates 1032
editing communication profile password policy 538
editing coverage time-of-day
  coverage time-of-day; edit 628
editing data modules
editing data modules *(continued)*
  data modules; edit 699
editing element instances 960
editing IP Office endpoint templates 1057
editing IP Office system configuration templates 1061
editing notification filter profile 890
Editing Off PBX Configuration Set 680
Editing Off PBX Endpoint Mapping 684
editing password policies 43
editing Remote Servers 1008
Editing report 1003
Editing report parameters 1003
editing session properties 44
  field descriptions 47
editing SNMP Access profile 839
editing SNMPv3 user profiles 883
editing software library 1161
editing subsciber templates CMM; field description 1051
editing subscribers CMM field description 574
editing subscribers MM field description 577
editing subscriber templates Messaging
  field descriptions 1048
editing subscriber templates MM; field description 1053
editing tenant 1126
editing the logon warning banner 44
editing the properties of an element instance 960
editing the select all attribute 585
editing the voice mail pro call flow 763
editing the voice mail pro system configuration 766
editing UDP entries 724
editing UDP Group 719
editing Uniform Dial Plan Group 719
editing vector directory number;
  vector directory number; edit 617
editing vector routing table 619
editing xmobile configuration
  xmobile configuration; edit 686
edit location 1174
Edit Location 1178
edit logger 937
Edit Logger page 939
edit password policies
  field description 45
Edit Private Contact List page 236
Edit Profile:Alarming UI page 812
Edit Profile:Communication System Management Configuration page 802
Edit Profile: Configuration page
  Inventory 805
Edit Profile:HealthMonitor UI page 816
Edit Profile: Inventory page 805
Edit Profile:Licenses page 817
Edit Profile:Logging page 818
Edit Profile:Logging Service page 819
Edit Profile:Shutdown page 815
Edit Profile: Trust Management field description 826
Edit profile Messaging field descriptions 806

Edit Profile System Manager page 811
Edit Public Contact List page 526
Edit Remote Server field descriptions 1009
Edit Scheduler Profile page 823
edit SNMP access profile 839
edit synchronization datasources 53
Edit Upgrade Configuration 1215
edit user
  user provisioning rule 177
Edit User Profile 277
Edit User Provisioning RuleView User Provisioning Rule
  field descriptions 545
edit users in bulk 183, 185
Edit vCenter 1203
edit virtual machine 1190
EJBCA 1079, 1102
EJBCA to Sub CA 1102
element
  add 1224
  create 833
  create Communication Manager 850
  create Messaging 850
  delete 852, 872
  edit 852
  import 833
  new 833
  view 852
Element
  Cut Through 680
element access profile
  add 845
  delete 845
  edit 845
Element Access Profile Management 846
Element Cut-Through 587, 631
Element Cut-Through; access 631
Element Cut-Through field description 631
element data export 853
element export from System Manager CLI 853
element instance
  delete 961
  edit 960
  edit properties 960
  remove 961
element instance field description 961
element management 831
Element Manager
  redirect CallPilot user 216
  redirect CS 1000 user 216
elements
  discover 834
  import 872
  refresh 1167
Elements Geographic Redundancy manageability status
matrix 89
elements upgrade
  target release 1206
element upgrade 1212
email configuration for reports 1006
Emergency Location Ext 646
EMU Login Allowed 659
enable
  Multi Tenancy 810
  password strength policy 41
enable self provisioning 173
enabling 958
  Geographic Redundancy replication 75
  Multi Tenancy 1121
Enabling
  pending jobs
    completed jobs 1016
enabling two-way TLS 1286
encrypt passwords 333, 334
end entry
  create 1098
endpoint
  adding dependencies 728
  change parameters globally 639
  duplicate 635
  save as template 636
endpoint administration
  endpoint management
    endpoints 632
Endpoint editor
  permissions 165
endpoint extension 669
  edit 636
  editing endpoint extension 636
endpoint list 643
Endpoint options 727
endpoints
  add 633
  assign range 164
  change set type of endpoints 673
  field-level RBAC 169
  range 163, 164
  releasing 641
  remove dependencies 728
  swap 670
Endpoints
  Element Cut Through 680
endpoints; bulk add
  bulk add endpoints 637
Endpoints; bulk delete 638
endpoints; busy out
  busy out endpoint 641
endpoints; delete 636
endpoints; edit
  editing endpoints 634
endpoints; status
  endpoint status 640
endpoints; testing
  testing endpoints 642
endpoints; view

endpoints; view *(continued)*
- viewing endpoints 635

endpoint template list 1038
endpoint template versions 1028
end user change communication profile password 173
end user self provisioning 173
Enhanced Call Fwd 661
enrollment password 1083
- generate 1083

Enrollment Password page 1093
ensuring certificate response 1104
Enterprise Configuration page 972
Enterprise Java Beans Certificate Authority 1079
enterprise licensing
- configure 963

Enterprise Usage page 980
environment variable
- Windows XP 737

environment variable; AdminLite installation 738
error codes 671
error codes for failout results 671
ESXi host
- add 1179
- add location 1202
- delete 1183
- edit 1180
- manage 1202
- nonmanage 1202
- remove location 1202

ESXi host Gateway
- change 1181
- edit 1181

ESXi host in vCenter
- add 1201
- delete 1202
- edit 1202
- remove 1202

ESXi host IP address
- change 1181
- edit 1181

ESXi host map to unknown location 1183
ESXi host password
- change 1182

ESXi hypervisor 31
Event processor page 803
Example
- bulk import and export of user by using Excel file 319

Excel
- bulk import 326
- Data entry warning 323
- Data link error 322
- export 317
- import 317

Excel file
- bulk import and export of user 319
- export 794
- import 794

Excel file *(continued)*
- import users 504

Excel template
- download 326

export
- communication profile 328
- contacts 328
- element 853
- global user settings 341
- user data 317, 323
- user data to Excel 317

export alarms 910
export CM Agent profile 317
export CM station data 317
export elements from System Manager CLI 853
export global settings 342
exporting CS 1000 user data 563, 565
exporting the user data 559
export logs 942
exportUpmGlobalsettings command, 343
export users 327
- System Manager UI 328

Export Users 511
Extension
- Station 645

extension pack
- deployment verification 1288

external authentication 1108
external server; system requirements 1167
external server for upgrade 1153

F

failback policy 771
Favorite 662
feature options
- voice mail number 659

Feature Options 648
field description
- anonymous communication profiles 906
- password policies 45
- SNMP Access Profile 841
- Subscribers (CMM) 574

field descriptions
- Add Communication Manager 876
- Add Mapping 157
- Add Trusted Certificate page 1094
- Application Server System Configuration template 1070
- ars toll 697
- Assigned Users 158
- Auto answer 672
- automatic route selection toll 697
- change password 1185
- Choose Address 204
- Choose Group 141
- Communication Manager Backup Configuration 1259
- corporate logo 48

field descriptions *(continued)*
Create Discovery Profile 837
Create Tenant 1132
customized interface 48
Data Transport Config 807
Deleted Users page 314
Delete Group Confirmation 134
Discovery Profiles 836
Duplicate User Provisioning Rule 545
Edit Discovery Profile 837
edit endpoint extension 669
Edit Group 132
Edit Host 1183
Edit Location 1178
Edit Profile:SMGR 811
Edit Public Contacts 526
Edit User Provisioning Rule 545
Element Access Profile Management 846
Export Users 511
Filter Profiles 892
Group Management 127
Hosts 1175
Import Global Settings page 509
IP Office System Configuration template 1063
Locations 1175
Manage Elements 862
Map vCenter 1203
Modify Access Profile Entry 846
Move Group 135
New Group 129
New Host 1183
New Location 1178
New Public Contact List page 528
New User Profile 257
New User Provisioning Rule 545
Notification Filter Profiles 892
Periodic cleanup of reports 804
replace identity certificates 1091
Resource Synchronization 136
Roles 155
session properties 47
SNMP Access Profiles 840
Software inventory 1253
Subnet Configurations 844
synchronization job history 62
Tenant Management 1132
TrapListener 824
UCM and Application Server System Configuration template 1070
UnAssign Roles 316
Unified Communications Module System Configuration template 1070
Upgrade Configuration 1215
upgrade management 1212
User Bulk Editor 185
User Provisioning Rules 185, 545
User Restore Confirmation Page 315

field descriptions *(continued)*
user synchronization datasource 54
user synchronization jobs 62
View Group 131
Viewing job summary 63
View Profile: SMGR 810
View Trust Certificate 1096
View User Provisioning Rule 545
Virtual Machines 1175
VM Deployment 1192, 1196
field level RBAC 166
Communication Manager objects 166
field-level RBAC in endpoints 169
file download manager 1170
file replication 69
File transfer field description 762, 769
file transfer settings; announcements 607
filter
alarm 888
informs 888
notification 888
traps 888
filtering alarms 911
filtering announcements 608
filtering class of service list 709
filtering Communication Manager objects
using filters; Communication Manager objects 591
filtering groups 125
filtering jobs 1013
filtering log harvesting profiles 928
Filtering log harvesting requests 928
filtering logs 942
filtering resources 126, 139
filtering SNMPv3 user profiles 884
filtering subscribers
using filters; subscribers 568
filtering target profiles 886
filtering templates
filtering endpoint templates 1028
filtering subscriber templates 1028
using filters; templates 1028
filter profile
assign to serviceability agent 891
create 889
unassign from serviceability agent 891
Filter Profiles
field descriptions 892
filter users 194
firewall basics 1303
firewall implementation in System Manager 1303
Floor
Station 660
Forwarded Destination 661
forward the secondary alarms to primary System Manger 915
FQDN 1296
change 1290
changeIPFQDN 1297

FQDN and IP address change on Geographic Redundancy 1288
FTP Configuration (F) 1162
FTP server
    configure as remote 1155
    install 1155

G

G430 gateway
    add 862
G450 gateway
    add 862
gateway protocol matrix 1277
General Configuration Details 1215
General Guidelines and Capabilities of User Provisioning Rules 541
General Options 646
generate identity certificates 1106
generate report
    field description 1001
generate report field description 1001
generate test alarm 914
generate test alarms 913
generateTrapdAndMibUnix 882
generateTrapdAndMibUnix.sh 881
generating basic reports 1000
generating certificate keystore 1099
generating detailed reports 999
generating test alarms 914
geographical redundancy 113
Geographical redundancy 69
Geographical Redundancy 73, 81, 113–116
Geographic Redundancy
    .... 65, 70, 78, 83, 85, 86, 851, 858, 988, 1288
    backup and restore 778
    disable 76
    enable 75
    prerequisites 69
Geographic Redundancy field descriptions 85
Geographic Redundancy key tasks 71
Geographic Redundancy licenses 66
Geographic Redundancy replication 69
Geographic Redundancy terminology 67
Geo Health 83
Geo Redundancy 76
Get
    Company ID 1149
get inventory 1236
Get inventory 773
Global Endpoint Change 639
global endpoint parameter change 639
global user settings import job
    abort 345
GLS 119
graceful shutdown 814, 815
Grace Period
Grace Period *(continued)*
    edit 815
    view 814
granular RBAC 160
GR-aware element
    manage 851
greeting files
    transfer 767
GR failover 91
GR Health field descriptions 86
group 729, 730
    copy 134
    duplicate 134
Group and Lookup Service 119
Group List 661
Group management 119
Group Management page 127
group membership 125
Group Membership 668
Group Name 157
groups
    copy 121
    create 120
    defined 668
    delete 122
    duplicate 121
    filter 125
    modify 121
    move 122
    view 120
GR-unaware elements 88

H

H.320 Conversion
    Attendant Console 657
H.320 Desktop Video Conferencing 652
H323 and SIP passwords 173
hardware and software prerequisites on the primary and secondary servers 69, 70
Hardware support 1271
Harvest Archives page 933, 935
Harvest Criteria Edit page 931
harvested log files; download 927
Headset 660
health monitor 816
health monitoring
    timeout interval 84
Health Monitor service 83
Hierarchy in communication profile worksheets 321
history
    synchronization job 62
Holiday After Coverage 624
Holiday Coverage 623
Holiday Table 624
host
    monitoring 1200

Host
  update 1185
Hosts 1175
HTTP/HTTPS Configuration (H) 1162
Hunt-to Station 651

I

identity certificate 1089, 1102
identity certificates 1088
  renew 1089
  replacing 1088
Identity Certificates page 1090
identity certificate updates
  confirm 1107
Idle Appearance Preference 657
impact of change in FQDN and IP address on Geographic Redundancy 1288
implicit permissions for Communication Manager objects . 161
implicit permissions for range 161
import
  elements 872
  user data 317, 323
  user data from Excel 317
Import as PEM certificate 1085
import CM station data 317
import CS1000 user data to User Management 562
import element; 833
Import Elements 872
Import from existing certificates 1085
Import from file 1085
Import Global Settings page 509
importing CS1000 Subscriber Manager data 562
importing CS 1000 Subscriber Manager data 563, 564
importing CS 1000 user data 563, 565
importing the Subscriber Manager data 562
importing the user data 559
import job on the Scheduler page
  view 338
import of users 326, 329
Import Status page 875
import the Subscriber Manager data 555, 557
import user considerations 335
import user data to User Management 554
import users 324
Import Users 504
Import using TLS 1085
Inactive session termination policy 42
incremental synchronization
  synchronizing Communication Manager data 899
information
  to create Communication Manager 850
  to create Messaging 850
infrastructure enhancements 35
initializing synchronization
  synchonizing Communication Manager data 898
initiate failback
initiate failback *(continued)*
  IP Office 772
Initiate failback 771
Initiating failback 771
install
  Application Enablement Services 1142
  Avaya Aura applications 1142
  Avaya Aura Media Server 1142
  Branch Session Manager 1142
  Communication Manager 1142
  Engagement Deployment Platform 1142
  patch from CLI 1298
  SAL 1142
  SDM 1142
  service pack from CLI 1298
  Session Manager 1142
  Solution Deployment manager client 1142
  System Manager 1142
  WebLM 1142
Installed Patches 1211
Installed Patches field descriptions 1198
install FTP server 1155
Installing and configuring an HTTP server as a remote server 1154
Installing and configuring an SCP or SFTP server as a remote server 1158
install license file 951
Install License page 955
Install on Same server 1230
install patches 1210
install patch from CLI 1298
install service pack from CLI 1298
install services packs 1210
install software patches 1210
Install System Manager patch 1199
Install System Manager patches 1224
Integrated Management transition 998
Internet Explorer
  compatibility view setting 36
Introduction 90
inventory
  collection 773
  refresh elements 1167
IP address 1296
  change 1290
IP address and FQDN change on Geographic Redundancy servers 1291
IP Audio Hairpinning
  Signaling Group 657
IP Office 740, 741, 745, 747
  about system configuration 740
  add device 879
  delete 880
  deleting files 769
  initiate failback 771
  overview 733
  reconfigure 111, 112

IP Office *(continued)*
security configuration 743
start 735
synchronizing system configuration 899
transferring files 767
upgrade 773, 775
user management 111
IP Office; configure 800
IP Office Application Server
synchronize 900
IP Office backup
field descriptions 747
IP Office configuration 109, 110
IP Office configuring for GR 110, 111
IP Office device
transfer files 768
unlock 735
IP Office device configuration
restore 746
IP Office device configuration backup 745
IP Office device configuration restoration 745
IP Office endpoint profile 219
delete 221
edit 220
view 220
IP Office endpoint template
view 1057
IP Office endpoint template field description 1059
IP Office endpoint templates
add 1056
delete 1058
edit 1057
field description 1059
remove 1058
upgrade 1059
IP Office failback field descriptions 772
IP Office field descriptions 744, 769
IP Office GR configuration 109
IP Office GR configuration in Active-Active scenario 111
IP Office GR configuration when primary nonfunctional 110
IP Office profile field description 801
IP Office Restore field descriptions 749
IP Office security configuration field description 744
IP Office security configuration field descriptions 744
IP Office System Configuration
field description 742
manage audio files 1063
IP Office System Configuration field descriptions 742
IP Office system configuration template
upload audio files 1064
IP Office System Configuration template
field descriptions 1063
IP Office System Configuration template field descriptions 1063
IP Office system configuration templates
add 1060
convert .wav to .c11 1064
IP Office system configuration templates *(continued)*
convert to .c11 1064
delete 1062
delete audio files 1065
edit 1061
view 1061
IP Phone Group ID 655
IP Softphone 657
IP Video 656

J

Jack 660
Job Details page 507, 513
Job Scheduling -Edit Job page 1022
Job Scheduling -On Demand Job page 1024
Job Scheduling -View Job page 1021
job summary
synchronization job history 63
Job summary 63
JRE requirement 734

K

KERBEROS 1108
Kerberos server 1111
key features
bulk export 323
bulk import 323
key size 2048 1101
key tasks
Geographic Redundancy 71

L

LDAP 1108
LDAP directory server 49–51, 177
LDAP replication 69
LDAP server; provision 1110
legal notice
Library Server Details (L) 1162
license capacity; view 953
license file 950
add mapping 960
install 951
license file; uninstall 954
license file installation 955
license files and elements 959
License management 100
License management for Conferencing 107
License management for Contact Center 112
Licensing
Geographic Redundancy 66
Life cycle management 1173
limitations
directory synchronization 51

Limitations of CallPilot 98
Limitations of CS 1000 98
Linkage 624
Linux-based CS1000 servers
  configuration 97
Linux Operating System upgrades 1242
  preupgrade check 1242
list of XML Schema Definitions and Sample XMLs for bulk import 347
list usage extension; announcements 608
list usage extension in vector directory number
  vector directory number; list usage extension 617
Localized Display Name 634
Local Survivable Processor(LSP) 1162
local WebLM 975
location
  add 1174
  delete 1175
  edit 1174
  view 1173
Location 648
Locations 1175
Lock Messages 646
lockout policy
  password 42
Log; log settings 936
log details; view 942
log file; search for text 926
Logged off/PSA/TTI
  Coverage Path 626
logger
  edit 937
logging 920
Logging Configuration page 937
logging on to System Manager
  admin 38
Logging page 943
logging service 920
log harvest; access 923
log harvester overview 922
Log Harvester page 929
log harvesting 922
log harvesting profile
  create 923
log harvesting profile; view details 924, 929
log harvesting profiles; filter 928
log harvest requests; filter 928
login password
  reset 848
login profiles
  overwrite 848
  overwriting profiles on devices 848
log into System Manager 38
logo
  add 45
Logo 45
logon banner 44
logon information
  admin 38
logon warning banner 43
  edit 44
logs; export 942
logs; log viewer 942
logs; search 943
Log Settings 936
logs for Conferencing 108
Logs Settings service; access 936
log types 921
log viewer 920
Log Viewer 942
Loss Group 652
LWC Activation 657
LWC Log External Calls 658
LWC Reception
  Agent Login ID 653

M

MAC address of server 963
mailbox administration
  subscriber management 566
Mailing reports 1007
maintenance
  clear amw all 642
manage
  applications 831
  elements 831
  GR-aware element 851
  identity certificate 1089
  tenant 1125
  trusted certificate 1087
Manage
  System Manager upgrades 1224
manage applications 831
manage audio field description 1065
manage certificates 1079
managed elements
  changing System Manager IP address 1291
manage elements 831, 858
  Geographic Redundancy 851
Manage Elements field descriptions 862
Management interface 33
manage Presence access control lists 536
manage public contact list 519
manage resources 136
manage shared address 531
Manage Software 1204
manage software library files field description 1166
manage users 171
Managing NRP 731
Managing NRP groups 731
managing resources 136
managing SNMPv3 user profiles 894, 895
managing software

managing software *(continued)*
IP Office ... 773
Unified Communications Module (UCM) and Application Server ... 773
managing target profiles ... 895
managing user profiles ... 895
Manual addition of elements ... 832
map
permission ... 158
permission from template ... 159
map ESXi host to unknown location ... 1183
map permission ... 153
map permissions
using templates ... 152
mapping
add ... 157
mapping elements and license files ... 959
Map vCenter ... 1201, 1203
Map vCentre ... 1203
Media Complex Ext ... 654
media server ... 609
Meeting Exchange configuration ... 99
Meeting Exchange element configuration ... 100
memory requirement ... 1243
Message Lamp Ext ... 646
messaging class of service ... 565
Messaging configuration ... 102
Messaging configuration in GR failback ... 103
Messaging configuration in operational mode ... 102
Messaging configuration in split network ... 104
Messaging configuration when primary is nonoperational . 103
messaging COS ... 565
messaging data
synchronize ... 901
Messaging field description ... 1048
Messaging field descriptions
add subscriber ... 569
Messaging profile
edit ... 806
view ... 806
MIB.properties ... 882
MIB tool ... 881, 882
MIBTOOL.jar ... 882
MIBXMLTAGS.properties ... 882
Microsoft Active Directory certificate ... 1084
modify
address ... 201
communication address ... 206
element access profile ... 846
port ... 857
user provisioning rule ... 543
Modify Access Profile Entry ... 846
modify appender ... 939
modify a user address ... 201
modify details of a private contact ... 230
modify details of a public contact ... 520
modify element ... 852
modify FQDN
primary System Manager ... 1293
secondary System Manager ... 1294
Modify FQDN
secondary System Manager ... 1295
modifying a CM Endpoint profile ... 210
modifying a contact address of a private contact ... 234
modifying a CS 1000 or CallPilot profile ... 218
modifying a local WebLM server configuration ... 966
modifying a managed element's IP address and FQDN .. 1290
modifying a messaging profile ... 213
modifying an access profile ... 856
modifying an appender ... 939
modifying an IP Office endpoint profile ... 220
modifying a port ... 857
modifying a postal address of a public contact ... 522
modifying a shared address ... 533
modifying contact in a contact list ... 223
modifying data retention rules ... 797
modifying default end entities ... 1105
modifying FQDN
System Manager ... 1290
modifying groups ... 121
modifying IP address
System Manager ... 1290
modifying postal address of a private contact ... 231
modifying SNMPv3 user profiles ... 883
modifying the communication address ... 206
modifying the details of a public contact ... 523
modifying user account ... 180
modifying user provisioning rule ... 543
modify IP address
primary System Manager ... 1293
secondary System Manager ... 1294, 1295
Modify local WebLM page ... 976
monitoring
host ... 1200
virtual machine ... 1201
VM ... 1201
Mounting ... 660
Move Group page ... 135
move primary System Manager server ... 113, 114
moving an announcement ... 607
moving announcements ... 607
moving groups ... 122
MPC firmware
update ... 1276
Multi Device Access ... 208
Multimedia Early Answer ... 658
Multimedia Messaging ... 112
multiple SIP endpoints
register ... 208
multiple users
assign groups ... 198
Multi Tenancy ... 1120, 1121, 1125–1127
Avaya SIP AST endpoints ... 1128
Communication Manager ... 1128, 1129

Multi Tenancy *(continued)*
- enable 810
- enabling 1121
- RBAC 1129
- scheduler 1129
- user management 1129
- user provisioning rule 1129

Multi Tenancy for Communication Manager 1129
Multi Tenancy for Communication Manager objects 1128
Music SourceMusic Source 659
Mute Button Enabled 658
MWI Served User Type 649

N

native name 634
network parameters
- change 1184

new
- role 156

New Element page 865
new features
- Communication Manager 34

New Group page 129
New Host 1183
new identity certificates
- System Manager 1106

New in this release 31
New Location 1178
New log harvesting profile 930
New Private Contact List page 235
new profile
- create 184

New Public Contact List page 528
new report field description 1001
new reports 999
New User Profile page 257
New User Provisioning Rule
- field descriptions 545

New vCenter 1203
Next Path Number 624
nodes; remove 991
non sip endpoints 678
non-station objects; view
- Communication Manager objects; view 590

Notification filtering 888
notification filter profile
- create 889
- delete 890
- edit 890
- view 890

Notification Filter Profiles
- field descriptions 892

notification ID 890
notification IDs 892
notify sync feature; overview 1279
notify sync on Communication Manager 1283

NRP groups 731
NRP sync 730
NRP sync feature 730
NTP server
- configure 1302

Number of Rings 626

O

Obtaining Microsoft Active Directory certificate 1084
obtain the license file 950
Off PBX Configuration Set
- Edit 680
- field description 681
- View 680

Off PBX Configuration Set field descriptions 681
Off PBX endpoint mapping
- add 683

Off PBX Endpoint Mapping
- edit 684
- field description 684
- view 684

Off PBX Endpoint Mapping field description 684
on-demand job 1010
Out of Band Management 33
Overview 88
overwriting login profiles 848

P

parameters 1003
parent group 142
password
- change 1185

Password aging policy enforcement 41
password change
- Appliance Virtualization Platform host 1182
- ESXi host 1182

password history enforcement policy 42
password lockout policy enforcement 42
password policies
- edit 43

password policies field description 45
password policy 538, 1182
- communication profile 538

password policy; logon warning banner 43
password strength policy enforcement 41
peak usage; view 953
peak usage for a licensed product 953
pending jobs
- view 1012

pending jobs; stop 1016
pending jobs; view 1012
Pending Jobs page 1017
Per Button Ring Control 658
performing
- Pre-Upgrade Check 1240

Performing a CM Audit 902
Periodic cleanup of reports 804
Periodic Status 985
periodic status of master and local WebLM servers 969
permission
    copy 158
    map 158, 159
permission mapping 152, 158, 159
permissions
    Scheduler 1011
    Solution Deployment Manager 150
Personalized Ringing Pattern 650
Personal List 661
Per Station CPN - Send Calling Number 649
PLDS access 1148
PLDS access to Avaya 1148
Point1, Point2, … 626
port
    modify 857
Port 865
    Station 645
Precedence Call Waiting 658
preparing CS 1000 Subscriber Manager data for import to System Manager 563
prerequisite for changing FQDN 1288
prerequisite for changing IP address 1288
prerequisites 69–71
Presence access control lists (ACLs) 536
Presence ACL 536
Presence communication profile administration 208
Presence Server
    configuration 100
Pre-Upgrade 1241
preupgrade check 1242
    applications 1171
Pre-Upgrade Check 1240, 1241
pre upgrade checks
    System Platform upgrades 1242
Preupgrade configuration 1171
Preupgrade Configuration 1171
preupgrade job status 1231
preupgrade status 1244
primary System Manager
    change FQDN 1292
    change IP address 1292
private contact
    add a contact address 233
    modify details 230
Private Contact 235
Problems in managing Session Manager 6.1 or 6.2 using System Manager 6.2 92
profile
    delete 925
Profile 663
Profile Criteria View page 932
profiles
    discovery 834
Profiles 1114
Profile Settings 663
Protocol consideration 1115
protocol matrix for upgrades 1277
protocol requirements to configure remote server 1154
protocol support
    software library 1154
provision
    users 540
provisioning the Kerberos server 1111
provisioning the LDAP server 1110
provisioning the radius server 1110
provision LDAP server field descriptions 1112
provision Remote Identity Provider 1117
provision the authentication servers 1110
public contact
    add 519
    add contact address 523
    add postal address 521
    choose a shared address 522
    delete 520
    delete contact address 524
    delete the postal address 522
    modify details 520
    view details 521
public contacts 171, 530
Public Contacts
    field descriptions 524
Public interface 33

Q

querying usage of feature licenses for master and local WebLM servers 969
Query Usage page 981
Quick Navigator 37
quick start to importing users 514

R

RADIUS 1108
range 160
    endpoints 164
Range in endpoints 163
RBAC 143
    built-in roles 143
    custom roles 147
RBAC for Conferencing 108
Ready for Upgrade 1259
receiving certificate response 1104
reconfiging Conferencing 108
reconfiguing Conferencing 107, 108
reconfiguing IP address and FQDN for Conferencing 108
reconfigure Conferencing 108
reconfiguring AES 112
reconfiguring Conferencing 107
reconfiguring Contact Center 112

reconfiguring IP Office 111
reconfiguring Visualization, Performance, and Fault Manager 112
recover primary server from disaster 116
redirect
    CallPilot user to Element Manager 216
    CS 1000 user to Element Manager 216
redirecting CallPilot user to Element Manager 216
redirecting CS 1000 to Element Manager 216
Redirect Notification 658
reestablish
    connection 1200
Reestablish Connection 1175
refresh elements in inventory 1167
refresh elements job status 1231
register
    multiple SIP endpoints 208
Reimporting SSO cookie domain value 1289
related documentation 25
releasing endpoint 641
remote backup server supported
    ciphers 788
    key exchange algorithms 788
    mac algorithms 788
Remote Identity Provider 1117
Remote Identity Provider; provision 1117
remote library 1162
Remote Off-hook Attempt 673
Remote Server
    add 1008
    delete 1009
    edit 1008
    view details 1008
Remote Server configuration
    field descriptions 1009
Remote Softphone Emergency Calls 651
remove an address 201
remove assigned elements 855
remove association between IP Office endpoint profile and user from properties file 222
remove a user from groups 198
remove endpoint dependencies
    field description 729
remove endpoint reference field description 729
remove ESXi host 1202
remove location from host 1202
remove replica node from queue 991
remove roles 197
remove user account 182
removing a local WebLM server 966
removing an appender from a logger 939
removing an association between a subscriber and a user 214
removing a node 991
removing assigned resources from group 127
removing association between an endpoint and a user 212
removing deleted users from database 182
removing dependencies of endpoints 728
removing license file 954
removing references to endpoints 728
removing trusted certificates 1087
removing users from role 153, 200
renewing identity certificates 1089
repairing a replica node 990
replace
    primary System Manager server 113
    secondary System Manager server 116
Replace Identity Certificate page 1091
replace identity certificates
    field descriptions 1091
replace primary System Manager server using secondary System Manager 115
replace System Manager servers 113
replacing identity certificates 1088
replica group; remove nodes 991
replica group; remove replica node from queue 991
replica groups; view 989
Replica Groups page 991
Replica Nodes page 992
replication
    database 69
    file 69
    LDAP 69
Replication Node Details page 995
report 1003
Report alarm properties 804
report list
    field description 998
report list field description 998
reports 998, 1004
    basic 1000
    delete 1007
    detailed
        generate 999
    download 1005
    email 1007
    email configuration 1006
    new
        generate 1004
    rerun 1004
reports field description 1006
reports history field description 1006
Reports output directory 804
Re run
    reports 1004
Re running reports 1004
resetting the password 848
resolving anonymous profiles 904
resources
    filter 126
    group 123
    manage 136
    remove 127
    search 124

resources *(continued)*
search group 125
resources; filter 139
resources; search 138
resources; synchronize 123
Resources page 139
Resource Synchronization page 136
restart
virtual machine 1192
restart virtual machine from SDM 1192
Restoration 745
restore 777
primary System Manager 78
primary System Manager server 114–116
Restore 745
restore backup
remote server 785
restore backup from remote server 785
Restore Confirmation Page 315
restore data backup 784
restore deleted user 199
Restoredevice configuration 753
Restore of UCM and Application Server 752
restore on System Manager Geographic Redundancy 778
Restore page 792
restore system backup from local server 784
restoring all announcements 606
restoring announcements 606
restoring announcements; all 606
restoring audio groups 613
restoring audio groups; field description 614
restoring IP Office device configuration 746
restoring the backup data through CLI 786
restoring through command line 786
Restrict Last Appearance 659
retrieving the System Manager CA certificate 1092
Rng 627
role
add 156
assign users 152
copy permission mapping 153
delete 155
details 156
edit 154
new 156
unassign users 153, 200
role based access control 143
Role Details 156
Role page 155
roles
built-in 143
RBAC 147
remove 197
Service Provider Administrator 143
System Administrator 143
Tenant Administrator 143
Roles 143
Room
Station 659
rules 540
runRTSCli.sh 853

S

SAC/CF Override 661
Salient features of SAML implementation in System Manager 1115
same host installation 1230
SAML 1114
SAML authentication 1113
SAML implementation 1114, 1115
SAML protocol 1113
SAMP/MPC firmware
update 1276
SAMP firmware
update 1276
sample scenario
range feature 163
sample upgrade scenario 1248–1250, 1269, 1270
sample upgrade workflow 1248–1250, 1269, 1270
sample XML file for a user with SIP Communication Profile 518
sample XML with a single user profile 515
Save as template 636
saving an announcement 605
saving an endpoint template 636
saving announcements 605
saving CM translations 901
saving Communication Manager trnaslations 901
Saving Voice Mail Pro call flow as a template 764
Saving Voice Mail Pro system configuration as a template 766
schedule
on-demand job 1010
schedule a user import job 335
Schedule Backup page 791
schedule data backup; remote server 782
scheduled backup job
deleting 783
Schedule Discovery 836
scheduled job
edit 1022
scheduled jobs
completed 1019
scheduler 1010
Scheduler
permissions 1011
scheduler; access 1011
scheduler service 1010
scheduling a data backup on a local server 781
scheduling a data backup on a remote server 782
scheduling a global user settings import job 343
scheduling a user synchronization job 61
SCP Configuration (S) 1162

SDM
  installation 1142
SDM client 1141
SDM client capabilities 1145
SDM client dashboard 1144
search
  Communication Manager objects 585
Search Archives page 934
searching Communication Manager objects 585
searching contacts on Avaya SIP AST endpoints 1128
searching for alarms 912
searching for a text in a log file 926
searching for logs 943
searching for resources 124, 125, 138
searching logs 943
search resource 139
search users 195
secondary server 76, 78
secondary server alarms
  view 915
secondary System Manager
  modify FQDN 1294
  modify IP address 1294
secondary System Manager failure 116
Security Code 647
security configuration
  edit 744
  view 743
security settings 44
select all attribute; edit 585
selected groups; adding resources 138
Selected Roles 312, 316
Select Flexi Footprint 1190
Select Last Used Appearance 656
select upgrade target release 1206
Select Upgrade Version 1206
Select Users 316
self provisioning
  enable 173
  end user 173
Sending reports through email 1007
Server Host ID 963
server properties; view 954
Server Properties page 963
server support
  Communication Manager 5.2.1 upgrade 1271
Server support
  Communication Manager 5.2.1 to 6.3.100 1271
Server support for Communication Manager Release 5.2.1 to 6.3.100 upgrades 1271
service
  Health Monitor 83
serviceability agent
  activate 894
  assign filter profile 891
  unassign filter profile 891
serviceability agents 881
serviceability agents *(continued)*
  activate 894
Serviceability agents
  repair 894
serviceability agents list 893
Service Link Mode
  Attendant Console 652
service observe
  coach 676
  listen-only 676
Service Profile Management 798
Session Manager
  configure during GR failover 91
Session Manager 6.3 configuration 90
Session Manager communication profile administration 207
Session Manager Communication profile administration 208
Session Manager correlation 731
Session Manager update 1210
Session Manager upgrade 1208
session properties; edit 44
session properties field descriptions 47
Session termination policy 42
Set Color 660
set enrollment password 1083
setting 662
setting environment variable in Windows XP 737
Settings icon 37
setting System Manager CA as subordinate CA 1102
setting the default CA 1104
setting the new CA as default CA 1104
setting up environment variable 738
setting up environment variable in Windows 7 738
Setting up System Manager to start IP Office 735
setting up System Manager to start IP Office element manager 735
set type 673
  H323 678
set type of endpoints 673
set up alternate source 1149
SFTP Configuration (T) 1162
SHA2 signing algorithm and 2048 key size 1101
shared address 531, 535
  assign 202, 531
shared addresses 171
shutdown 1137
shut down from Web console 1138
shut down System Manager 1138
Single administration
  Dual Registration 678
Single Sign-On 1113–1115
SIP endpoint
  feature button 674
SIP endpoints 679
site
  create 1121
  editing 1126
  viewing 1126

Site Data ... 659
- building ... 659
- cable ... 659
- floor ... 659
- jack ... 659
- room ... 659

SNMP access profile
- edit ... 839

SNMP Access profile
- add ... 839
- delete ... 840

SNMP Access Profile ... 841
SNMP Access Profiles ... 840
SNMP alarms
- CS 1000 ... 96

SNMP attributes ... 865
SNMP discovery
- device list ... 835

SNMP target profile
- add ... 886
- edit ... 887

SNMP target profile; view ... 887
SNMP target profile list ... 886
SNMP target profiles; delete ... 888
SNMP target profiles field descriptions ... 888
SNMP traps ... 948
SNMP V1 ... 841
SNMP V1 protocol ... 840
SNMP V3 ... 841
SNMP V3 protocol ... 840
SNMPv3 user profile; add ... 883
SNMPv3 user profile; create ... 883
SNMPv3 user profile; delete ... 884
SNMPv3 user profile; edit ... 883
SNMPv3 user profile; filter ... 884
SNMPv3 user profile; view ... 883
SNMPv3 user profiles
- assign ... 895
- manage ... 895

SNMPv3 user profiles field description ... 884
software
- analyze ... 1237
- download ... 774, 1169, 1186, 1238

Software inventory
- field descriptions ... 1253

Software Inventory ... 1232
Software Inventory field descriptions ... 1253
software library
- delete ... 1161, 1165
- protocol support ... 1154
- software library management ... 1164
- sync files ... 1166
- upload files ... 1166
- viewing a file ... 1164

Software library ... 1153
software library; add ... 1160
software library; create ... 1160
software library; edit ... 1161
software library; view ... 1161
software library; viewing files ... 1164
software library files ... 1166
software library files field descriptions ... 1166
software management ... 35
- analyze software ... 1238

Software Management ... 1204
software management infrastructure enhancements ... 35
software upgrade
- analyze software ... 774

Solution Deployment Manager ... 31, 1139, 1145, 1168, 1204
- install ... 1219, 1221
- permissions ... 150
- restart virtual machine ... 1192
- start virtual machine ... 1191
- stop virtual machine ... 1191

Solution Deployment Manager client ... 31, 1139–1141
- install ... 1142

Solution Deployment Manager client capabilities ... 1145
Solution Deployment Manager client dashboard ... 1144
Speaker ... 660
Speakerphone ... 652
specifying range for endpoints ... 164
SSO cookie domain value ... 1289
- reimport ... 1289

SSO for Conferencing ... 108
SSO login ... 1289
stand-alone ... 83
start
- virtual machine ... 1191

starting IP Office element manager ... 735
starting the IP Office element manager ... 735
start virtual machine from SDM ... 1191
status
- Analyze ... 1232
- analyze job ... 1231
- element records import ... 875
- Preupgrade check ... 1232
- preupgrade check job ... 1231
- Refresh elements job ... 1231
- upgrade job ... 1231
- upgrade jobs ... 1232

stop
- virtual machine ... 1191

Stop Confirmation page ... 1026
stopping pending jobs ... 1016
stop virtual machine from SDM ... 1191
submitting a request for harvesting log files ... 925
Subnet Configurations field descriptions ... 844
subnets ... 844
subnets list ... 844
subnetwork
- add ... 843
- delete ... 844
- edit ... 844

subscriber; view

subscriber; view *(continued)*
  viewing subscribers ... 567
subscriber class of service ... 565
subscriber COS ... 565
subscriber list ... 568
Subscriber Manager
  datasource attributes ... 558
  datasource parameters ... 558
Subscriber Manager data
  import ... 557
Subscriber Manager user data
  importing ... 562
subscribers; add
  adding subscribers ... 566
  subscribers; new ... 566
subscribers; delete
  deleting subscribers
    removing subscribers ... 568
subscribers; edit
  editing a subscriber ... 567
  editing subscribers ... 567
Subscribers (CMM) ... 574
subscriber template list ... 1038
subscriber templates; delete
  deleting subscriber templates
    deleting templates; subscriber ... 1037
subscriber templates; duplicate
  duplicating subscriber templates
    duplicating templates; subscribers ... 1037
subscriber templates; edit
  editing subscriber templates
    editing templates; subscriber ... 1036
subscriber templates; view
  viewing subscriber templates
    viewing templates; subscriber ... 1037
subscriber template versions ... 1028
support ... 28
Supported servers ... 1243
Survivable COR ... 653
Survivable GK Node Name ... 653
Survivable Trunk Dest ... 656
swap endpoints field descriptions ... 670
sync ... 730
Sync files ... 1166
synchronization ... 49, 988
  DRS clients ... 988
  limitations ... 51
synchronization datasource
  add ... 51
  deleting ... 54
  edit ... 53
synchronization from LDAP directory server ... 50, 51
synchronization job history ... 62
synchronization job history field description ... 62
synchronization job summary
  view ... 63
synchronization to LDAP directory server ... 50
synchronize
  CM data ... 898
  configuring options ... 898
synchronize CM data ... 898
synchronize communication profiles field description ... 905
synchronize UCM and Application Server system configuration ... 900
synchronizing CallPilot profiles ... 903
Synchronizing Communication Manager data
  Synchronizing messaging data
    Inceremental Synchronization
      Initializing Synchronization ... 896
synchronizing communication profiles ... 903
synchronizing CS 1000 profiles ... 903
synchronizing messaging data ... 901
synchronizing resources ... 123
synchronizing System Manager master database and replica computer database ... 990
Synchronizing the VMPro system configuration ... 900
Syslog server ... 1301
system
  scheduled job ... 1010
system configuration ... 754
System Manager
  7.0 ... 1231
  installing patches ... 1223
  Solution Deployment Manager ... 1223
  upgrade ... 1219, 1221, 1231
  upload files ... 768
  Virtual Machines ... 1223
  VM Management ... 1223
System Manager; Communication Manager capabilities ... 583
System Manager; firewall ... 1303
System Manager; firewall implementation ... 1303
System Manager CA certificate; retrieve ... 1092
System Manager CA Generation utility ... 36
System Manager capabilities
  certificate generation ... 1079
  certificate management ... 1079
system manager certificate; download ... 1280
System Manager certificate authority ... 1102
System Manager dashboard ... 37, 38
System Manager documents ... 25
System Manager login ... 38
System Manager restore ... 78
System Manager shutdown ... 1137
System Manager training ... 26
System Manager trust store; Communication Manager certificate ... 1285
System Manager upgrade ... 1226
System Manager VM management ... 1198
System Manager VM update ... 1199
System Manager web console ... 37
System Manage UI
  export users ... 328
System Platform ... 1219, 1221
  add ... 859

System Platform upgrades
preupgrade checks ... 1242
system recovery process ... 116
system requirements for the external server ... 1167
system template
manage audio field description ... 1065

T

target profile; manage ... 895
target profiles ... 881
edit ... 887
target profiles; delete ... 888
target profiles; filter ... 886
target profiles field descriptions ... 888
target release ... 1206
select ... 1206
team
create ... 1121
editing ... 1126
template ... 1243
map permissions ... 152
Template for permission set ... 152, 159
template list ... 1038
templates ... 1028
upgrade ... 1029
templates for mapping permission ... 152
template versioning ... 1028
template versions ... 1028
tenant
create ... 1121
delete ... 1127
editing ... 1126
viewing ... 1126
tenant administrator
assign ... 1125
unassign ... 1125
tenant administrator role
add ... 149
tenant management ... 1125
Tenant Management ... 1120
console ... 39
field descriptions ... 1132
Tenant Management page ... 1132
tenant organization
create ... 1121
tenant partitioning
Avaya SIP AST endpoints ... 1128
Communication Manager ... 1128
Terminate to Coverage Pts. with Bridged Appearances ... 627
terminating single sign-on sessions ... 1118
test alarm from CLI
generate ... 914
test alarms from web console
generate ... 914
third-party identity certificate ... 1102
threshold value
threshold value *(continued)*
disk space ... 778
throttling period ... 912
Through ... 680
Time of Day Coverage Table ... 629, 630
Time of Day Lock Table ... 653
timeout interval
configure ... 84
time zone
configure ... 1302
TN ... 646
TN boards
upgrade ... 1272
TN Boards
protocols ... 1277
transfer custom prompt files ... 761
transfer files
UCM or Application Server ... 761
Transferring audio field description ... 769
transferring audio field descriptions ... 762
transferring audio files ... 767
transferring files to IP Office device ... 768
transferring greeting files ... 767
transferring greeting files to IP Office ... 767
Transferring greetings field description ... 769
TrapListener ... 948
field descriptions ... 824
Trap listener field description ... 824
TrapListener service ... 824, 948
Traplistener service; alarming UI ... 824
TrapListener service; configure ... 824
Triple Ringer Type
Call Pickup button ... 674
configuration ... 674
trusted certificate ... 1087
trusted certificate; add ... 1282
trusted certificates
add ... 1085
view ... 1086
trusted certificates; remove ... 1087
Trusted Certificates page ... 1093
Trust Management ... 1079
Trust management for Conferencing ... 107, 108
turn off compatibility mode ... 36
Turn On Mute ... 673
Turn On Mute for Remote Off-hook Attempt ... 673
two-way TLS ... 1286
Two-way TLS ... 1285
two-way TLS; configure notify sync ... 1283
two-way TLS in System Manager ... 1286

U

UCM
synchronize ... 900
UCM and Application Server ... 751, 753, 754
UCM and Application Serverbackup ... 752

UCM and Application Server Backup field descriptions 755
UCM and Application Server Restore field descriptions 756
UCM and Application Server security configuration field descriptions 760
UCM and Application Serversystem configuration 754
UCM and Application Server System Configuration template
field descriptions 1070
UCM or Application Server
transfer files 761
UCM or IP Office Application Server field descriptions 762
UCM or IP Office Application Server system configuration field descriptions 758
UDP 724
field description 722
UDP entries
add 724
edit 724
update 725
view 724
UDP field descriptions 722
UDP Group
deleting 720
udp groups 719
UDP groups
access 726
assign permission 726
udp groups field description 720
unassign
tenant administrator 1125
unassigning filter profile from serviceability agent 891
UnAssign Roles page 316
unassign users
roles 153, 200
unconfigure
Geographic Redundancy 83
understanding
groups 668
Unified Communications Module (UCM) and Application Server
upgrade 773
uniform dial plan 724
Uniform dial plan
UDP 907
Uniform Dial Plan field descriptions 722
Uniform Dial Plan Group
deleting 720
uniform dial plan group; add 719
Uniform Dial Plan Group; edit 719
Uniform Dial Plan Group; view 720
uniform dial plan groups 719
uninstalling a Communication Manager patch 1276
uninstalling a license file 954
Uninstall License page 962
Unknown location host mapping 1183
Unlocking an IP Office device 735
unmanage elements 858
update
Solution Deployment Manager *(continued)*
Appliance Virtualization Platform 1185
update 1180
Appliance Virtualization Platform host 1180
Communication Manager 1210
Session Manager 1210
Solution Deployment Manager ......
update Appliance Virtualization Platform host ... 1180
updateASG 1298
update software 1210
update static routing 1198
Update Static Routing 1175
update System Manager VM 1199
Update UDP entries 725
field description 725
Updating a Communication Manager 1276
updating the SAMP/MPC firmware 1276
Updating UDP entries 725
Updating UDP entries field description 725
upgrade 1246
6.3.100 1234
Avaya Aura application 1208
Branch Session Manager 1205, 1207, 1208, 1215
checklist 1207
Communication Manager . 1205, 1207, 1208, 1215, 1234
Communication Manager 6.x 1246
elements 1211
IP Office 775, 1205
IP Office Application Server 775
IP Office UCM 775
Session Manager 1205, 1207, 1208, 1215
System Manager 1298
System Platform 1246
target release 1206
Upgrade 1215
Communication Manager 1275
TN boards 1272
upgrade 6.x
checklist 1246
upgrade Avaya Aura application 1145
upgrade Communication Manager 5.2.1
different server 1257
same server 1257
Upgrade Configuration
field descriptions 1215
Upgrade Configuration Details 1215
upgrade jobs
deleting 1231
status 1232
upgrade job status 1231
Upgrade job status
Viewing 1231
upgrade management
field descriptions 1212
user settings 1151
Upgrade Management 1204, 1226, 1232
Upgrade management workflow summary 1244

upgrade media gateways 1273
upgrade media modules 1273
Upgrade Release Selection 1206
Upgrade Release Setting 1206, 1232
upgrades
    supported protocols 1277
Upgrade System Manager 1224
upgrading CM Agent template 1029
upgrading CM Endpoint template 1029
Upgrading Communication Manager 5.2.1 ....1257, 1266
upgrading Communication Manager 5.2.1 to 6.3.100 1269
Upgrading Communication Manager 5.2.1 to release 6.3.100 1270
Upgrading Communication Manager 5.2.1 to release 6.3.6 1248
Upgrading Communication Manager 5.2.1 to release 6.3.7 1269
Upgrading Communication Manager 5.x 1275
Upgrading Communication Manager 6.x to release 6.3.100 1249
Upgrading Communication Manager 6.x to release 6.3.6 ....1249, 1250
upgrading devices
    protocol matrix 1277
upgrading IP Office endpoint templates 1059
upgrading System Platform 1246
Upgrading TN boards 1272
upload file to software library 1166
uploading an audio file in IP Office system configuration template 1064
uploading files to the System Manager repository 768
UPM 204
UPR
    duplicate 544
Usage by local WebLM page 979
usage options 727
Usage Summary page 979
user
    assign groups 312
    restore 199
user account
    create 175
    remove 182
User Attribute Options 511
User Bulk Editor 185
User Bulk Editor field descriptions 185
User Bulk Import Profile 826
user-defined templates 1028
User Delete Confirmation page 311
user details; view 174
user import job
    cancel 338
    delete 338
    schedule 335
User Management
    assigning permissions 164
    roles 164
User management for Application Enablement Services 112
User management for Conferencing 108
User management for IP Office 111
User Management page 241
User Preference 37
user profile
    create 175, 176
User Profile Duplicate page 295
User Profile Edit page 277
user profile management 171
user profiles 881
User Profile View page 244
user provisioning rule 177, 540
    add service to user 542
    create 542
    create user 176
    delete 544
    duplicate 544
    modify 543
    view 543
User Provisioning Rule 257
User Provisioning Rules 185
    field descriptions 545
User Restore Confirmation Page 315
user roles
    view 147
users
    assign 158
    assign groups 197, 198
    bulk edit 183, 185
    bulk export 328
    manage 171
    search 195
users; filter 194
user settings
    field description 1151
User settings
    configure 1148
User Settings 1151
user settings for upgrades 1148
user synchronization datasource
    field descriptions 54
user synchronization job
    create 60
    schedule 61
user synchronization jobs
    delete 61
user synchronization jobs field description 62
using clear amw all 642
using filters
    filtering endpoints 638
using native name 634
using swap endpoints
    endpoints; swap endpoints 643
utility
    bulk import encryption 332

V

validating connectivity to local WebLM servers for a product 967
vCentre 1203
 add 1203
 edit 1203
VDN
 adding dependencies 728
vector directory number,
 vdn 615
vector directory number list 616
vector routing table
 call center; vector routing table 618
vector routing table; add 618
vector routing table; edit 619
vector routing table; field description 619
vector routing table; view 618
vector routing table field description 619
vector routing table list 618
verifying changes to date and time configuration 1301
verifying successful deployment of extension pack 1288
videos 27
view 1088
 global user settings import job details 344
 grace period 814
 import global user settings job 345
 location 1173
 secondary server alarms 915
 user import job details 339
 user provisioning rule 543
view an import global user settings job 345
view an import global user settings job on the Scheduler page 345
view backup files 779
View by feature page 971
View by local WebLM page 972
view completed jobs 1012
view contact list member page 227
view contents; log harvested files 927
view details; log harvesting request 926
view details of a global user settings importing job 344
view details of element 852
view details of import job 344
View Element page 865
view endpoint
 field descriptions 644
view endpoint template
 field descriptions 644
view filter profiles 892
View Group page 131
viewing
 department 1126
 groups 120
 resources for a group 120
 roles 147
 site 1126
viewing *(continued)*
 tenant 1126
 user roles 147
viewing active sessions 1118
viewing agent data
 agents; view data 592
viewing alarms 909
viewing allocations by features 970
viewing allocations by local WebLM 970
viewing a messaging profile of a user 214
viewing an announcement 604
viewing an audio group 613
viewing an IP Office endpoint template 1057
viewing announcements 604
Viewing an Off PBX Endpoint Mapping 684
viewing an SNMP target profile 887
viewing an SNMPv3 user profile 883
viewing associated subscribers
 viewing subscribers 1038
viewing a station profile of a user 210
Viewing a UCM and Application Server Configuration template 1067
Viewing a UCM and Application Server system configuration 757
viewing audio groups 613
viewing authorization code
 authorization code; view 713
Viewing Automatic Alternate Routing Digit Conversion data
 Automatic Alternate Routing Digit Conversion; viewing data 690
Viewing Automatic Route Selection Digit Conversion
 Automatic Route Selection Digit Conversion; viewing data 693
viewing automatic route selection toll data 696
Viewing a VMPro call flow template 1075
Viewing a VMPro System Configuration template 1071
viewing bulk user edit jobs 183
viewing class of service data 709
viewing class of service group
 class of service group; view 715
viewing CM Agent template
 CM Agent template;
  view 1031
viewing CM Endpoint templates 1033
Viewing contents of the certificate 1101
viewing coverage path
 coverage path; view 622
viewing coverage time-of-day
 coverage time-of-day; view data 628
viewing data modules
 data modules; view 699
viewing data retention rules 796
viewing deleted users
 view deleted users 199
viewing details of a log harvesting profile 924, 929
viewing details of a log harvesting request 926
viewing details of a user 174

viewing enterprise usage of a license feature 968
viewing files in the software library 1164
viewing groups 120
viewing harvested log files in an archive 924
viewing identity certificates 1088
viewing IP Office endpoint profiles 220
viewing IP Office system configuration templates 1061
viewing job summary 63
Viewing job summary field descriptions 63
viewing license capacity 953
viewing license capacity of a feature 967
viewing list of backup files 779
viewing log details 942
viewing loggers for a log file 937
viewing notification filter profile 890
Viewing Off PBX Configuration Set 680
viewing peak usage 953
viewing pending jobs 1012
Viewing Remote Servers 1008
viewing replica groups 989
viewing replica node details 990
viewing replica nodes in a replica group 989
viewing replication details for a replica node 990
viewing reports 1005
viewing resources for a group 120
viewing security configuration 743
viewing server properties 954
viewing software library 1161
viewing subscribers CMM field description 574
Viewing Subscribers MM field description 577
viewing subscriber templates CMM; field description
    CMM field description 1051
viewing subscriber templates Messaging
    field descriptions 1048
viewing subscriber templates MM; field description
    MM field description 1053
viewing system configuration file 740
viewing the contents of harvested log files 927
viewing the details of a contact in the contact list 224
viewing the details of a private contact 230
Viewing the status of a Voice Mail Pro call flow 764
viewing the voice mail pro call flow 763
viewing the voice mail pro system configuration 765
viewing UCM and Application Server security configuration
....759
Viewing UDP entries 724
viewing Uniform Dial Plan Group 720
viewing usage by WebLM 968
viewing usage summary 971
viewing user provisioning rule 543
viewing user roles 147
viewing vector directory number
    vector directory number; view 616
viewing vector routing table data 618
Viewing Xmobile Configuration data
    Xmobile Configuration; view data 685
view last contacted status of the local WebLM servers 967
view license capacity 953, 955
View Local WebLMs page 974
view location 1173
view log details 942
view loggers 937
view log harvested files; archive 924
view logs
    completed jobs 1012
    pending jobs 1012
View peak usage 956
view periodic status of master and local WebLM servers ..969
View Private Contact List page 238
View Profile:Alarming UI page 811
View Profile:Communication System Management
Configuration page 801
View Profile:Configuration page 805
View Profile:HealthMonitor UI page 815
View Profile:Logging page 817
View Profile:Logging Service page 819
View Profile:Shutdown page 814
View Profile: SMGR Element Manager page 820
View Profile: Trust Management field description 825
View Profile: User Bulk Import Profile page 826, 828
View Profile Inventory page 805
View profile Messaging field descriptions 806
View Profile System Manager page 810
View Public Contact List page 524
View Remote Server field descriptions 1009
view replica groups 989
View Scheduler Profile page 823
view secondary server alarms 915
View SNMP Profile page 822
view the details of a public contact 521
view the details of a user import job 339
View Trust Certificate page 1096
view trusted certificates 1086
view UDP Groups 720
view user import job on the Scheduler page 338
View WebLM page 816
virtual machine
    create 1188
    edit 1190
    monitoring 1201
    restart 1192
    start 1191
    stop 1191
Virtual machine management 1173
Virtual Machines 1175
Visualization, Performance, and Fault Manager 112
VM connection reestablish 1200
VM Deployment 1192, 1196
VM Management 1219, 1221
VMPro Call Flow Templates field descriptions 1077
VMPro system configuration Templates
    field descriptions 1074
VMware server in Geographic Redundancy setup 70
VOA Repeat 677

voice mail number 659
Voice Mail Pro call flow field descriptions 765
voice mail pro system configuration field descriptions 767
Voice Terminal 648
VPFM 112
VxWorks-based CS 1000 server
  configuration 97

W

warning
  data entry in Excel 323
warranty 28
WebLM access 951
WebLM Home page 955
WebLM overview 950
WebLM servers
  periodic status 969
What's new in this release 31
What is an audio group 612
Windows XP
  setting environment variable 737

X

XML file
  export 794
  import 794
  import users 504
XML for user with core attributes 514
xmobile configuration,
  endpoints; xmobile configuration 685
Xmobile Configuration field description
  Xmobile Configuration; field description 686
xmobile configuration list 685