Administering Avaya Aura® System Manager

Release 10.2.x
Issue 18
February 2026

© 2019-2026, Avaya LLC
All Rights Reserved.

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 in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. 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 or on the express behalf of 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. Please refer to your agreement with Avaya 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

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, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, 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

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction ... 27
Purpose ... 27
Change history ... 27
Chapter 2: Overview ... 32
System Manager overview ... 32
Discontinued support for IP Server Interface (TN2312, commonly known as “IPSI”) ... 34
Log on to System Manager ... 34
Supported browsers ... 34
System Manager web console ... 35
System Manager Dashboard field descriptions ... 37
Logging on to the System Manager web console ... 39
Change Password field descriptions ... 43
Configuring the operating system single-user mode credentials for the root user ... 44
Logon information for users with administrator privilege ... 45
Certificate based authentication ... 45
Tenant Management web console ... 49
Password and security policies for all administrators ... 50
Password aging policy enforcement ... 50
Password strength policy enforcement ... 50
Password history policy enforcement ... 51
Password lockout policy enforcement ... 51
Editing password policies ... 51
Password policies field descriptions ... 52
Managing System Manager command line password policy ... 55
Inactive session termination policy ... 63
Editing Session Properties ... 63
Session Properties field descriptions ... 63
Inactive Account Deactivation Policy field descriptions ... 64
Security settings ... 64
Login Failure Message ... 65
Customized interface ... 66
Reimporting the SSO cookie domain value ... 67
Administrative users ... 68
Viewing administrative user details ... 68
Adding an administrative user ... 68
Editing administrative user details ... 68
Editing administrative user roles ... 69
Enabling an administrative user ... 69
Disabling an administrative user ... 70
Deleting an administrative user ... 70

Terminating administrative user sessions.... 70
Administrative Users field descriptions.... 70
Add New Administrative User field descriptions.... 71
Chapter 3: Directory synchronization.... 72
Directory synchronization overview.... 72
Results of synchronization from the LDAP directory server to System Manager.... 73
Results of synchronization from System Manager to the LDAP directory server.... 73
Limitations in the synchronization of the LDAP directory server.... 74
Adding the synchronization datasource.... 75
Viewing the synchronization datasource.... 76
Editing the synchronization datasource.... 77
Deleting a synchronization datasource.... 77
User synchronization datasource field descriptions.... 78
Preferred languages.... 83
Creating the user synchronization job.... 84
Scheduling a user synchronization job.... 85
Deleting a user synchronization job.... 86
User active synchronization job field descriptions.... 86
Synchronization job history.... 87
Synchronization job history field descriptions.... 87
Stopping a user synchronization job.... 88
Deleting a user synchronization job history.... 88
Viewing Job Summary.... 89
Viewing Job Summary field descriptions.... 89
Chapter 4: Geographic Redundancy.... 91
Geographic Redundancy overview.... 91
Licensing in Geographic Redundancy.... 92
Geographic Redundancy terminology.... 92
Geographic Redundancy replication.... 95
Prerequisites for the Geographic Redundancy setup.... 95
Hardware resource and parameter for the Geographic Redundancy setup.... 96
Key tasks for Geographic Redundancy.... 97
Prerequisites before configuring Geographic Redundancy.... 99
Geographic Redundancy prerequisites overview.... 99
Copying the CRL URL.... 100
Configuring CRL download on the secondary System Manager server.... 102
Adding the trusted certificate of primary server to the secondary System Manager server... 103
Configuring Geographic Redundancy.... 103
Enabling the Geographic Redundancy replication.... 105
Disabling the Geographic Redundancy replication.... 106
Scenarios of auto-disable for the Geographic Redundancy system.... 107
Activating the secondary System Manager server.... 108
Deactivating the secondary System Manager server.... 109

Restoring the primary System Manager server ... 109
Reconfiguring Geographic Redundancy ... 112
Converting the primary System Manager server to the standalone server ... 114
About the Health Monitoring service ... 114
Configuring the timeout interval for health monitoring ... 115
Geographic Redundancy field descriptions ... 116
GR Health field descriptions ... 117
Prerequisites for configuring disaster recovery ... 119
Disaster recovery prerequisites ... 119
Configuring CRL download on the primary System Manager server ... 120
Adding the trusted certificate of secondary server to the primary System Manager server ... 121
Replacing System Manager servers ... 121
Replacement of System Manager servers ... 121
Moving the existing primary System Manager server to a different location ... 121
Restoring the primary System Manager server using the old primary server backup data ... 122
Restoring the primary System Manager server using the data on the secondary System Manager server ... 123
Replacing the secondary System Manager server on the site ... 123
Recovering the primary System Manager server from disaster ... 124
Configuring the GR-unaware elements to work with System Manager ... 127
Geographic Redundancy-unaware elements overview ... 127
Elements Geographic Redundancy manageability status matrix ... 127
Configuring various elements to change to the secondary System Manager ... 128
Introduction ... 128
Session Manager configuration ... 128
Communication Manager configuration ... 131
CS 1000 configuration ... 134
Meeting Exchange configuration ... 137
Presence Server configuration ... 138
Messaging configuration ... 139
Avaya Meetings Server configuration ... 143
IP Office configuration ... 145
Visualization, Performance, and Fault Manager ... 148
Application Enablement Services ... 148
Avaya Aura® Contact Center ... 148
Avaya Multimedia Messaging configuration ... 149
Chapter 5: Managing groups and roles for resources ... 150
Managing groups ... 150
Group management ... 150
Viewing groups ... 151
Creating groups ... 151
Modifying groups ... 151
Creating duplicate groups ... 152

Deleting groups..... 152
Moving groups..... 153
Synchronizing resources for a resource type..... 153
Assigning resources to a group..... 154
Searching for resources..... 154
Searching for groups..... 155
Filtering groups..... 156
Filtering resources..... 156
Removing assigned resources from a group..... 157
Group Management field descriptions..... 157
New Group field descriptions..... 159
View Group field descriptions..... 160
Edit Group field descriptions..... 162
Delete Group Confirmation field descriptions..... 163
Duplicate Group field descriptions..... 164
Move Group field descriptions..... 164
Resource Synchronization field descriptions..... 165
Managing resources..... 165
Manage resources..... 165
Accessing resources..... 165
Assigning resources to a new group..... 165
Adding resources to a selected group..... 166
Searching for resources..... 167
Filtering resources..... 167
Resources field descriptions..... 168
Choose Group field descriptions..... 169
Choose Parent Group field descriptions..... 170
Managing roles..... 171
Role Based Access Control..... 171
Built-in roles..... 171
Custom roles..... 176
Viewing user roles..... 177
Adding a custom role..... 177
Adding a custom tenant administrator role..... 178
Assigning permissions to access Solution Deployment Manager..... 180
Mapping permissions by using the template..... 181
Assigning users to a role..... 181
Unassigning users from role 182
Copying permission mapping for a role..... 182
Editing a custom role..... 183
Deleting custom roles..... 184
Roles field descriptions..... 184
Add New Role field descriptions..... 185

Role Details field descriptions..... 185
Add Mapping field descriptions..... 186
Assigned Users field descriptions..... 186
Permission mapping field descriptions..... 187
Chapter 6: Granular role based access control..... 188
Granular RBAC..... 188
Implicit permissions required for Communication Manager objects..... 189
Sample scenario for the range feature..... 191
Assigning permissions in User Management..... 191
Assigning permissions through User Management..... 191
Field-level RBAC..... 193
Endpoints..... 197
Range in endpoints..... 197
Assigning range for endpoints..... 198
Assigning permissions for fields in endpoints..... 200
Hunt Group..... 202
Assigning range for hunt group..... 202
Assigning permissions for fields in hunt group..... 204
Trunk Group..... 206
Assigning permissions for fields in trunk group..... 206
Chapter 7: Managing users, public contacts, and shared addresses..... 208
Managing users..... 208
Users, public contacts, and shared addresses..... 208
Access to administrative users..... 209
End user self provisioning..... 210
Enabling self provisioning..... 210
Disabling self provisioning..... 211
Generating the communication profile password from the self provisioning interface..... 211
Changing the communication profile password from the self provisioning interface..... 212
Viewing details of a user..... 213
Creating a new user account..... 213
Creating a new user profile using the user provisioning rule..... 214
Results of using the user provisioning rule..... 215
Modifying user accounts..... 219
Creating duplicate users..... 220
Removing user accounts..... 221
Removing the deleted users from the database..... 221
Editing users in bulk..... 222
Viewing bulk user edit jobs..... 222
Deleting the bulk user edit job..... 223
Create new profile option..... 223
User Provisioning Rules and User Bulk Editor..... 224
User Bulk Editor field descriptions..... 224

Filtering users.... 236
User searchable fields.... 237
Searching for users by using Search component.... 237
Searching for users by using Advanced Search.... 237
Assigning roles to a user.... 238
Assigning roles to multiple users.... 239
Removing roles from a user.... 239
Assigning groups to a user.... 239
Assigning groups to multiple users.... 240
Removing a user from groups.... 240
Assigning a user to a group using XML.... 241
Removing a user from a group using XML.... 242
Viewing deleted users.... 242
Restoring a deleted user.... 243
Assigning users to roles.... 243
Unassigning users from role 244
Managing addresses.... 244
Managing communication profiles.... 247
Managing default contact list of the user.... 265
Managing private contacts of a user.... 271
User Management field descriptions.... 282
User Profile | Add field descriptions.... 285
User Profile | Edit | <User Name> field descriptions.... 307
User Profile | View | <User Name> field descriptions.... 328
User Profile | Duplicate | <User Name> field descriptions.... 344
User Delete Confirmation field descriptions.... 362
Assign Roles to Multiple Users field descriptions.... 363
Assign Roles field descriptions.... 363
Assign Groups field descriptions.... 364
Assign Groups to Multiple Users field descriptions.... 364
Deleted Users field descriptions.... 365
User Restore Confirmation field descriptions.... 366
Assign Users To Roles field descriptions.... 366
UnAssign Roles field descriptions.... 367
Managing bulk import and export.... 368
Managing public contacts.... 598
Manage public contact list.... 598
Adding a new public contact.... 598
Modifying details of a public contact.... 599
Deleting public contacts.... 599
Viewing the details of a public contact.... 600
Adding a postal address for a public contact.... 600
Modifying postal address of a public contact.... 600

Deleting the postal addresses of a public contact..... 601
Choosing a shared address for a public contact..... 601
Adding a contact address of a public contact..... 601
Modifying the details of a public contact..... 602
Deleting the contact address of a public contact..... 602
View Public Contact field descriptions..... 602
Edit Public Contact field descriptions..... 604
New Public Contact field descriptions..... 606
Public Contacts field descriptions..... 608
Managing shared addresses..... 609
Manage shared address..... 609
Assigning a shared address to the user..... 609
Adding a shared address..... 610
Modifying a shared address..... 610
Deleting a shared address..... 610
Add Address field descriptions..... 611
Edit Address field descriptions..... 611
Shared Address field descriptions..... 612
Managing presence access control lists..... 613
Manage Presence Access Control Lists..... 613
Presence ACL field descriptions..... 613
Communication profile password policy enforcement..... 614
Communication profile password policy..... 614
Editing the password policy for the communication profile 615
Communication Profile Password Policy field descriptions..... 616
Chapter 8: Managing user provisioning rules..... 618
User Provisioning Rule..... 618
Capabilities and guidelines of user provisioning rules..... 619
Adding User Provisioning Rules..... 620
Creating the user provisioning rule..... 621
Modifying the user provisioning rule..... 621
Viewing the user provisioning rule..... 622
Creating a duplicate user provisioning rule..... 622
Deleting a user provisioning rule..... 623
User Provisioning Rules field descriptions..... 623
New User Provisioning Rule field descriptions..... 624
Chapter 9: Managing elements..... 635
Importing users from Subscriber Manager to User Management..... 635
User data import to System Manager..... 635
Preparing the Subscriber Manager user data for import to User Management..... 636
Importing the Subscriber Manager user data to User Management..... 637
Subscriber Manager datasource parameters and attributes..... 639
Exporting the user data and creating the user profile..... 640

Importing users from CS 1000 Subscriber Manager to User Management..... 642
CS 1000 Subscriber Manager data import options..... 642
Preparing the CS 1000 Subscriber Manager user data for import to System Manager..... 642
Importing the CS 1000 Subscriber Manager user data to System Manager..... 643
Exporting the CS 1000 user data and creating the user profile..... 643
Preparing the CS 1000 Subscriber Manager user data for import to System Manager..... 643
Importing the CS 1000 UCM Subscriber Manager user data to System Manager..... 644
Exporting the CS 1000 user data and creating the user profile..... 645
Managing messaging..... 645
Messaging Class Of Service..... 645
Viewing Class Of Service..... 645
Class of Service List field descriptions..... 646
Messaging..... 646
Chapter 10: Managing Communication Manager..... 653
System Manager Communication Manager capabilities..... 653
Configuring Communication Manager user profile settings..... 654
Editing the Select All attribute in a table..... 655
Search component for Communication Manager objects..... 655
Managing Communication Manager objects..... 657
Communication Manager objects..... 657
Agents..... 663
Announcements..... 675
Audio Groups..... 688
Holiday Table..... 691
Vector Directory Number..... 693
Vector Routing Table..... 697
Service Hours Tables..... 700
Coverage Path..... 702
Coverage Time-of-day..... 710
Element Cut-Through..... 714
Endpoints..... 716
Hunt Group..... 785
Trunk Group..... 789
Managing Off PBX Configuration Set..... 792
Managing Off PBX Endpoint Mapping..... 795
Xmobile Configuration..... 796
Automatic Alternate Routing Digit Conversion..... 801
Automatic Route Selection Digit Conversion..... 804
Automatic Route Selection Toll..... 806
Cluster Session Manager..... 808
Data Modules..... 809
Class of service..... 819
Authorization Code..... 822

Class of Service Group.... 824
Uniform Dial Plan Groups.... 828
Uniform Dial Plan.... 832
Usage options.... 836
NRP Group.... 840
Decommissioning Communication Manager from System Manager.... 843
Chapter 11: Managing backup and restore.... 848
Backup and restore.... 848
/emdata/svars/ backup in System Manager.... 849
Backup failure due to lack of disk space in /swlibrary.... 849
Disk space management for System Manager backup.... 850
Backup and restore on System Manager that is configured for Geographic Redundancy.... 850
Accessing the Backup and Restore service.... 851
Viewing list of backup files.... 851
Enabling backup encryption.... 852
Creating a data backup on a local server.... 852
Creating a data backup on a remote server.... 853
Scheduling a data backup on a local server.... 854
Scheduling a data backup on a remote server.... 855
Editing a scheduled backup job.... 856
Deleting the scheduled backup job.... 856
Restoring data backup from a local server.... 857
Restoring a backup from a remote server.... 858
Disk space required for backup.... 860
Time duration for backup and restore.... 860
Supported ciphers, key exchange algorithms, and mac algorithms.... 861
Backup and Restore field descriptions.... 862
Backup field descriptions.... 863
Schedule Backup field descriptions.... 865
Restore field descriptions.... 866
Chapter 12: Configuring applications.... 868
Managing data retention rules.... 868
Data retention rules.... 868
Excluded log files.... 868
Accessing the Data Retention Rules service.... 869
Modifying data retention rule.... 870
Applying data retention rule.... 870
Data Retention field descriptions.... 870
logRetention command.... 871
updateLogRetention command.... 871
pruneAllLogs command.... 872
Configuring applications.... 872
Configuration management.... 872

View Profile: Agent Management field descriptions..... 872
Configuring IP Office..... 874
IP Office profile field descriptions..... 874
View Profile: Communication System Management Configuration field descriptions..... 875
Edit Profile: Communication System Management Configuration field descriptions..... 876
View Profile: Event processor field descriptions..... 877
View Profile:Configuration field descriptions..... 877
View profile:Inventory field descriptions..... 878
Edit Profile:Inventory field descriptions..... 879
View and Edit Profile Messaging field descriptions..... 879
View Profile: Data Transport Config field descriptions..... 880
View Profile: Data Transport Static Config field descriptions..... 883
View and Edit Profile SMGR field descriptions..... 883
View Profile:Alarming UI field descriptions..... 886
Edit Profile:Alarming UI field descriptions..... 886
View Profile:Common Console field descriptions..... 887
Edit Profile:Common Console field descriptions..... 888
View Profile:GracefulShutdown field descriptions..... 888
Edit Profile:GracefulShutdown field descriptions..... 889
View Profile:HealthMonitor field descriptions..... 889
Edit Profile:HealthMonitor field descriptions..... 889
View Profile:Licenses field descriptions..... 890
Edit Profile:Licenses field descriptions..... 890
View Profile:Logging UI field descriptions..... 891
Edit Profile:Logging UI field descriptions..... 891
View Profile:Logging Service field descriptions..... 892
Edit Profile:Logging Service field descriptions..... 893
View and Edit Profile: SMGR Element Manager field descriptions..... 894
View Profile:SNMP field descriptions..... 896
View Profile:Scheduler field descriptions..... 896
Edit Profile:Scheduler field descriptions..... 897
Configuring the TrapListener service..... 897
View Profile: TrapListener field descriptions..... 898
Configuring Trust Management..... 898
View Profile: TrustManagement field descriptions..... 899
Edit Profile: TrustManagement field descriptions..... 899
View Profile: User Bulk Import Profile field descriptions..... 900
Edit Profile: User Bulk Import Profile field descriptions..... 901
Chapter 13: Managing inventory..... 904
Element management..... 904
Methods to add elements to System Manager..... 906
Manual addition of elements..... 906
Adding a new element..... 906

Bulk import of elements.... 906
Discovering elements.... 907
Working with Elements in System Manager.... 922
Additional information required for creating the Communication Manager or Messaging element.... 922
Manage elements in System Manager configured with Geographic Redundancy.... 923
Determining the System Manager that manages a GR-aware element.... 923
Viewing details of an element.... 924
Modifying an element.... 924
Deleting an element.... 925
Exporting elements from the System Manager command line interface.... 925
runRTSCli.sh command.... 925
Assigning elements to an element.... 927
Removing assigned elements.... 927
Managing access profiles and ports.... 927
Managing and unmanaging elements from System Manager.... 930
Adding Platform type elements to System Manager.... 930
Adding System Platform to System Manager.... 930
Adding Application type elements to System Manager.... 932
Adding Utility Services to System Manager.... 932
Adding or editing a Communication Manager instance to System Manager.... 932
Adding a Session Manager instance to System Manager.... 934
Adding an Application Enablement Services instance to System Manager.... 935
Adding G430 or G450 Branch Gateway to System Manager.... 936
Adding an Avaya Messaging profile for a user.... 937
Product Initiated Registration overview.... 938
Configuring SAL Gateway.... 939
Configuring Avaya Services registration.... 939
Viewing notification status.... 940
Viewing certificate add status of elements.... 941
Field descriptions.... 941
Manage Elements field descriptions.... 941
Element details field descriptions.... 944
Delete Element Confirmation field descriptions.... 951
Import Elements field descriptions.... 952
Import Status field descriptions.... 954
Add Communication Manager field descriptions.... 955
Adding an Application Enablement Services instance to System Manager field descriptions 959
Add IP Office field descriptions.... 960
Delete IP Office field descriptions.... 961
Managing Serviceability Agents.... 961
Serviceability Agents.... 961
Converting a common alarm definition file to MIB file and trapd file.... 962

Configuration files in the MIBTOOL.jar file..... 963
generateTrapdAndMibUnix..... 963
Managing SNMPv3 user profiles..... 964
Managing SNMP target profiles..... 967
Notification filtering..... 969
Managing user and target profiles..... 974
Command line interface alternative to Serviceability Agents..... 979
Creating SNMP user profiles 980
Listing SNMP user profiles 981
Creating SNMP target profiles..... 981
Listing SNMP target profiles 982
Attaching and detaching target profiles from serviceability agents 982
Listing target profiles attached to agents..... 983
Listing agents attached to target profiles..... 983
Creating notification filter profiles..... 983
Listing notification filter profiles..... 984
Attaching or detaching filter profiles to or from target profile serviceability agents..... 984
Listing filter profiles attached to given target profiles and agent IP addresses..... 985
Synchronization of Data..... 985
Communication Manager, Messaging data, and IP Office synchronization..... 985
Synchronizing the Communication Manager data and configuring options..... 988
Running an initializing synchronization..... 988
Running force initialize data synchronization..... 989
Running an incremental synchronization..... 989
Synchronizing the IP Office system configuration..... 990
Synchronizing the IP Office Application Server system configuration..... 990
Synchronizing the VMPro system configuration..... 991
Synchronizing the messaging data..... 992
Saving the Communication Manager translations..... 992
About CM audit..... 992
Performing a Communication Manager audit..... 993
CM audit field descriptions..... 993
Audit report field descriptions..... 993
Communication Profiles synchronization..... 994
Communication profiles synchronization..... 994
Synchronizing the CS 1000 profile..... 995
Assigning anonymous profiles..... 995
Deleting anonymous profiles..... 996
Cleaning up communication profiles..... 996
Synchronize communication profiles field descriptions..... 997
Anonymous Communication Profiles field descriptions..... 997
Average duration of CS 1000 account operations..... 998
Connection pooling..... 998

Connection pooling.... 998
Configuring Communication Manager Connection Pool.... 998
Connection Pooling field descriptions.... 1000
Modifying the maximum number of simultaneous logins for a user.... 1001
Configure options.... 1001
Chapter 14: Managing events.... 1003
Managing alarms.... 1003
Alarming.... 1003
Cluster level alarming.... 1003
Remote key server alarms.... 1004
Viewing alarms.... 1004
Changing the alarm status.... 1004
Exporting alarms.... 1005
Deleting alarms.... 1005
Filtering alarms.... 1005
Searching for alarms.... 1006
Changing the throttle period from default 720 minutes to other period for specific alarm ... 1006
Configure a threshold to raise the System Manager backup alarm.... 1007
Generating test alarms.... 1008
Managing Geographic Redundancy related alarms.... 1010
AutoRefresh Alarm List field descriptions.... 1011
Alarming field descriptions.... 1012
Managing logs.... 1015
Logging service.... 1015
Log Types.... 1016
Managing log harvester.... 1016
Managing log settings.... 1029
Managing log viewer.... 1035
Audit Logging.... 1041
configureSyslog command.... 1042
Configuring remote syslog server from CLI.... 1043
Viewing remote syslog server configuration from CLI.... 1044
Deleting the remote syslog server configuration from CLI.... 1045
TrapListener service.... 1045
Chapter 15: Managing licenses.... 1047
WebLM overview.... 1047
Obtaining the license file.... 1047
Finding LAC for System Manager in PLDS.... 1048
Accessing WebLM.... 1048
Installing a license file.... 1049
Client node locking.... 1050
Viewing the license capacity and utilization of the product features 1051
Viewing peak usage for a licensed product.... 1051

Uninstalling a license file.... 1052
Viewing the server properties.... 1052
WebLM Home field descriptions.... 1053
Install license field descriptions.... 1053
View License Capacity field descriptions.... 1054
View Peak Usage field descriptions.... 1055
Centralized licensing.... 1056
About centralized licensing.... 1056
Enabling centralized licensing.... 1057
Configure centralized licensing field descriptions.... 1057
Adding an element instance and assigning the element instance to a license file.... 1058
Editing an element instance and license file assignment.... 1059
Deleting an element instance.... 1060
Element instance field descriptions.... 1060
Disabling centralized licensing.... 1061
Uninstall license field descriptions.... 1061
Server Properties field descriptions.... 1062
Adopter application cannot communicate with WebLM Server.... 1062
Enterprise licensing 1062
Configuring enterprise licensing.... 1062
Retrieving the local WebLM certificate from browser.... 1064
Adding local WebLM certificate as trusted certificate in System Manager.... 1064
Adding a local WebLM server.... 1065
Modifying a local WebLM server configuration.... 1066
Removing a local WebLM server.... 1067
Viewing the license capacity of the licensed features of a product.... 1067
Viewing the connectivity status of the local WebLM servers 1067
Validating connectivity to local WebLM servers for a product.... 1068
Viewing usage by WebLM.... 1068
Viewing enterprise usage of a license feature.... 1068
Viewing the periodic status of the master and local WebLM servers.... 1069
Querying usage of feature licenses for master and local WebLM servers.... 1069
Changing allocations of licensed features for a local WebLM server.... 1070
Viewing allocations by features.... 1070
Viewing allocations by the local WebLM server.... 1070
Viewing usage summary.... 1071
View by feature field descriptions.... 1071
View by local WebLM field descriptions.... 1071
Enterprise Configuration field descriptions.... 1072
View Local WebLMs field descriptions.... 1074
Add local WebLM field descriptions.... 1074
Modify local WebLM field descriptions.... 1075
Delete local WebLM field descriptions.... 1077

Deletion of the local WebLM server.... 1077
Usage Summary field descriptions.... 1077
Usage by WebLM field descriptions.... 1078
Enterprise Usage field descriptions.... 1079
Query Usage field descriptions.... 1079
Allocations by Features field descriptions.... 1080
Allocations by Local WebLM field descriptions.... 1081
Change Allocations field descriptions.... 1082
Periodic Status field descriptions.... 1083
Metering Collector configuration overview.... 1083
Metering Collector Configuration field descriptions.... 1084
Deleting the metering collector configuration.... 1084
Chapter 16: Data Replication Service.... 1086
Data Replication Service.... 1086
Synchronization in a Geographic Redundancy scenario.... 1087
DRS client audit.... 1087
Viewing replica groups.... 1088
Viewing replica nodes in a replica group.... 1088
Repairing a replica node.... 1089
Repairing all replica nodes in a replica group.... 1089
Viewing replication details for a replica node.... 1090
Removing a replica node.... 1090
Removing a replica node from the queue.... 1090
Replica Groups field descriptions.... 1091
Replica Nodes field descriptions.... 1092
Replication Node Details field descriptions.... 1095
Chapter 17: Managing reports.... 1098
Reports.... 1098
Reports Generation field descriptions.... 1098
Accessing the tabs main buttons, feature buttons, expansion/module buttons, and softkeys buttons.... 1099
Generating a detailed report.... 1100
Generating a basic report.... 1101
New Report field descriptions.... 1102
Editing report parameters.... 1105
Rerunning reports.... 1106
Customizing reports.... 1106
Downloading reports.... 1107
Reports History field descriptions.... 1108
Configuring email properties.... 1108
Configuring the External Admin Connect Properties.... 1109
Sending reports through email.... 1110
Deleting reports.... 1110

Configuring report properties.... 1110
Remote server configuration.... 1111
Adding a remote server.... 1111
Viewing the details of a remote server.... 1111
Editing the details of a remote server.... 1111
Deleting a remote server.... 1112
Add Server field descriptions.... 1112
Remote Server Configuration field descriptions.... 1112
Chapter 18: Managing scheduled jobs.... 1114
Scheduler.... 1114
Functions of the User Management scheduled job.... 1118
Accessing scheduler.... 1118
Assigning permissions to access Scheduler.... 1118
Viewing pending jobs.... 1119
Viewing completed jobs.... 1119
Viewing logs for a job.... 1120
Filtering jobs.... 1120
Editing a job.... 1121
Deleting a job.... 1121
Disabling a job.... 1122
Enabling a job.... 1122
Stopping a job.... 1123
Pending Jobs field descriptions.... 1123
Completed Jobs field descriptions.... 1125
Job Scheduling-View Job field descriptions.... 1127
Job Scheduling-Edit Job field descriptions.... 1129
Job Scheduling-On Demand Job field descriptions.... 1130
Disable Confirmation field descriptions.... 1131
Stop Confirmation field descriptions.... 1132
Delete Confirmation field descriptions.... 1133
Chapter 19: Templates.... 1135
Template management.... 1135
Template versioning.... 1135
Filtering templates.... 1135
Upgrading a template.... 1136
Adding CM Agent template.... 1137
Editing CM Agent template.... 1137
Viewing CM Agent template.... 1138
Deleting CM Agent template.... 1138
Duplicating CM Agent template.... 1138
Adding CM Endpoint templates.... 1139
Editing CM Endpoint templates.... 1139
Viewing CM Endpoint templates.... 1140

Deleting CM Endpoint templates..... 1140
Duplicating CM Endpoint templates..... 1141
Assigning permissions for CM templates..... 1141
Adding subscriber templates..... 1142
Editing subscriber templates..... 1143
Viewing subscriber templates..... 1144
Deleting subscriber templates..... 1144
Duplicating subscriber templates..... 1144
Viewing associated subscribers..... 1145
Templates List..... 1145
Add Agent Template field descriptions..... 1147
Subscriber Messaging Templates field descriptions..... 1153
Subscriber CMM Templates field descriptions..... 1156
Subscriber MM Templates field descriptions..... 1158
Managing IP Office Endpoint template..... 1161
Adding an IP Office endpoint template..... 1161
Viewing an IP Office endpoint template..... 1162
Editing an IP Office endpoint template..... 1162
Duplicating an IP Office endpoint template..... 1163
Deleting an IP Office endpoint template..... 1163
Upgrading IP Office endpoint templates..... 1164
IP Office endpoint template field descriptions..... 1164
Managing IP Office System Configuration template..... 1165
Adding an IP Office System Configuration template..... 1165
Viewing an IP Office System Configuration template..... 1166
Editing an IP Office system configuration template..... 1166
Deleting an IP Office system configuration template..... 1166
Applying an IP Office system configuration template on an IP Office device..... 1167
IP Office System Configuration template field descriptions..... 1168
Manage audio files..... 1168
Uploading an audio file..... 1168
Converting a .WAV audio file to a .C11 audio file..... 1169
Deleting an audio file..... 1169
Manage Audio field descriptions..... 1170
Managing Application Server system configuration templates..... 1171
Adding an Application Server Configuration template..... 1171
Viewing an Application Server Configuration template..... 1171
Editing an Application Server Configuration template..... 1172
Deleting an Application Server Configuration template..... 1172
Applying an Application Server Configuration template..... 1173
IP Office Application Server Templates field descriptions..... 1173
Managing VMPro system configuration templates..... 1174
Adding a VMPro System Configuration template..... 1174

Viewing a VMPro System Configuration template.... 1174
Editing a VMPro System Configuration template.... 1175
Deleting a VMPro System Configuration template.... 1175
Applying a VMPro System Configuration template on a device.... 1176
Duplicating a VMPro System Configuration template.... 1176
VMPro System Configuration Templates field descriptions.... 1177
Managing VMPro call flow templates.... 1177
Adding a VMPro Call Flow template.... 1177
Viewing a VMPro Call Flow template.... 1178
Editing a VMPro Call Flow template.... 1178
Deleting a VMPro Call Flow template.... 1179
Applying a VMPro Call Flow template on a device.... 1179
Duplicating a VMPro Call Flow template.... 1180
VMPro Call Flow Templates field descriptions.... 1180
Chapter 20: Security.... 1182
Extended Security Hardening.... 1182
Enabling Commercial Grade Hardening.... 1183
Enabling Military Grade hardening.... 1184
Optional settings for security hardening.... 1185
Security hardening options.... 1186
Enabling security hardening options.... 1186
Disabling security hardening options.... 1187
Viewing the status of the security hardening options.... 1188
Configuring the TLS cipher suite list.... 1189
Changing the TLS version.... 1189
Changing the TLS version of System Manager.... 1189
Changing the TLS version of primary and secondary System Manager.... 1190
outboundConnectionLogging command.... 1191
Enabling outbound connection logging.... 1191
Disabling outbound connection logging.... 1192
configureOutboundFirewall command.... 1192
Configuring the outbound firewall rules.... 1194
Viewing the list of outbound firewall rules.... 1195
Viewing the outbound firewall rule status.... 1195
Removing outbound firewall rules.... 1196
Disabling the outbound firewall rule.... 1196
Overwriting the existing outbound firewall rules.... 1197
Managing the outbound firewall rule logging.... 1198
Managing certificates.... 1198
Trust Management.... 1198
Certificate generation and certificate management capabilities in System Manager.... 1199
Setting the enrollment password.... 1202
Managing trusted certificates.... 1204

Managing identity certificates.... 1210
Certificate renewal command overview.... 1218
Using the certificate renewal command.... 1218
Certificate Revocation.... 1220
Manage Entity Classes.... 1222
manageEntityClassWhitelist command.... 1226
Retrieving the System Manager CA certificate.... 1232
Certificate Authorities.... 1232
Applying third-party certificates to Appliance Virtualization Platform.... 1232
Creating or editing generic CSR.... 1234
Generating certificates from System Manager.... 1234
External SSL configurations in System Manager.... 1247
Set the System Manager CA as the subordinate CA.... 1247
Configuring DTLS for CS 1000.... 1259
Configuring SIP TLS for CS 1000.... 1260
Managing certificate revocation list.... 1260
Deletion of expired certificates data from System Manager.... 1270
Extended Hostname Validation.... 1271
Enabling Extended Hostname Validation.... 1271
External authentication.... 1271
External authentication.... 1271
Editing the authentication scheme.... 1272
Provisioning of authentication servers.... 1273
Provisioning the LDAP server.... 1273
Provisioning the RADIUS server.... 1274
Provisioning the Kerberos server.... 1274
Provisioning user certificate authentication.... 1275
Authentication Servers field descriptions.... 1275
SAML authentication.... 1277
SAML setup.... 1282
Configuring SSO between System Manager and Microsoft ADFS.... 1282
Establish SSL trust between System Manager and Active Directory Federation Service.... 1283
Configure System Manager as a Relying Party in ADFS.... 1284
Configuring ADFS for Form based authentication.... 1285
Configure ADFS as a Remote Identity Provider (R-IDP) in SMGR.... 1285
Launching the System Manager web console from ADFS using SSO.... 1286
SAML sequence and flow diagram for SAML SSO authenticate for System Manager.... 1287
Active sessions.... 1288
Viewing active sessions.... 1288
Terminating Single Sign-On sessions.... 1288
Regenerating data protection keys.... 1288
Regenerating symmetric keys for System Manager.... 1288
Regenerating asymmetric keys for System Manager.... 1289

Regenerating asymmetric keys for geographic redundancy-enabled System Manager..... 1290
Chapter 21: Managing tenants..... 1292
Multi Tenancy..... 1292
Enabling Multi Tenancy..... 1293
Creating a tenant..... 1294
Assigning the tenant administrator to the tenant..... 1297
Unassigning the tenant administrator..... 1298
Viewing the tenant..... 1298
Modifying the tenant..... 1299
Deleting a tenant..... 1299
Multi Tenancy for Avaya SIP AST endpoints..... 1301
Multi Tenancy for Communication Manager objects..... 1301
Notes on Multi Tenancy for Communication Manager..... 1302
Tenant Management field descriptions..... 1305
Create Tenant field descriptions..... 1305
Chapter 22: Shutting down System Manager..... 1310
Overview..... 1310
Shutting down System Manager from the web console..... 1311
Rebooting the System Manager virtual machine from the web console..... 1312
Rebooting the System Manager virtual machine through command-line interface..... 1313
Viewing the shutdown history from the System Manager web console..... 1313
Shutdown System Manager field descriptions..... 1313
Chapter 23: Solution deployment and upgrade..... 1315
Solution Deployment Manager..... 1315
Solution Deployment Manager overview..... 1315
Solution Deployment Manager Client..... 1316
Solution Deployment Manager..... 1324
Solution Deployment Manager configuration settings 1326
User settings..... 1326
Establishing PLDS connection to Avaya..... 1327
Establishing the connection to an alternate source..... 1328
User Settings field descriptions..... 1331
Software library management..... 1332
Software library..... 1332
Enabling and disabling FTP on System Manager..... 1333
Configuring System Manager as local software library..... 1333
Configuring external server as a remote software library for upgrades..... 1334
Creating a software library..... 1341
Editing a software library..... 1341
Viewing a software library..... 1341
Deleting a software library..... 1342
Software library field descriptions..... 1342
Viewing a file in the software library..... 1344

Downloading the OVA file to System Manager.... 1344
Uploading a file to the software library.... 1345
Deleting a file from the software library.... 1346
Software Library Files field descriptions.... 1347
System requirements for the external server.... 1347
Applications pre-upgrade functions.... 1348
Refreshing elements.... 1348
Analyzing software.... 1349
Downloading the software.... 1349
File Download Manager field descriptions.... 1350
Performing the preupgrade check.... 1351
Preupgrade Configuration field descriptions.... 1352
Application management.... 1353
Application management.... 1353
Managing the location.... 1354
Managing the platform.... 1356
Managing certificates.... 1392
Managing the application.... 1396
Monitoring a host and virtual machine.... 1417
Managing vCenter.... 1418
Managing syslog profiles.... 1424
Viewing the job history of virtual machine operations.... 1427
Application Management field descriptions.... 1427
Job History field descriptions.... 1432
Upgrading Avaya Aura® applications.... 1433
Upgrade Management overview.... 1433
Avaya Aura® applications upgrade.... 1434
Upgrade checklist for Avaya Aura® Virtual Appliance 1435
Upgrade target release selection.... 1436
Installing software patches by using Solution Deployment Manager.... 1437
Installing custom software patches.... 1439
Installed Patches field descriptions.... 1441
Upgrade Management field descriptions.... 1442
Upgrade Configuration field descriptions.... 1444
Edit Upgrade Configuration field descriptions.... 1445
Uploading a custom patch.... 1452
Uploading custom patch field descriptions.... 1453
Rolling back to Utility Services.... 1454
Retrying Utility Services to AVP Utilities upgrade.... 1454
Upgrading Branch Session Manager instances in bulk.... 1455
System Manager upgrade management.... 1462
Upgrade Management field descriptions.... 1462
Add Element field descriptions.... 1462

Edit Elements field descriptions.... 1463
Upgrade Management field descriptions.... 1464
Upgrade job status.... 1472
Upgrade job status.... 1472
Viewing the Upgrade job status.... 1473
Editing an upgrade job.... 1473
Deleting Upgrade Jobs.... 1473
Upgrade Job Status field descriptions.... 1474
Upgrading media gateways and media modules.... 1474
G430 Branch Gateway and G450 Branch Gateway multistep upgrade overview.... 1476
Configuring EASG during G430 Branch Gateway and G450 Branch Gateway upgrade.... 1478
Downloading a file.... 1479
Protocol matrix for upgrades.... 1480
Uploading the version.xml file.... 1481
Chapter 24: Data Encryption.... 1482
Remote Key Server.... 1483
Data Encryption password policy.... 1483
Data encryption commands.... 1483
encryptionPassphrase command.... 1484
encryptionRemoteKey command.... 1486
encryptionLocalKey command.... 1488
Viewing data encryption status.... 1489
Chapter 25: Communication Manager Notify Sync.... 1490
Communication Manager notify synchronization.... 1490
Downloading the System Manager PEM certificate.... 1492
Downloading the pem file to Communication Manager.... 1492
Adding a trusted certificate to Communication Manager.... 1493
Configuring notify sync between Communication Manager and System Manager.... 1494
Configure two-way TLS.... 1496
Adding the Communication Manager certificate to the System Manager trust.... 1496
Enabling two-way TLS in System Manager.... 1497
Chapter 26: System Manager Network Configuration.... 1499
Out of Band Management in System Manager.... 1499
Configuring Out of Band Management on System Manager.... 1500
Configuring Out of Band Management on System Manager in the Geographic Redundancy setup.... 1501
Changing the IP address and FQDN in System Manager.... 1502
Impact of change in FQDN and IP address on the Geographic Redundancy feature.... 1502
SSO login to remote machine fails.... 1503
Changing network parameters on System Manager.... 1503
Changing IP address or FQDN of managed elements.... 1506
Changing the System Manager IP address in managed elements.... 1506

Changing the IP address and FQDN on the System Manager servers in Geographic Redundancy ... 1507
Change in IP address and FQDN on the primary and secondary System Manager servers 1507
Changing the IP address and FQDN on the primary System Manager when the secondary is in the standby or active mode ... 1508
Changing the IP address and FQDN on the primary System Manager server when the secondary is nonoperational ... 1508
System Manager command line interface operations ... 1510
editHosts ... 1521
Chapter 27: Configuring the date and time ... 1522
Verifying changes to the date and time configuration ... 1522
Changing date and time on System Manager running on VMware ... 1522
Configuring the NTP server ... 1522
Configuring the time zone ... 1523
Chapter 28: System Manager localization ... 1524
Installing language pack on System Manager ... 1525
Chapter 29: Resources ... 1526
System Manager documentation ... 1526
Finding documents on the Avaya Support website ... 1527
Accessing the port matrix document ... 1527
Avaya Documentation Center navigation ... 1528
Training ... 1529
Viewing Avaya Mentor videos ... 1529
Support ... 1530
Using the Avaya InSite Knowledge Base ... 1530
Appendix A: Firewall implementation in System Manager ... 1532
Firewall basics ... 1532
Firewall implementation in System Manager ... 1532
Appendix B: Communication Manager reports available through System Manager ... 1534
List reports ... 1534
Display reports ... 1539
Status reports ... 1542
Appendix C: Remote Access ... 1546
Remote access of System Manager ... 1546
EASG login for System Manager ... 1546
Logging on to the System Manager web console by using EASG login ... 1547
Glossary ... 1548

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.

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 provides, and customers.

Change history

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

Issue	Date	Summary of changes
18	February 2026	Updated the following section: • Scheduler on page 1114
17	December 2025	Added the following section for Release 10.2.1.3: • Configuring the External Admin Connect Properties on page 1109 Updated the following section for Release 10.2.1.3: • View and Edit Profile SMGR field descriptions on page 883
16	October 2025	Updated the following sections: • New Report field descriptions on page 1102 • Data Encryption on page 1482
15	July 2025	Updated the following section: • Editing administrative user roles on page 69 • Editing a custom role on page 183 • Modifying user accounts on page 219

Table continues…

Issue	Date	Summary of changes
14	June 2025	Updated the following section: • Adding G430 or G450 Branch Gateway to System Manager on page 936
13	May 2025	Updated the following sections: • Configuring email properties on page 1108 • About centralized licensing on page 1056
12	April 2025	Added the following sections for Release 10.2.1.1: • Certificate revocation list overview on page 1260 • HTTP proxy support checklist on page 1261 • Adding an HTTP proxy on page 1262 • Editing an HTTP proxy on page 1262 • Deleting an HTTP proxy on page 1263 • HTTP proxy field descriptions on page 1264 Updated the following sections for Release 10.2.1.1: • Schedule CRL Download field descriptions on page 1265 • CRL Download Configuration field descriptions on page 1267 • Refreshing elements on page 1348 • System Manager command line interface operations on page 1510 • Restoring a backup from a remote server on page 858 • Provisioning user certificate authentication on page 1275

Table continues…

Issue	Date	Summary of changes
11	December 2024	Added the following sections for Release 10.2.1: • Assigning a user to a group using XML on page 241 • Removing a user from a group using XML on page 242 • Group types on page 241 • Running force initialize data synchronization on page 989 • Command line interface alternative to Serviceability Agents on page 979 • Creating SNMP user profiles on page 980 • Listing SNMP user profiles on page 981 • Creating SNMP target profiles on page 981 • Listing SNMP target profiles on page 982 • Attaching and detaching target profiles from serviceability agents on page 982 • Listing agents attached to target profiles on page 983 • Listing target profiles attached to agents on page 983 • Creating notification filter profiles on page 983 • Listing notification filter profiles on page 984 • Attaching or detaching filter profiles to or from target profile serviceability agents on page 984 • Listing filter profiles attached to given target profiles and agent IP addresses on page 985 • Viewing the synchronization datasource on page 76 • Stopping a user synchronization job on page 88 • Deleting a user synchronization job history on page 88 Updated the following sections for Release 10.2.1: • User Bulk Editor field descriptions on page 224 • New User Provisioning Rule field descriptions on page 624 • Communication Manager, Messaging data, and IP Office synchronization on page 985 • Adding the synchronization datasource on page 75 • Editing the synchronization datasource on page 77 • Deleting a synchronization datasource on page 77 • Creating the user synchronization job on page 84 • Scheduling a user synchronization job on page 85 • Deleting a user synchronization job on page 86

Table continues…

Issue	Date	Summary of changes
		• Viewing Job Summary on page 89 • Adding a private contact to a user on page 271 • User Profile | Add field descriptions on page 285 • User Profile | Edit | <User Name> field descriptions on page 307 • User Profile | View | <User Name> field descriptions on page 328 • User Profile | Duplicate | <User Name> field descriptions on page 344 • Serviceability Agents on page 961
10	August 2024	Updated the section Adding a vCenter to Solution Deployment Manager on page 1419
9	August 2024	• Updated the section View and Edit Profile SMGR field descriptions on page 883 • Removed two sections.
8	June 2024	• Updated the section Geographic Redundancy prerequisites overview on page 99 • Updated the section Disaster recovery prerequisites on page 119
7	May 2024	• Removed two sections. • Updated the section Scheduler on page 1114
6	May 2024	• Added the section SAML sequence and flow diagram for SAML SSO authenticate for System Manager on page 1287 • Updated the section Communication Manager notify synchronization on page 1490 • Updated the section What is an announcement? on page 675 • Updated the section List of XML Schema Definitions and sample XMLs for bulk import on page 403
5	April 2024	• Updated the section Directory synchronization overview on page 72 • Updated the section Results of synchronization from the LDAP directory server to System Manager on page 73 • Updated the section External authentication on page 1271
4	April 2024	• Updated the section Installing a license file on page 1049 • Updated the section Configuring the IP Phone Group ID for an endpoint on page 755
3	March 2024	• Updated the section Installing language pack on System Manager on page 1525 • Updated the section Identity certificate management on page 1210 • Updated the section System Manager web console on page 35
2	January 2024	Updated the section System Manager command line interface operations on page 1510

Table continues…

Issue	Date	Summary of changes
1	December 2023	Initial issue of Release 10.2 document

Chapter 2: Overview

System Manager overview

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

System Manager includes the following shared management services:

Service	Description
Solution Deployment Manager	To: • Deploy Avaya Aura® applications. • Upgrade and migrate Avaya Aura® applications. **Note:** When an application is configured with Out of Band Management, Solution Deployment Manager does not support upgrade for that application. For information about upgrading the application, see the application-specific upgrade document on the Avaya Support website. • 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, and media modules - Session Manager - Branch Session Manager - AE Services With the Solution Deployment Manager client, you can: • Deploy Avaya Aura® applications • Upgrade System Manager • Install software patches for System Manager

Table continues…

Service	Description
Users	Provides features to administer users, shared address, public contact list, and information of system presence access control list. 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	To create user provisioning rules. When the administrator creates the user with the user provisioning rule, the system populates the user attributes from the rule. The administrator requires to provide minimal information.
Bulk import and export	To provide bulk import and export of user profiles and global settings.
Directory synchronization	To provide bidirectional synchronization of user attributes from System Manager to the LDAP directory server.
Elements	To provide features of individual components of System Manager. Some links provide access to generic features of System Manager. Most links provide access to features provided by System Manager components.
Events	To administer 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	To handle scenarios when the primary System Manager server fails or the data network fragments. In such a 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	To administer groups and roles. You can create and manage groups, roles, and permissions.
Licenses	To administer licenses for individual components of Avaya Aura® Unified Communication System.
Security	To: • Authenticate using certificates • Configure the certificate authority

Table continues…

Service	Description
System Manager data	To: • Back up and restore System Manager configuration data • Monitor and schedule jobs • Replicate data from remote nodes • Configure data retention settings and profiles for various services that System Manager provides
Tenant Management	To: • Create a tenant • Edit tenant details • Duplicate an existing tenant • Delete a tenant

Discontinued support for IP Server Interface (TN2312, commonly known as “IPSI”)

With Release 10.2, Communication Manager does not support the IP Server Interface (IPSI). As a result, access and functionality are removed. This means, the IPSI connected cabinets and gateways do not work with Communication Manager Release 10.2. Examples of IPSI connected cabinets and systems include G3cfs, G3csi, G3i, G3r, G3s, G3si, G3vs, G3x, G600, G650, MCC, SCC, CMC, IPSI, IP Server Interface, and IP port network.

Discontinued support also includes the TN8412, which previously paired with the TN8400 blade server. TN8412 was last supported with Communication Manager Release 5.x.

For more information, see the End of sale G650 document published on the Avaya Support website.

Log on to System Manager

Supported browsers

The following are the minimum tested versions of the supported browsers:

- Microsoft Chromium Edge Release 93
- Google Chrome Release 91
- Mozilla Firefox Release 93

Note:

- From Avaya Aura® Release 10.1 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

System Manager web console

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

Note:

- On a client, a single sign-on workflow must have the same domain name as System Manager. The domain name of the System Manager server must match that of the web client-server. For instance, if the hostname of System Manager is `smgr.ca.avaya.com`, the server with the web client can have a hostname such as `client.ca.avaya.com` or `client.us.avaya.com`.
- With System Manager, you can open seven tabs simultaneously. The default number of tabs to open is five. However, you can set the value to the maximum of seven on the System Manager Web Console. The pages that are opened in each tab should be from different Element Managers. If you open pages falling under the same Element Manager, you may encounter an error based on the operation you are performing. For example, editing the same station in two tabs may throw an error message.

The resolution of the System Manager web console is 1024×768. The System Manager web console provides the following:

- Corporate logo: You can add a logo on the web console.
- **Options** icon ( ): You can navigate to **Help**, **About**, **Change Password**, and **Log Out** links.
- **Shortcuts**: You can set shortcuts to various pages by hovering the mouse on menu options and dragging an item to the Shortcuts area. You can also delete the shortcuts.

  Note:

  If you have user preferences (shortcuts) associated with users in version 7.1.x or lower, they are not retained if you upgrade to version 8.0 or higher. You must recreate the shortcuts.
- Quick Navigator: You can type the name of the link to search. The web console displays all related links with the search text on the top-right corner of the page. You can click a link to navigate to the specific page.
- A message on the web console prompting you to restart the System Manager virtual machine after a patch installation if the kernel is upgraded.

All the operational links are available under different menus, such as, **Users**, **Elements**, **Services**, **Widgets**, and **Shortcuts**.

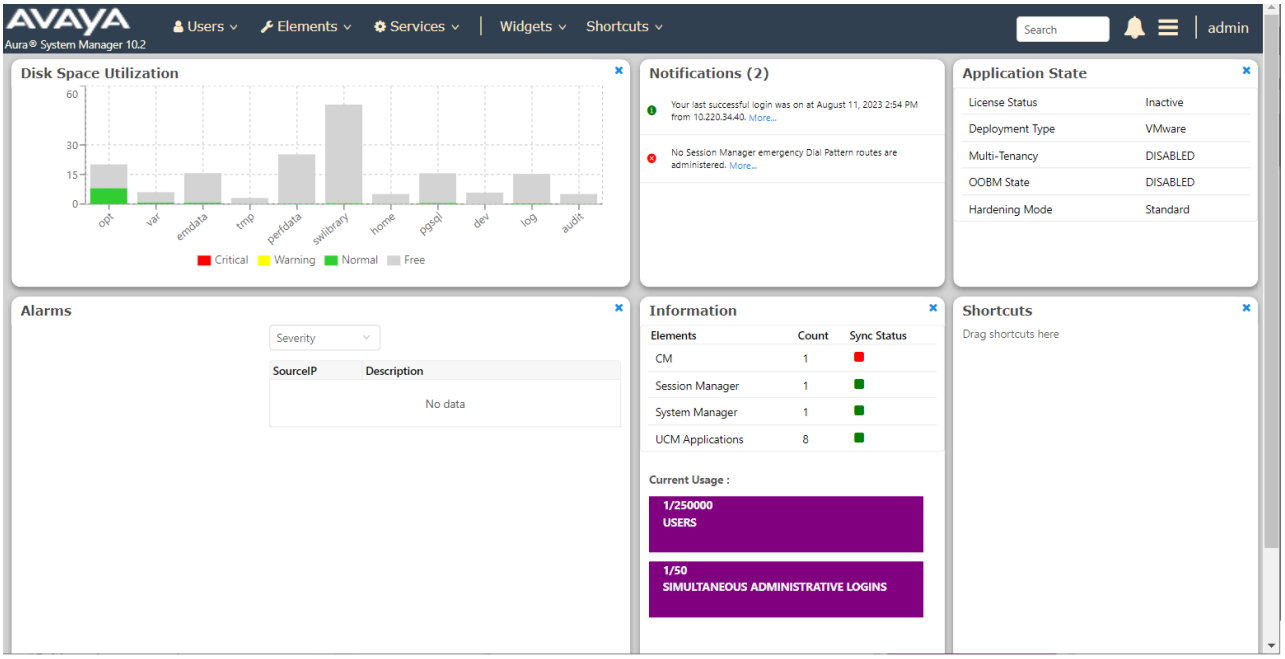
By default, the System Manager dashboard displays the following widgets:

- **Alarms**
- **Application State**
- **Notifications**
- **Disk Space Utilization**
- **Information**
- **Shortcuts**

Note:

After login, if you remove one of the default widgets, then it is available under the **Widgets** menu.

From System Manager Release 8.1.3.1 and later, you cannot close the **Notifications** widget. If you closed the **Notifications** widget during the last login on the System Manager Release 8.1.3 and earlier, then after upgrading to System Manager Release 8.1.3.1 and later, the system displays the default dashboard layout.



System Manager Dashboard field descriptions

Name	Description
Disk Space Utilization	The disk space utilization of the System Manager system in percentage (%). Displays the data of the following directories: • **`opt`:** Partition containing System Manager application-specific data. • **`var`:** Partition containing OS-specific data and some application-specific data for System Manager. • **`emdata`:** Partition containing System Manager application-specific data. Primarily contains Breeze (svars) and CS1k-specific data. • **`tmp`:** Standard RHEL `tmp` folder partition. • **`perfdata`:** Session Manager performance data collection folder. • **`swlibrary`:** Partition for storing System Manager application-specific data. • **`home`:** Partition for the `home` folder for System Manager OS users. • **`pgsql`:** Partition for the System Manager database. • **`dev`:** OS-specific partition. • **`log`:** Partition for the System Manager application and OS logs. • **`audit`:** Partition for the System Manager audit logs. The System Manager web console displays the following disk space utilization status: • Critical • Warning • Normal • Free To manage the `tmp` and `home` partitions, remove the files you created. **Note:** Do not perform any action to the /home/ucmdeploy/ directory and its files. For `swlibrary`, check `/swlibrary/HeapDump/`. From `swlibrary`, you can remove the following: • Service pack, Security Service pack, and Feature pack binaries. • `/swlibrary/LogsBackup_*.tar.gz` file. • Backup file.

Table continues…

Name	Description
	Ensure to copy the backup file to another location before you remove it. If you need to manage files and folders of any other partition, contact the Avaya Support website.
Notifications	The current notification from the application. From Release 8.1.3.1, the **Notifications** widget on the System Manager dashboard displays the user login information message and emergency Dial Pattern routes notification message for Emergency Location Management Solution. From Release 10.1.0.1, the **Notifications** widget displays the demo certificate usage message if Session Manager or WebLM has demo certificates installed. The messages in the **Notifications** widget are short. To view the complete details of each message, hover the cursor over the message. From System Manager Release 8.1.3.1 and later, you cannot close the **Notifications** widget. If you close the **Notifications** widget during your last login on System Manager Release 8.1.3 or earlier, then after upgrading to System Manager Release 8.1.3.1 or later, System Manager displays the default dashboard layout. If you set **Minimum TLS Version** to **TLSv1.0** or **TLSv1.1** on the **Services** > **Security** > **Configuration** > **Security Configuration** page, System Manager displays the following message in the **Notifications** widget: `Warning! TLS <1.0/1.1> is enabled. For increased security, it is recommended that the Minimum TLS Version be set to TLS 1.2 or higher if these protocol levels can be supported in your configuration.`
Shortcuts	The shortcut of the menu options. You can drag and drop your favorite menu options in the **Shortcuts** section.

Table continues…

Name	Description
Alarms	The alarms data of the application. You can filter the alarms by **Severity**, **Age (in days)**, and **Element Type**. The following are the alarm types available based on **Severity**: • Critical : Displays the number of critical alarms • Major : Displays the number of major alarms • Indeterminate : Displays the number of uncategorized alarms • Minor : Displays the number of minor alarms • Warning : Displays the number of warning alarms The alarms are categorized under the following day ranges when you filter the alarms based on **Age (in days)**: • 0 to 30 days • 30 to 60 days • 60 to 90 days • 90 to 120 days The dashboard also displays the source IP Address and description of the alarms.
Information	The **Information** section displays the application name, number of application instances, synchronization status of the application, and current usage. Current usage lists the number of users and simultaneous administrative logins.
Application State	The current status of the application and its major feature configurations, such as License Status, Deployment Type, Multi-Tenancy, OOBM State, and Hardening Mode.

Options icon ( )

Button	Description
Help	Displays the help documentation page.
About	Displays the System Manager Release and build details.
Change Password	Displays the Change Password window.
Log Out	Logs off from the System Manager web console.

Logging on to the System Manager web console

About this task

The System Manager web console is the main interface of Avaya Aura® System Manager. You must log on to the 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 from System Manager depend on your assigned role.

Before you begin

Deploy the System Manager OVA.

Procedure

1. On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, the System Manager URL.

   In the security deployments, System Manager displays the Login Warning Banner page.
2. **(Optional)** On the Login Warning Banner page, click **Continue**.
3. In the **User ID** field, type the user name.
4. In the **Password** field, type the password.
5. 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 do not match, System Manager displays an error message and prompts you to enter the user name and password again.

   Once you log in, depending on the system and element configurations, System Manager can display one or more error or notification messages in an Alert Messages pop-up window. For information about these messages, see the “System Manager alert messages at logon” section.
6. Click **OK** to continue.

System Manager message with login details

Important:

From Release 8.1.3.1, System Manager displays the last login information in the **Notifications** widget on the dashboard.

In System Manager Release 8.1.3, after your first successful login, when you log in to the System Manager web console, System Manager displays the Welcome <SystemManager_UserName> pop-up window at your every subsequent login.

Note:

When you log in to the System Manager web console for the first time, System Manager does not display the Welcome <SystemManager_UserName> pop-up.

Depending on the last successful or unsuccessful login details, System Manager displays the messages in the Welcome <SystemManager_UserName> pop-up window.

For example:

```
You have successfully logged into System Manager

Your last successful login was at <Month> <Date>, <YYYY> <HH:MM>
<AM/PM> from <Source_system_IPAddress>
Your last unsuccessful login was at <Month> <Date>, <YYYY> <HH:MM>
<AM/PM> from <Source_system_IPAddress>
There were <n> unsuccessful login attempts since last successful login
```

If a user logs into the System Manager command-line interface and then logs in to the System Manager web console, then this message also displays the successful and unsuccessful login attempts with the Timestamp and IP address details of the source system.

Note:

After each successful login, on the System Manager web console or CLI, System Manager resets the unsuccessful login count.

- If the login attempt is successful without any unsuccessful login attempt, System Manager displays the following message. For example:

```
You have successfully logged into System Manager

Your last successful login was at <Month> <Date>, <YYYY> <HH:MM>
<AM/PM> from <Source_system_IPAddress>
There were 0 unsuccessful login attempts since last successful login
```

- If the login attempt is successful after one or more unsuccessful login attempts, System Manager displays the following message. For example:

```
You have successfully logged into System Manager

Your last successful login was at September 16, 2020 11:18 AM from
13.12.18.24
Your last unsuccessful login was at September 16, 2020 11:20 AM
from 13.12.18.24
There were 1 unsuccessful login attempts since last successful login
```

System Manager alert messages at login

When you log in to the System Manager web console, depending on the system and element configurations, System Manager can display one or more of the following messages.

System Manager license error message

```
System Manager requires a valid license from Avaya. Use of this
software without a valid license is a violation of the Avaya EULA and
can result in legal action by Avaya. Please install a System Manager
license file on WebLM or immediately discontinue use of this software.
```

To resolve this error, install the System Manager license file.

System Manager Geographic Redundancy feature entitlement license error message

```
The System Manager Geo-Redundancy Feature requires a valid license from
Avaya with the Geo-Redundancy Feature Entitlement. Use of the System
Manager Geo-Redundancy Feature without a valid license from Avaya with
the Geo-Redundancy Feature Entitlement is a violation of the Avaya EULA
and can result in legal action by Avaya. Please install a System
Manager License file on WebLM with the Geo-Redundancy Feature
Entitlement or immediately disable use System Manager Geo-Redundancy.
```

To resolve this error, install the System Manager license file.

Appliance Virtualization Platform license error message

```
Warning - This instance of Avaya Aura® Appliance Virtualization
Platform is currently unlicensed. Note: each instance of Appliance
Virtualization Platform is separately licensed and ordered. For
example, if you or the Avaya Channel Partner would like to install two
instances of the same type of products, then two products of that type
must be ordered. Appliance Virtualization Platform is licensed via
WebLM with license files obtained from PLDS. Please consult the
Appliance Virtualization Platform 7.1.2 or later user documentation for
more details onto how to acquire and install a license file. This
message will continue to be displayed until the system is correctly
licensed. Failure to license the system is in violation of the Avaya
Global Software License Agreement for the product. Please immediately
place an order using the normal Avaya ordering process to obtain the
required license. Avaya Aura® Appliance Virtualization Platform (AVP)
License Error Mode: Grace period expires: 01/09/2017 If the grace
period expires, AVP will enter License Restricted Mode and AVP
Management functionality will be restricted. Check license status on /
Home/Services/Solution Deployment Manager (SDM)/Application Management/
Location/Hosts/ for impacted AVP hosts.
```

If the grace period of the Appliance Virtualization Platform license file is less than 15 days or Appliance Virtualization Platform is in License Error Mode or License Restricted Mode, System Manager displays the AVP License Error message.

For information about Appliance Virtualization Platform license and administration, see *Deploying Avaya Aura® Appliance Virtualization Platform*.

Session Manager emergency Dial Pattern routes message

System Manager displays the following message only on the Release 8.1.3 system:

```
No Session Manager emergency Dial Pattern routes are administered. To
insure proper emergency number handling and routing, please administer
Routing Locations, Routing Policies, and Dial Patterns per emergency
calling guidelines.
```

Note:

From Release 8.1.3.1, System Manager displays the Session Manager emergency Dial Pattern routes notification message for Emergency Location Management Solution in the **Notifications** widget on the dashboard.

For information about administering routing locations, routing policies, and dial patterns for emergency calling, see *Administering Avaya Aura® Session Manager*.

Avaya Demo Certificate warning message

- From Release 10.1.0.1, System Manager displays the following message, if Session Manager has demo certificates installed:

  ```
  Warning: The presence of demo or temporary identity certificates
  with
  upcoming expiration dates has been identified on one or more
  Session
  Managers. These certificates contain deprecated key sizes and
  signatures that do not meet current NIST standards. You must
  replace
  the certificates prior to expiry with Avaya Aura® System Manager
  signed, Enterprise PKI, or Public CA certificates. Failure to
  replace
  the certificates before expiration will likely result in an
  unplanned
  service outage upon or after certificate expiration. Certificate
  expiration dates are detailed in the latest version of the Product
  Support Notice PSN020514u available at support.avaya.com.
  ```

  To remove the default (demo) certificates, see the PSN020514 on the Avaya support site. When you add or remove Session Manager demo certificates, System Manager updates the Alert Messages dialog box and Notifications widget only after a day.

- From Release 10.1.0.1, System Manager displays the following message, if WebLM has demo certificates installed:

  ```
  The presence of demo or temporary identity certificates with
  upcoming expiration dates has been identified in this system for
  the WebLM service. These certificates contain deprecated key
  sizes and signatures that do not meet current NIST standards. You
  must replace the certificates prior to expiry with Avaya Aura®
  System Manager signed, Enterprise PKI, or Public CA certificates.
  ```

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	Retype the new password.

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

Configuring the operating system single-user mode credentials for the root user

About this task

From System Manager Release 10.1.0.2, you can use the **`setSingleUserModeCred.sh`** script to set the credentials for the single-user mode login. With these credentials the super user can reboot the operating system to edit, and access the GRUB (GRand Unified Bootloader) menu for emergency maintenance or troubleshooting purpose. Without configuring these credentials, you cannot reboot the operating system into single-user mode.

Only the root users can run the **`setSingleUserModeCred.sh`** script and set the credentials for the single-user mode login.

Note:

The **`setSingleUserModeCred.sh`** script is not applicable for Software-Only deployments.

Before you begin

Deploy the System Manager Release 10.1 OVA and apply the System Manager Release 10.1.0.2 patch.

Procedure

1. Log in to the System Manager command-line interface with root credentials.

   System Manager displays the following message:

```
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
 *                                                                                     *
 *   WARNING: The password for booting into single user mode is not configured.  *
 *   This needs to be done at the earliest to allow booting into single user     *
 *                 mode for maintenance or emergency in future.                  *
 *                                                                                     *
 * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

2. Type the `sh setSingleUserModeCred.sh` command.

   System Manager displays the prompt to change the user name.

   The default super user name is *avboot*.

3. To change the user name, type `Yes`.
4. At the **Enter a Super User Name which is not a system account** prompt, type a unique super user name.
5. At the **Enter the GRUB's Super User Password** prompt, type a super user password.

   The password must match with the System Manager password policy. You can run the **`setSecurityPolicy --display-only`** command to view the current password policies.

6. At the **Re-enter the GRUB's Super User Password to confirm** prompt, retype the super user password.

System Manager generates the GRUB configuration file and displays the following message:

```
Single User mode login credentials applied successfully
```

Logon information for users with administrator privilege

This logon information applies only to users with administrator privilege.

- After installation, when you log on to System Manager for the first time, type the administrator privilege credentials that you created during the deployment or upgrade of System Manager.

  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 using the default password.

Important:

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

- Using a disabled account to log on
- Using an invalid password
- Exceeding the maximum number of failed logon attempts limit
- Using an expired password

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

Password strength policy enforcement on page 50

Certificate based authentication

Certificate-based authentication overview

With System Manager 7.1, you can disable the password-based login and configure the certificate-based authentication for system login. The certificates for this authentication can be issued by:

- System Manager as the default certificate authority
  - Using System Manager user interface
  - Using System Manager CLI
- Third-party certificate authority

Configuring username retrieval from certificate

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.

2. In the 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, navigate to **Provision User Certificate Authentication**.
5. Select the **Certificate Purpose**.
6. Select the certificate field names to be used to retrieve the username.
7. Click **Save**.

Enabling certificate-based authentication

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Configuration** > **Security Configuration**.
3. On the Security Configuration page, click **SMGR**.
4. In **Cert based authentication** section, enable the required options.

   Caution:

   Enabling the **System Manager User Interface** option disables the password-based authentication for the System Manager user interface. The System Manager user interface is accessible using a valid certificate.
5. Click **Commit**.

Creating certificate using System Manager default CA

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **RA Functions** > **Add End Entity**.
4. Type the **Username**.
5. Type the **Password** and **Confirm 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. Click **Add**.

   The system displays the message `End Entity <username> added successfully`.
7. In the navigation pane, click **Public Web**.
8. Click **Create Browser Certificate**.

9. Type the **Username** and **Password**.
10. Click **OK**.
11. Click **Enroll**.
12. **(Optional)** If the certificate is not installed automatically, click **Install Certificate**.

Next steps

If the automatic certificate installation fails, download the certificate and install it in the web browser manually.

Generating certificate from CLI

About this task

Use this procedure to generate a user-specific certificate for System Manager to facilitate the certificate-based authentication.

Before you begin

- To reach the System Manager command-line interface, use one of the following methods:
  - Open vSphere Client (HTML5) and click the **Console** tab or the icon.
  - Use PuTTY.

Procedure

1. Log in to the System Manager command-line interface.
2. Type `getUserAuthCert`, and press `Enter`.
3. Provide the user password and press `Enter`.
4. Type the enrollment password and press `Enter`.
5. Retype the enrollment password and press `Enter`.
6. Type a password for the keystore and press `Enter`.
7. Retype the keystore password and press `Enter`.
8. Type the username and press `Enter`.
9. To generate an identity certificate in the corresponding format, type one of the following and press `Enter`:
   - For `PKCS12` format, type `1`.
   - For `JKS` format, type `2`.
   - For `PEM` format, type `3`.
   - For `PEM-UNENC` format, type `4`.
   - For `PEM-PKCS8` format, type `5`.
   - For `PEM-PKCS8-AES256-CBC` format, type `6`.

10. Press `Enter`.

    The system displays the path of the generated identity certificate.

11. Download the certificate and install it in the web browser.

Certificate-based SSH login

Certificate-based CLI access overview

System Manager does not provide a default Command Line Interface (CLI) access to a user. To gain CLI access, an administrator must provide Base OS permissions to the user.

CLI access can be enabled using the following:

- System Manager Web Console
- Putty-CAC

Enabling CLI using Putty-CAC

Procedure

1. Download Putty-CAC for certificate-based login from https://risacher.org/putty-cac/.
2. Open a putty session.
3. In the **Host name (or IP address)** field, enter the hostname or IP address of System Manager.
4. In the navigation pane, expand the **Connection** > **SSH**, and click **CAPI**.

   Options controlling MS CAPI SSH authentication dialog box opens.

5. Select the **Authentication methods** check box.
6. Click **Browse** to select your identity certificate.

   Note:

   Ensure that you add the identity certificate in the browser manually or use an ActivClient tool to add the CAC certificate in the browser.

7. Click **OK** to select the certificate for CAPI Authentication.
8. Click **Open** to start the SSH session.
9. On the CLI, type the username provided in the certificate and press the **Enter** key on the keyboard.

   The system displays the pop-up window, Signing data with your private exchange key.

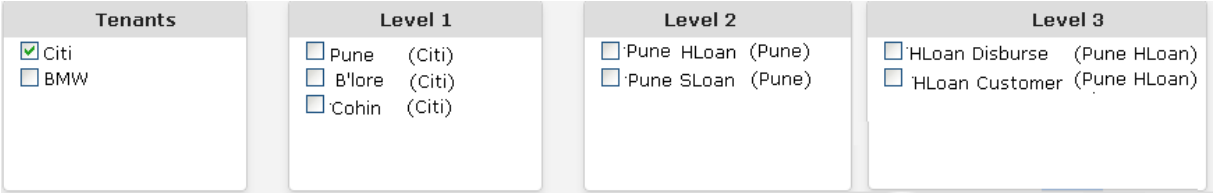
10. On the Signing data with your private exchange key window, click **OK**.

    The system provides access to the System Manager CLI.

Tenant Management web console

From the 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.

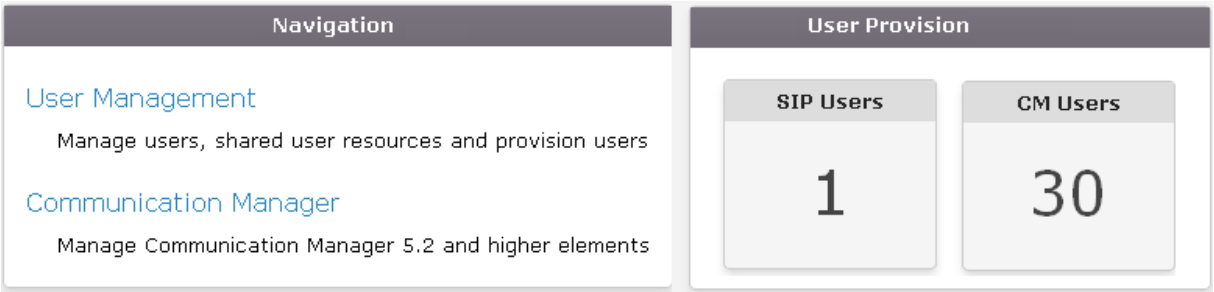


- View all child levels of the selected item in the subsequent panel.
  - When the tenant administrator selects an item, the system:
    - Selects all parent items of the selected item.
    - Displays the child levels of the selected item in the subsequent panel.
  - When the tenant administrator clears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

Note:

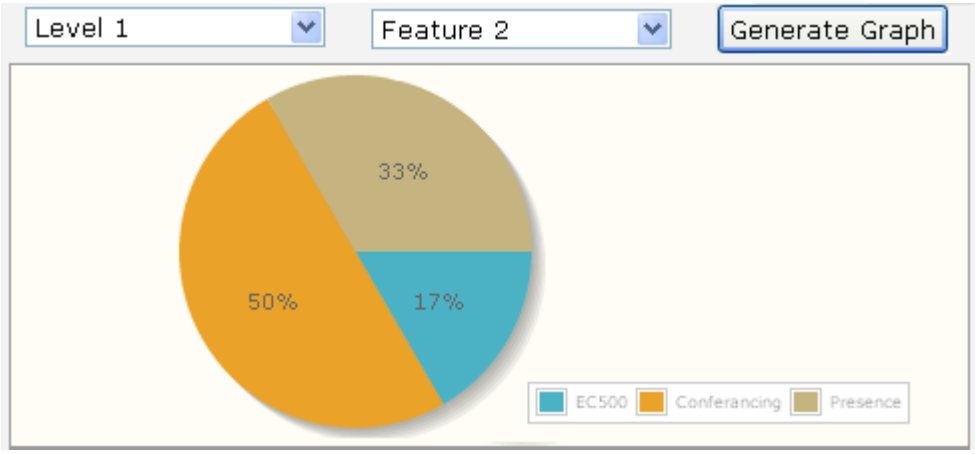
Select at least one tenant. If you do not select a tenant, the system displays a message.

- Gain access to:
  - User Management
  - Communication Manager. Only if the role has permissions to Communication Manager



- View the **User Provision** section that displays the number of SIP 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, 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

Multi Tenancy on page 1292

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 three 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 password threshold expires and before the threshold to disable the account. The password remains locked until the system administrator resets the password.

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 14.

- Passwords must contain a combination of the following characters: a-z, A-Z, 0-9, {, }, |, (,), <, >, ,, /, ., =, [,], ^, _, @, !, $, %, &, -, +, ", :, ?, `, \, or ;
- Passwords do not require a minimum character type. However, the default is one lowercase, one uppercase, one numeric, and one special character. The sum cannot exceed the minimum total length.
- Password can contain a maximum of 2 consecutive characters. The valid values are from 1 through 5. The default value is 2.
- Password can contain a maximum number of 4 consecutive characters from the same character type. The valid values are from 1 through 5. The default value is 4.
- Passwords must not be your user ID, in forward or reverse order.
- Passwords must not be a value based on a dictionary word.

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

You can disable the password strength policy.

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 value for blocking the number of previous password is 10.

Password lockout policy enforcement

The lockout policy limits 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 login attempts.

By default, if you make five unsuccessful consecutive attempts within 10 minutes, the system locks you out for 10 minutes.

Editing password policies

About this task

A user with the system administrator role can edit the password settings.

Note:

If the Password policy is enabled on earlier release system, then System Manager retains the values configured on the earlier system, when you upgrade System Manager from earlier release to Release 10.1.

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the 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**.

   For more information on password policies, contact the system administrator.
6. **(Optional)** To undo your changes and return to the previous page, click **Cancel**.

Related links

Password policies field descriptions on page 52

Password policies field descriptions

This page is accessible only for system administrator.

The password policy applies to all administrator logins. There are no exceptions.

Aging

Name	Description
Enforce password aging policy	The option to enable or disable the password aging policies. By default, the password aging policy is disabled. To enforce the password aging policies, select the check box. If you clear the check box, the password aging policy is not applicable. **Note:** If the password policy is disabled earlier and you enable it then all users whose password now match the criteria are asked to change their password.
Enable expired password change	If this is enabled, you can change the password after it expires. If this is disabled, only the system administrator can change the password. When you log in with the system administrator-provided password, you must change the password.
Expiration period	The maximum number of days you must change the password. The valid values are from 2 through 365. The default value is 90.

Table continues…

Name	Description
Expiration warning	The number of days for password expiry before which the password expiration warning message must be sent to the user. The valid values are from 1 through 15. From Release 10.1, the default value is 10. For earlier release system, the default value is 7. If you upgrade to Release 10.1, the older values are retained, if policy was enabled on the earlier system. When you log in to System Manager and the number of days for password expiration warning is reached to the set value, System Manager forces you to immediately change the password. For example, with the default values configuration, if the value in **Expiration period** is set to 90 days and **Expiration warning** is 10 days, then System Manager forces you to change the password on the 80 day.
Minimum age for password change	The minimum number of days for password age. The valid values are from 0 through 7. The default value is 3. Ensure that the expiration period is greater than the minimum password age.

History

Name	Description
Enforce policy against previously used passwords	The option to enable or disable the password policy against previously used passwords. By default, the password policy against previously used passwords is disabled. To enforce the password policy against previously used passwords, select the check box. If you clear the check box, the password policy against previously used passwords is not applicable.
Previous passwords blocked	The number of latest passwords that the system maintains in history. You cannot reset your password to these values. The valid values are from 1 through 99. From Release 8.1.3, the default value is 10. For earlier release system, the default value is 6.

Strength

Name	Description
Enforce password content standards	The option to enable or disable the password content standards. By default, the password content standards is disabled. To enforce the password content standards, select the check box. If you clear the check box, the password content standards is not applicable.
Minimum total length	The minimum number of characters to use in the password. The password can be of 6 to 25 characters. From Release 8.1.3, the default value is 14. For earlier release system, the default value is 8.
Minimum by character Type: Lower case	The minimum number of lowercase characters to use in the password. The default value is 1.
Minimum by character Type: Upper case	The minimum number of uppercase characters to use in the password. The default value is 1.
Minimum by character Type: Numeric case	The minimum number of numeric characters to use in the password. The default value is 1.
Minimum by character Type: Special case	The minimum number of special characters to use in the password. The default value is 1.
Maximum repeated consecutive characters	The maximum number of repeated consecutive characters. The valid values are from 1 through 5. The default value is 2. For example, if the maximum repeated consecutive characters value is set to 2: • Valid password is: Buildd123$ • Invalid password is: Builddd123$
Maximum consecutive characters from same character type	The maximum number of consecutive characters from the same character type. The valid values are from 1 through 5. The default value is 4. For example, if the maximum repeated consecutive characters of the same character type is set to 4: • Valid password is: Build123$ • Invalid password is: Build12345$

Lockout

Name	Description
Lockout	The option to enable or disable lockout after failed log-in attempts. By default, this is disabled. To enforce the lockout after failed log-in attempts, select the check box. If you clear the check box, the lockout after failed log-in attempts is not applicable.
Consecutive Invalid Login Attempts	The number of consecutive failed attempts in the configured **Interval for Consecutive Invalid Login Attempts**. The valid values are from 1 through 20. The default value is 5.
Interval for Consecutive Invalid Login Attempts	The time interval in minutes between invalid log-in attempts. The valid values are from 0 through 120. The default value is 10.
Lockout Time	The number of minutes that the account must be locked. The valid values are from 0 through 120. From Release 10.1, the default value is 10. For earlier release system, the default value is 2. If the value is set to 0 and consecutive failure attempts reached to the set value, the user account gets locked, and only the system administrator or another admin can reset the password. If there is no other admin, reset the password by using the local login password reset. For information about resetting the password, see *Troubleshooting Avaya Aura® System Manager*.

For example, with the default values configuration, if you reach up to 5 number of consecutive invalid login attempts within 10 minutes, then the user account gets locked. After 10 minutes, you can log in.

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

Managing System Manager command line password policy

setSecurityPolicy command

With Release 8.1.3, you can modify the default password policy settings of System Manager using the **`setSecurityPolicy`** command. This command is only applicable for changing or setting up the password for the CLI or root user created during deployment.

Note:

When you create a user through the System Manager web console, the System Manager web console password policy applies.

You can run the **setSecurityPolicy** command in the following modes:

- **Interactive mode:** This is the default mode for operating this command. You can display, change, restore, and refresh the password policy settings.
- **Non-interactive mode:** You can view the status, display the current settings, restore the standard default settings, and refresh the current profile, including any custom settings.

Syntax

```
setSecurityPolicy
```

Displays the interactive mode where you can change the password policy settings.

Syntax

```
setSecurityPolicy [--status] [--display-only] [--restore-standard] [--refresh-custom]
```

--status	Displays the password policy settings status.
--display-only	Displays all the password policy settings.
--restore-standard	Removes all customized values and restores the password policy settings to the default profile settings.
[--refresh-custom]	Refreshes the custom profile settings in case of backup and restore.

Related links

Managing the command line password policies on page 56
Changing the password policies through CLI on page 57
Viewing the password policy status on page 60
Displaying the password policies on page 60
Restoring the default password policy settings on page 61
Refreshing the default password policy settings on page 62

Managing the command line password policies

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type **setSecurityPolicy**.
3. When the system prompts for the [sudo] password, type the password.

   System Manager displays the set of options.

   For example:

```
Main Menu:

    Loaded Profile Type: standard
         Custom Profile: yes   (Custom Settings: 1)

1) Display Current Property Settings
2) Change Property Settings
3) Restore Standard Property Settings and Exit
```

```
4) Refresh Current Property Settings and Exit
5) Exit (no settings changed)

Select Action:
```

Where:

- **Loaded Profile Type:** Specifies the profile selected during deployment. The options are:
  - **standard**
  - **DoD/Hardened**
- **Custom Profile:** The options are:
  - **no**: Specifies that System Manager is using the default values from the loaded profile. This is the default value.
  - **yes**: Specifies that a user has made some changes to customize the security profile.

    When the **Custom Profile** setting is **yes**, System Manager displays the **Custom Settings** field with the number of changes made to the default password profile.

    For example:

    ```
    Custom Settings: <n>
    ```
  - **Restore Standard Property Settings and Exit:** When you make a change to the password policy settings, System Manager displays this option to remove all the changes and restore the standard property settings to the default values.

4. In **Select Action**, type one of the following:
   - **1:** to display the current property settings.
   - **2:** to change the current property settings.
   - **3:** to restore the standard property settings and exit the command.
   - **4:** to refresh the current property settings and exit the command.
   - **5:** to exit the command without saving the changes.

Related links

setSecurityPolicy command on page 55

Changing the password policies through CLI

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type **`setSecurityPolicy`**.
3. When the system prompts for the [sudo] password, type the password.

   System Manager displays the set of options.

   For example:

   ```
   Main Menu:
   ```

```
    Loaded Profile Type: standard
         Custom Profile: yes   (Custom Settings: 1)

1) Display Current Property Settings
2) Change Property Settings
3) Restore Standard Property Settings and Exit
4) Refresh Current Property Settings and Exit
5) Exit (no settings changed)

Select Action:
```

4. In **Select Action**, type `2`.

   System Manager displays the set of options to change the parameters.

```
Change Property Settings:

    Loaded Profile Type: standard
         Custom Profile: yes   (Custom Settings: 1)

  Note: [Current Value: M=modified C=customized D=disabled]

 1) Return to Main Menu
 2) Change minimum password length [14]
 3) Change minimum days between password changes [1]
 4) Change maximum days before password expires [-1: D]
 5) Change password expiration warning (days) [10]
 6) Change mimimum required uppercase characters [0: D]
 7) Change mimimum required lowercase characters [0: D]
 8) Change mimimum required numeric characters [0: D]
 9) Change minimum required special characters [0: D]
10) Change required difference from previous password [4]
11) Change minimum required character classes [3]
12) Change maximum repeated characters [2]
13) Change maximum class repeat [10: C]
14) Change inactive account disable time (days) [0]
15) Change remember previous passwords [10]
16) Change max login attempts before lock out [0: D]
17) Change root lock out allowed [no]
18) Change lock out time (seconds) [900]
19) Change unlock time (seconds) [600]
20) Change delay (seconds) after failed login attempt [1]

Select Action:
```

5. In **Select Action**, type the number for which you want to change the value.

   For example, if you want to change the minimum password length, type `2`.

   When you type `2`, System Manager displays the following prompt.

```
Changing minimum password length:
    Current Value: 14  (Minimum: 6, Maximum: 25)

Enter new value:
```

6. In **Enter new value**, type the required value.

   When you type the value, System Manager displays the following prompt with the number of pending changes made.

   For example:

```
Change Property Settings:
```

```
    Loaded Profile Type: standard
         Custom Profile: yes   (Custom Settings: 1)
        Pending Changes: 1

  Note: [Current Value: M=modified C=customized D=disabled]

 1) Return to Main Menu
 2) Change minimum password length [10: M]
 3) Change minimum days between password changes [1]
 4) Change maximum days before password expires [-1: D]
 5) Change password expiration warning (days) [10]
 6) Change mimimum required uppercase characters [0: D]
 7) Change mimimum required lowercase characters [0: D]
 8) Change mimimum required numeric characters [0: D]
 9) Change minimum required special characters [0: D]
10) Change required difference from previous password [4]
11) Change minimum required character classes [3]
12) Change maximum repeated characters [2]
13) Change maximum class repeat [10: C]
14) Change inactive account disable time (days) [0]
15) Change remember previous passwords [10]
16) Change max login attempts before lock out [0: D]
17) Change root lock out allowed [no]
18) Change lock out time (seconds) [900]
19) Change unlock time (seconds) [600]
20) Change delay (seconds) after failed login attempt [1]

Select Action:
```

7. To return to the main menu, in **Select Action**, type `1`.

   System Manager displays the main menu.

   For example:

```
Main Menu:

    Loaded Profile Type: standard
         Custom Profile: yes   (Custom Settings: 1)
        Pending Changes: 1

1) Display Current Property Settings
2) Change Property Settings
3) Apply Changes and Exit
4) Exit (discarding all pending changes)

Select Action:
```

8. To apply the changes to the password policy settings, in **Select Action**, type `3`.

   System Manager applies the profile changes, updates the system settings, and displays the number of changes made to the password policy settings.

   For example:

```
Loaded Profile Type: standard
         Custom Profile: yes   (Custom Settings: 1)
        Pending Changes: 1

Applying Profile Changes:

    Loaded Profile Type: standard
         Custom Profile: yes   (Custom Settings: 2)

Updating System Settings:
```

```
    Executing pam-settings.sh
    Executing password-policy.sh
```

Related links

setSecurityPolicy command on page 55

Viewing the password policy status

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type **`setSecurityPolicy`** `--status`, and press `Enter`.

   System Manager displays the password policy status.

   Following is the example where the default password policy has not been changed.

```
    Loaded Profile Type: standard
         Custom Profile: no
```

   Following is the example where one setting of the default password policy has been changed.

```
Loaded Profile Type: standard
         Custom Profile: yes   (Custom Settings: 1)
```

Related links

setSecurityPolicy command on page 55

Displaying the password policies

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type **`setSecurityPolicy`** `--display-only`, and press `Enter`.

   System Manager displays the configured password policy.

   For example:

```
setSecurityPolicy --display-only

    Loaded Profile Type: standard
         Custom Profile: no

                 Property                    Value            Notes

                   minimum password length:     14
     minimum days between password changes:      1
      maximum days before password expires:     -1  Disabled
        password expiration warning (days):     10
     mimimum required uppercase characters:      0  Disabled
     mimimum required lowercase characters:      0  Disabled
       mimimum required numeric characters:      0  Disabled
       minimum required special characters:      0  Disabled
required difference from previous password:      4
        minimum required character classes:      3
```

```
                maximum repeated characters:      2
                       maximum class repeat:      4
      inactive account disable time (days):      0
                remember previous passwords:     10
        max login attempts before lock out:      0  Disabled
                      root lock out allowed:     no
                    lock out time (seconds):    900
                      unlock time (seconds):    600
delay (seconds) after failed login attempt:      1
```

Related links

setSecurityPolicy command on page 55

Restoring the default password policy settings

About this task

When you make some changes to customize the default password policy and later to restore the default password policy for the current profile, use the following procedure.

- In the Interactive mode, do the following:
  1. Type **`setSecurityPolicy`**.
  2. When the system prompts for the [sudo] password, type the password.

     System Manager displays the set of options.

     For example:

     ```
     Main Menu:

         Loaded Profile Type: standard
              Custom Profile: yes   (Custom Settings: <n>)

     1) Display Current Property Settings
     2) Change Property Settings
     3) Restore Standard Property Settings and Exit
     4) Refresh Current Property Settings and Exit
     5) Exit (no settings changed)

     Select Action:
     ```

  3. In **Select Action**, type `3`.

     System Manager updates the system settings and restores the default password policy settings.

     ```
     Loaded Profile Type: standard
              Custom Profile: no

     Updating System Settings:
         Executing pam-settings.sh
         Executing password-policy.sh
     ```

- In the Non-interactive mode, do the following:
  1. Type **`setSecurityPolicy`** `--restore-standard`, and press `Enter`.
  2. When the system prompts for the [sudo] password, type the password.

System Manager updates the system settings and restores the default password policy settings.

```
Loaded Profile Type: standard
         Custom Profile: no

Updating System Settings:
    Executing pam-settings.sh
    Executing password-policy.sh
```

Related links

setSecurityPolicy command on page 55

Refreshing the default password policy settings

About this task

When a custom profile is restored during a backup and restore, use the following procedure to apply the changes to the system settings.

- In the Interactive mode, do the following:
  1. Type **`setSecurityPolicy`**.
  2. When the system prompts for the [sudo] password, type the password.

     System Manager displays the set of options.

     For example:

     ```
     Main Menu:

         Loaded Profile Type: standard
              Custom Profile: no

     1) Display Current Property Settings
     2) Change Property Settings
     3) Refresh Current Property Settings and Exit
     4) Exit (no settings changed)

     Select Action:
     ```

  3. In **Select Action**, type `4`.

     System Manager refreshes the system settings.
- In the Non-interactive mode, do the following:
  1. Type **`setSecurityPolicy`** `--refresh-custom`, and press `Enter`.
  2. When the system prompts for the [sudo] password, type the password.

     System Manager updates the system settings and refreshes the default password policy settings.

Related links

setSecurityPolicy command on page 55

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.

Editing Session Properties

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the 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

Session Properties field descriptions on page 63

Session Properties field descriptions

Name	Description
Maximum Session Time	The maximum time in minutes a session can remain active. The default value is 120. The valid values are 10 through 1440.
Maximum Idle Time	The maximum time in minutes a session can remain idle. The default value is 10. The valid values are 10 through 1440. **Note:** • You must set the session idle time out to 10 minutes before running a security scan against System Manager using tools like Nessus or IBM AppScan. • The maximum idle time must not exceed the maximum session time.
Maximum Sessions Per User	The maximum number of active sessions per user with the same set of credentials. The default is 5. The valid values are 1 through 25.

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

Inactive Account Deactivation Policy field descriptions

Name	Description
Maximum Inactive Period	The maximum time in days that a user can remain inactive. The valid values are from 7 through 365. The default value is 35. You cannot disable this.
Account Deactivation Warning	The maximum time in days before which the account deactivation warning is sent. The valid values are from 1 through 60. The default value is 5. **Note:** This is applicable for all users except username admin user.
Maximum Inactive Period for accounts with Temporary Password	The maximum time in days for accounts with temporary password. The valid values are from 1 through 7. The default value is 1.

Button	Description
Save	Saves the changes made on the current page.
Cancel	Cancels the changes and returns to the previous page.

Security settings

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

Login warning banner

System Manager provides the following:

- Login warning banner: The system administrator can change the text in the login warning banner.
- Additional Postlogin warning banner: In the security deployment, after you log in, System Manager displays a warning banner. You can change only the configurable part of the message.

The Last Login Data window displays the following:

- Last successful login
- Server for the last successful login
- Number of unsuccessful login attempts (if any)

Editing the login warning banner

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the navigation pane, click **Security** > **Policies**.

3. On the Policies page, in the Security Settings section, click **Edit**.
4. On the Security Settings page, do the following:
   a. In the Login Warning Banner area, edit the text as appropriate.
   b. **(Optional)** For security deployments, in the Additional Post Login Banner Message area, change only the configurable part of the additional text as appropriate.

      Note:

      You cannot change the actual message. You can change only the configurable part of the post-login banner text.
5. Click **Save**.

Security Settings field descriptions

Name	Description
Login Warning Banner	The text displayed during System Manager login. The system administrator can change this text.
Additional Post Login Banner Message	The text displayed after logging on to System Manager. The text contains two components, the login banner and the additional text. Only the additional text is configurable.

Button	Description
Save	Saves the changes on the Login Warning Banner page.
Cancel	Ignores the changes and returns to the previous page.

Login Failure Message

From System Manager Release 10.1, you can configure the text to display on the login page when a System Manager user fails to log in to the System Manager web console.

Editing the login failure message

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the navigation pane, click **Security** > **Policies**.
3. On the Policies page, in the Login Failure Message section, click **Edit**.
4. On the Login Failure Message page, in **Login Failure Message**, type the required text.
5. To save the changes, click **Save**.

   The default message is:

   ```
   Need more help? please contact support team.
   ```

   If you fail to log in with the credentials, System Manager displays the following message:

   ```
   Login error. Please check your username and password.
   ```

```
<Customized Text>
```

Login Failure Message field descriptions

Name	Description
Login Failure Message	The text displayed on the System Manager login page. The system administrator can change this text. You can provide a login failure message of a maximum of 500 characters.

Button	Description
Save	Saves the changes on the Login Failure Message page.
Cancel	Cancels the changes and returns to the previous page.

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.

Adding the corporate logo

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the 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 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 for 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

Customized Interface field descriptions on page 67

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

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

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

Reimporting the SSO cookie domain value

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the navigation pane, click **Security** > **Policies**.
3. In the Single Sign-on Cookie Domain section, click **Edit**.
4. In the **Single Sign-on Cookie Domain**, select the appropriate domain based on the FQDN of the deployed servers.
5. Click **Save**.
6. Log out and close all browser windows you opened when logging on to the System Manager server.
7. To accept the updated cookies from the new Single Sign-On (SSO) cookie domain name, clear the browser cache.

Administrative users

Viewing administrative user details

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the Administrative Users page, select the required user ID.

   The system displays the User Details page with the administrative user details.

Adding an administrative user

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the Administrative Users page, click **Add**.

   The system displays the Step 1: Identify the new user page.
4. On the Add New Administrative User page, enter the user ID, full name, and email address.
5. In the **Authentication Type** field, select **Local** or **External**.
6. Do one of the following:
   - In the **Temporary password** and **Re-enter password** fields, type the same password.
   - Click **Generate Password**.

     Note:

     The auto-generated password applies if **Authentication Type** is set to **Local**.
7. Click **Commit and Continue**.

   The system displays the Step 2: Assign Role(s) page.
8. Select the required roles to be assigned to the user, and click **Commit**.

Editing administrative user details

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the Administrative Users page, select the required user ID.
4. On the User Details page, make the required changes.

5. Click **Commit**.

Editing administrative user roles

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the Administrative Users page, select the required user ID.
4. Click **Select Roles**.
5. On the User Roles page, select the required roles for the administrative user and click **Commit**.

Note:

When a user edits any role assigned to their account and commits the changes in System Manager, the user is logged out immediately and redirected to the login page of System Manager web console.

For example, if the user `user@domain.com` is logged into System Manager web console and edits one of the roles assigned to their account, the user is logged out of System Manager immediately and redirected to the login page of System Manager web console.

Note:

When a user edits a role in System Manager, all other users assigned to that role are logged out after their next action and redirected to the login page of System Manager web console.

For example, User 1 is assigned the `System Admin role`, while User 2 and User 3 are assigned the `Test role`. If User 1 edits the `Test role`, User 2 and User 3 are logged out after their next action and redirected to the login page of System Manager web console.

Enabling an administrative user

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the Administrative Users page, click the required user ID.

   The system displays the User Details page.
4. In **User Status**, click **Enabled**.
5. Click **Commit**.

Disabling an administrative user

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the Administrative Users page, do one of the following:
   - Select the user, and click **Disable**.
   - Click the required user ID, click **Disabled**, and click **Commit**.

Deleting an administrative user

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the Administrative Users page, select the users to delete.
4. Click **Delete**.
5. On the Delete Users page, click **Delete** to confirm the user deletion.

Terminating administrative user sessions

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the Administrative Users page, click **Active Sessions**.
4. On the Active Sessions page, select the sessions to terminate.
5. Click **Terminate**.

Administrative Users field descriptions

Name	Description
User ID	The unique user identification of the administrative user.
Name	The name of the administrative user.
Roles	The list of roles assigned to the administrative user.
Type	The type of the administrative user.
Account Status	The status of the administrative user’s account.

Button	Description
Add	Displays the Add New Administrative User page on which you add the administrative users.
Disable	Use this button to disable the selected administrative users.
Delete	Displays the Delete Users page on which you confirm deletion of selected administrative users.
Active Sessions	Displays the Active Sessions page on which you can terminate active administrative user sessions.
Refresh	Refreshes the element information in the table.

Add New Administrative User field descriptions

Step 1: Identify the new user

Name	Description
User ID	Unique user identification of the administrative user.
Authentication Type	The type of authentication. The options are: • **Local**: Avaya Authentication Service performs the user login authentication. • **External**: The enterprise authenticates the user login.
Full Name	The full name of the administrative user.
E-Mail	The email address of the administrative user.
Temporary Password	The first-time login password for the administrative user account.
Re-enter Password	The password that you re-enter for confirmation.

Button	Description
Generate Password	Generates a password for the administrative user.
Commit and Continue	Saves the user details and takes you to Step 2: Assign Role(s).
Cancel	Cancels the operation for adding an administrative user.

Step 2: Assign Role(s)

Button	Description
Role Name	The name of the role.
Elements	The elements that are a part of the role.
Description	A description of the role.

Button	Description
Commit	Saves the selected user roles for the new administrative user.
Cancel	Cancels the operation for selecting the roles for the new administrative user.

Chapter 3: Directory synchronization

Directory synchronization overview

System Manager integrates with 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:

- Microsoft Active Directory 2012
- Microsoft Active Directory 2016
- Microsoft Active Directory 2019
- Microsoft Active Directory 2022
- OpenLDAP 2.4.46
- 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 Microsoft Active Directory or other supported directory server 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.

Note:

If there are multiple directory server datasource configurations, you can only delete a user from System Manager using the sync from datasource configuration that created/owns the user.

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.

Note:

If there are multiple directory server datasource configurations, you can only delete a user from System Manager using the sync from datasource configuration that created/owns the user.

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. From System Manager Release 8.0 and later, you can delete the Enterprise/LDAP user from the System Manager web console. However, if the user is still available in the LDAP directory server, the system synchronizes the user in System Manager even after you delete the user from System Manager on next synchronization job.

Adding the synchronization datasource

Procedure

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

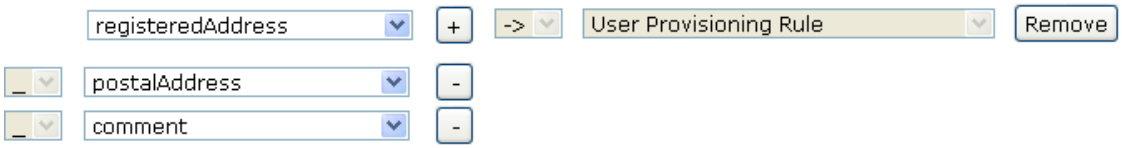
   If the connection is successful, the system displays the status icon. Click the status icon to view the message. Continue with the next step to map attributes in System Manager to LDAP attributes.

   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:
   a. 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.

   b. Select an LDAP attribute that you map to the user provisioning rule.

   c. 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.
- The **New** button for adding a synchronization data source is enabled if users have **Create Data Source** permission within Directory Synchronization or have logged in as an administrator. If users do not have these permissions, the **New** button is disabled.

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 78
Results of using the user provisioning rule on page 215

Viewing the synchronization datasource

Procedure

1. On the System Manager web console, click **Users** > **Directory Synchronization**.
2. In the navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Synchronization Datasources** tab.
4. Click the records that you want to view.
5. Click **View**.

   You can view all parameters in read-only mode.

   Note:

   The **View** button for viewing a synchronization data source is enabled if users have **View** or **Edit** permissions within Directory Synchronization or have logged in as an administrator. If users do not have these permissions, the **View** button is disabled.

Related links

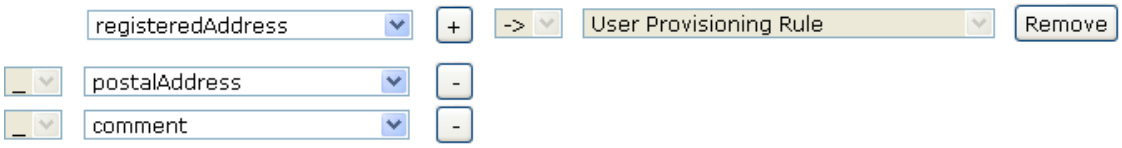
User active synchronization job field descriptions on page 86

Editing the synchronization datasource

Procedure

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

Note:

The **Edit** button for editing a synchronization data source is enabled if users have **Edit Data Source** permission within Directory Synchronization or have logged in as an administrator. If users do not have these permissions, the **Edit** button is disabled.

Related links

User synchronization datasource field descriptions on page 78
Results of using the user provisioning rule on page 215

Deleting a synchronization datasource

Procedure

1. On the System Manager web console, click **Users** > **Directory Synchronization**.

2. In the 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.`
- The **Delete** button for deleting a synchronization data source is enabled if users have **Delete Data Source** permission within Directory Synchronization or have logged in as an administrator. If users do not have these permissions, the **Delete** button is disabled.

User synchronization datasource field descriptions

Directory Parameters

Name	Example values	Description
Datasource Name	Win2K8ADA	The name to identify the directory server. You might require the name later to create a synchronization job.
Host	111.140.111.126	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 directory server that has permissions to create or update users.
Password	<password>	The password to connect to the directory server. From Release 8.1.3, you can enter up to 256 characters for the directory server.
Port	389, 636	The port number of the directory used for an LDAP connection. It is recommended to use a secure SSL connection. Typically on LDAP servers, port 389 is for a non-SSL connection and port 636 is for a secure 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.

Table continues…

Name	Example values	Description
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 directory server. The default value is inetOrgPerson.
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 directory server. 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 the directory server.
Allow Null values in LDAP	False when you clear the check box	The option to allow null values to be inserted by System Manager in LDAP.
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.

Table continues…

LDAP Attribute	System Manager Attribute	Description
userPrincipalName	loginName **Note:** If you are using Microsoft Active Directory for external authentication with System Manager, the attribute userPrincipalName of the user in the external server must contain a valid value.	The attribute that defines the login name in System Manager.
sn	surname	The attribute that defines the last name of the user.
givenName	givenName	The attribute that defines the given name.
displayName	displayName	The attribute that defines the display name.
middleName	middleName	The attribute that defines the middle name.
mail	email	The attribute that defines the communication profile handle.
postalCode	postalCode	The attribute that defines the postal code of the user. The system creates the address of the user, Registered_User_Address.
streetAddress	streetAddress	The attribute that defines the postal code of the user. The system creates the address for the user with a name.
preferredLanguage	preferredLanguage	The preferred language of the user. Mapping of the LDAP attribute to preferredLanguage must be in the LanguageCode_CountryCode format. For the format that the preferredLanguage attribute supports, see “Preferred languages”.
mail	otherEmail	The attribute for the secondary email of the user.
roomNumber	room	The room number of the user. The system creates the address of the user, Registered_User_Address.
co	country	The country of the user. The system creates the address of the user, Registered_User_Address.
otherTelephone	otherBusinessPhone	The secondary business telephone number of the user, Registered_User_Address address.
facsimileTelephoneNumber	fax	The fax number of the user, Registered_User_Address address.

Table continues…

LDAP Attribute	System Manager Attribute	Description
homePhone	homePhone	The residential phone number of the user, Registered_User_Address.
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 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.

Table continues…

LDAP Attribute	System Manager Attribute	Description
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, if CS 1000 is supported. 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.

Table continues…

LDAP Attribute	System Manager Attribute	Description
memberOf	userRoles	When synchronized with Enterprise Directory, the roles, rights, and restrictions for administrators are automatically configured for the correct role and inherit the capability of roles. You can map the userRoles attribute to one of the following: • Groups in LDAP. For example in Active Directory, the attribute memberOf contains the fully qualified group name, such as CN=DnsAdmin,CN=Users,DC=avaya,DC=com. The system searches for DnsAdmin role name. • Other LDAP attribute: System searches for the exact name with the value in LDAP attribute that matches with the role in System Manager.

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 77
Preferred languages on page 83

Preferred languages

System Manager supports the following locales to set as language preference.

Language	Format
Arabic	ar
Bulgarian	bg
Chinese (Simplified)	zh_CN
Chinese (Traditional)	zh_TW
Czech	cs
Danish	da
Dutch	nl

Table continues…

Language	Format
English (Canada)	en_CA
English (United Kingdom)	en_GB
English (United States)	en_US
Estonian	et
Finnish	fi
French (Canada)	fr_CA
French (France)	fr_FR
German (Germany)	de_DE
Greek	el
Hebrew	iw
Hungarian	hu
Irish	ga
Italian (Italy)	it_IT
Japanese (Japan)	ja_JP
Korean (Korea)	ko_KR
Latvian	lv
Lithuanian	lt
Maltese	mt
Polish	pl
Portugese (Brazil)	pt_BR
Romanian	ro
Russian (Russia)	ru_RU
Slovak	sk
Spanish (Mexico)	es_MX
Swedish	sv
Ukrainian	uk

Creating the user synchronization job

Procedure

1. On the System Manager web console, click **Users** > **Directory Synchronization**.
2. In the 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:
   - Click **Run Job** to run the job immediately.
   - Select the **Schedule job for future execution** check box to schedule the job at a later time.

     You can delete a job that you 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.
- The **Create New Job** button for creating a user synchronization job is enabled if users have **Create Job** permission within Directory Synchronization or have logged in as an administrator. If users do not have these permissions, the **Create New Job** button is disabled.

Related links

User active synchronization job field descriptions on page 86

Scheduling a user synchronization job

Procedure

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

   Note:

   The **Create New Job** button for scheduling a user synchronization job is enabled if users have **Create Job** permission within Directory Synchronization or have logged in as an administrator. If users do not have these permissions, the **Create New Job** button is disabled.

Deleting a user synchronization job

Procedure

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

   The web console displays a confirmation message.
5. Click **OK**.

   Note:

   - You can delete a job that is scheduled to run in the future.
   - The **Delete Job** button for deleting a user synchronization job is enabled if users have **Delete Data Source** permission within Directory Synchronization or have logged in as an administrator. If users do not have these permissions, the **Delete Job** button is disabled.

User active synchronization job field descriptions

Name	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 87

Synchronization job history field descriptions

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

Stopping a user synchronization job

Procedure

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

   The web console displays a confirmation message.
5. Click **OK**.

   Note:

   - The **Stop Job** button is available for jobs in the Running state.
   - The **Stop Job** button for stopping a user synchronization job is enabled if users have **Create Job** permission within Directory Synchronization or have logged in as an administrator. If users do not have these permissions, the **Stop Job** button is disabled.

Deleting a user synchronization job history

Procedure

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

   The web console displays a confirmation message.
5. Click **OK**.

   Note:

   - You can delete a job created for user synchronization.
   - The **Delete Job** button for deleting a user synchronization job history is enabled if users have **Delete Data Source** permission within Directory Synchronization or have logged in as an administrator. If users do not have these permissions, the **Delete Job** button is disabled.

Viewing Job Summary

Procedure

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

Note:

The **View Job Summary** button for viewing a synchronization data source is enabled if users have **View** or **Edit** permissions within Directory Synchronization or have logged in as an administrator. If users do not have these permissions, the **View Job Summary** button is disabled.

Related links

Viewing Job Summary field descriptions on page 89

Viewing Job Summary field descriptions

Name	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.
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.

From Release 8.0.1, System Manager also supports Geographic Redundancy in a mixed deployment environment.

From Release 7.0.1, System Manager supports deployment on different server types and different deployment modes in Geographic Redundancy. System Manager supports mixed:

- Servers from any combination of Avaya Supplied Avaya Solutions Platform 130 severs supported for System Manager.
- The primary System Manager server running as the only Avaya application on the server, while the secondary System Manager running along with other Avaya applications on another server and vice-versa.
- Servers from both customer-provided virtualized environment and Avaya Solutions Platform 130.

  For example, the primary System Manager server can be on Avaya Solutions Platform 130 and the secondary System Manager server can be on a customer-provided virtualized environment.

The following are some 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 deploy 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 interact 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 whether 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 127

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 the primary System 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 the System Manager manages. For example, a Session Manager server or a Communication Manager server.

In the context of System Manager Geographic Redundancy, the elements can be classified as follows:

- Geographic Redundancy-unaware element: An element that does not support Geographic Redundancy, such as Avaya Aura® Session Manager Release 6.2.x and earlier. If you have a Geographic Redundancy-unaware element that is configured and managed by the primary System Manager server, and if the primary System Manager goes down or a Split brain scenario occurs, then you cannot use the secondary System Manager to manage the element either automatically or with a simple click of a button. If you need to manage a Geographic Redundancy-unaware element, then you need to make the changes manually. The manual changes differ from one Geographic Redundancy-unaware element to another.
- Geographic Redundancy-aware element: An element that supports Geographic Redundancy, such as Avaya Aura® Session Manager Release 6.3 and later. These elements can leverage the services of the primary or the secondary System Manager servers, either automatically or with the simple click of a button. The Geographic Redundancy-aware elements are classified in the following types:
  - Elements capable of automatically switching between the primary and secondary System Manager servers depending on the state of the System Manager servers - If the primary System Manager server goes down or a Split brain scenario occurs and you activated the secondary System Manager server, then the element can detect it and depending on the current state of the System Manager server, the element automatically switches to the appropriate System Manager server, so that the element can be managed by it.

    For example, if you have a System Manager 8.1.x Geographic Redundancy deployment, (Sunny Day) with a few Session Manager 8.1.x servers configured and you activated the secondary System Manager due to a network split, then each Session Manager server detects this. If the primary System Manager is not reachable, then the Session Manager

server automatically switches to the active secondary System Manager server. If the primary System Manager server is reachable, then the element does not switch to the secondary System Manager, even though it is active. This does not mean that you cannot manage them. To manage the element through the secondary System Manager server, on secondary System Manager go to the Manage Elements page, select the element, and then click the **More Options** > **Force Manage** option.

- Elements that require manual switch - If the primary System Manager server goes down or a Split brain scenario occurs, and you need to manage the element from the secondary System Manager server, then on secondary System Manager go to the Manage Elements page, select the element, and then click the **More Options** > **Force Manage** option. This step is required to manage such elements from the secondary System Manager server.

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 the Geographic Redundancy setup

In a Geographic Redundancy setup, the two standalone System Manager servers that you designate as primary and secondary servers must meet the following requirements:

- Contain the same version of the software that includes software packs.
- Contain the same profile for primary and secondary System Manager Geographic Redundancy virtual machines. For example, if the primary System Manager contains Profile 2, the secondary System Manager must also contain Profile 2.
- Contain the same version of the System Manager software that includes service pack and software patches.
- 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.
- Communicate with each other over the network by using the IP address and FQDN.
- In the Geographic Redundancy setup, the primary and secondary System Manager must use the same VFQDN.
- Have a synchronized network time.
- 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.
- Have open required ports 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/.
- Have T1 as the minimum data pipe between the primary and the secondary System Manager server. T1 provides 1.544 Mbps.

- Have network latency that is less than 500 ms.
- In the Geographic Redundancy setup, if you need to configure the outbound firewall rules, then you need to add the peer IP addresses on the primary and secondary System Manager servers.

Hardware resource and parameter for the Geographic Redundancy setup

#	Hardware Resource or Parameter	Similar on Primary and Secondary? (Mandatory or Recommended)	Does System Manager take care?	Notes
1	64 bit architecture	Mandatory	No	Require 64 bit system for both servers. Require x86_64 architecture to support System Manager provided operating system and then for the Geographic Redundancy setup.
2	Byte Order (Big or Little endian)	Mandatory	Yes	This depends on CPU architecture.
3	64 bit OS	Mandatory	Yes	-
4	PostgreSQL major version	Mandatory	Yes	-
5	PostgreSQL minor version	Recommended	Yes	-
6	Number of CPUs	Recommended	No	Mandatory CPU reservation: • Profile 2: 6 • Profile 3: 8 • Profile 4: 18 Validated along with profile validation during Geographic Redundancy configuration.

Table continues…

#	Hardware Resource or Parameter	Similar on Primary and Secondary? (Mandatory or Recommended)	Does System Manager take care?	Notes
7	Memory	Recommended	No	Mandatory memory reservation: • Profile 2: 12 GB • Profile 3: 18 GB • Profile 4: 36 GB Validated along with profile validation during Geographic Redundancy configuration.
8	Storage	Recommended	No	Mandatory Total storage of 120 GB is required for profile 2 Validated along with profile validation during Geographic Redundancy configuration.
9	System Manager profile	Mandatory	Yes	System Manager validates during Geographic Redundancy configuration.
10	System Manager version	Mandatory	Yes	System Manager validates during Geographic Redundancy configuration.
11	Synchronized Time	Mandatory	Yes	System clock and hardware clock must be set if required keeping synchronized Time on primary and secondary. System Manager validates during Geographic Redundancy configuration.

Key tasks for Geographic Redundancy

Prerequisites

Ensure that the two System Manager servers meet the requirements that are defined in “Prerequisites for 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 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 from the primary System Manager server.
  - During the system maintenance or upgrades, Geographic Redundancy replication must be disabled. After maintenance activity is complete, you must enable Geographic Redundancy replication if it was manually or automatically disabled due to the maintenance activity.

    Note:

    If the heartbeat between the two System Manager servers in which the Geographic Redundancy replication is enabled stops due to network connectivity failure or the server failure, 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.

    When the network connectivity is restored, enable the Geographic Redundancy replication. For information about the network latency and bandwidth, see “Prerequisites for the Geographic Redundancy setup”.

    For information about the auto-disable scenarios, see Scenarios of auto-disable for the Geographic Redundancy system on page 107.
  - 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 appropriate section in this document.

Prerequisites before configuring Geographic Redundancy

Geographic Redundancy prerequisites overview

Before enabling and configuring Geographic Redundancy, do the following:

1. Configure CRL download on the secondary System Manager server.

   Note:

   By default, CRL is valid only for 7 days. Therefore, you must configure Geographic Redundancy before the expiry date of CRL.

2. Add the trusted certificate of the primary server to the secondary System Manager server.

   Note:

   This step is mandatory. Complete this step even if you are replacing the certificates with third-party signed certificates.

3. If the certificate is replaced on the primary server by a third-party signed certificate, then the same certificate type must be replaced on the secondary server by the same third-party CA.

   For example, If a third-party CA replaces *Management Container TLS Service* signed certificate on the primary server, then the same type of certificate must be replaced on the secondary server by the same third-party CA.

4. Install a third-party certificate on both servers on both servers before and after the Geographic Redundancy configuration.
5. Ensure that a third-party CA certificate is added to the trust store of both System Manager servers.
6. The replaced certificate must have a full chain (id certificate ->inter CA (if present) certificate -> root CA certificate) and must contain the correct FQDN/VFQDN in the required places.
7. **Note:**

   Configuring CRL download is mandatory for Geographic Redundancy.

   If the CRL URL for the third-party is not accessible from System Manager, then set **Certificate Revocation Validation** from **BEST_EFFORT** to **NONE** on the **Security** > **Configuration** > **Security Configuration** > **Revocation Configuration** page.

   When you click **Commit**, System Manager displays the following message:

   ```
   Changes are updated successfully. An Application server restart is
   required for changes to take effect. Click Ok to restart it now.
   Click Cancel to restart it later. Web Console would be unavailable
   for 10-15 minutes during a restart.
   ```

Related links

Configuring CRL download on the secondary System Manager server on page 102
Adding the trusted certificate of primary server to the secondary System Manager server on page 103
Configuring CRL download on the secondary System Manager server on page 102
Adding the trusted certificate of primary server to the secondary System Manager server on page 103

Copying the CRL URL

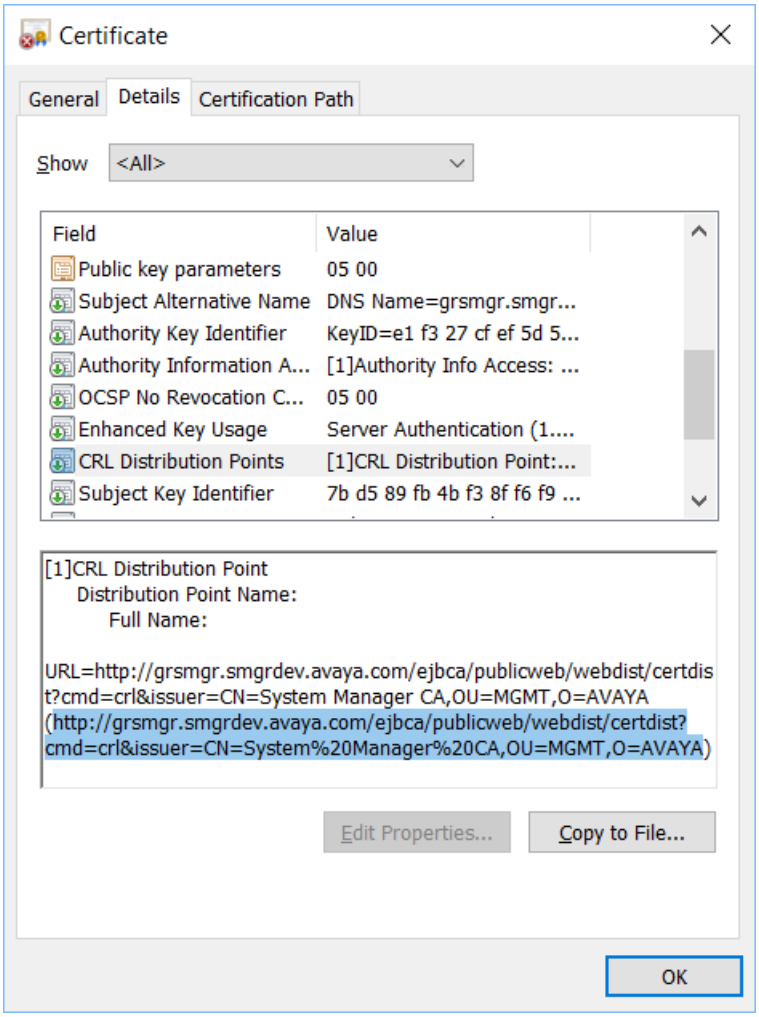
Procedure

1. On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, the System Manager URL.

2. On the address bar, click the Lock icon.
3. Click **View certificates**.
4. On the Certificate dialog box, do the following:
   a. Click on the **Details** tab.
   b. Scroll down and click the **CRL Distribution Points** field.

      The system displays the CRL URL in the text box.

      For example: http://<vFQDN>/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA



   c. Press **Ctrl+C** and copy the URL in Notepad for configuring CRL download in the Geographic Redundancy set up.
   d. Click **OK**.

Configuring CRL download on the secondary System Manager server

Procedure

1. Access the login page of the primary System Manager server.
2. Copy the CRL of the browser certificate.

   For information about copying the CRL URL, see “Copying the CRL URL.”
3. Replace the vFQDN in the CRL with the IP address of the primary System Manager server.

   For example, the CRL in the certificate is:

   ```
   http://<vFQDN>/ejbca/publicweb/webdist/certdist?
   cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
   ```

   The new CRL for the certificate will be:

   ```
   http://<ip-address>/ejbca/publicweb/webdist/certdist?
   cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
   ```

   Where, <*vFQDN*> and <*ip-address*> are the respective vFQDN and IP address.

   Note:

   If you installed a third-party certificate on System Manager servers, this step is not required. If third-party certificate, then configure CRL URL of the third-party certificate for CRL download.
4. Log on to the secondary System Manager web console.
5. On the System Manager web console, click **Services** > **Security**.
6. In the navigation pane, click **Configuration** > **CRL Download**.
7. On the CRL Download Configuration page, click **Add**.

   System Manager displays the Schedule CRL Download page.
8. In **Job Name**, type the job name.
9. In **Job Frequency**, set the frequency and recurrence to schedule the job within a few minutes after the CRL addition.

   For more information, see Schedule CRL Download field descriptions.
10. Copy the new CRL URL from Notepad and paste the URL in the **Configure CRL Distribution Point** field.

    For information about copying the CRL URL, see “Copying the CRL URL.”

    CRL URL example:

    ```
    http://<ip-address>/ejbca/publicweb/webdist/certdist?
    cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
    ```
11. Click **Add**, and then click **Commit**.

    Ensure that the job is completed successfully.

Next steps

Add the trusted certificate of the primary server to the secondary System Manager server.

Adding the trusted certificate of primary server to the secondary System Manager server

Procedure

1. Log in to the primary System Manager web console.
2. On the System Manager web console, click **Services** > **Security**.
3. In the navigation pane, click **Certificates** > **Authority**.
4. Click **CA Functions** > **CA Structure & CRLs**.
5. Click **Download PEM file**.
6. Log in to the secondary System Manager web console.
7. On the System Manager web console, click **Services** > **Inventory**.
8. In the navigation pane, click **Manage Elements**.
9. On the Manage Elements page, select the System Manager certificate and click **More Actions** > **Manage Trusted Certificates**.
10. On the Manage Trusted Certificates page, click **Add**.
11. Click **Choose File** and select the previously downloaded PEM file.
12. Click **Retrieve Certificate**, and then click **Commit**.

Configuring Geographic 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 you change CLI passwords on primary and secondary System Manager servers.

  60 days after the System Manager CLI password expires, Geographic Redundancy becomes nonoperational. You must set a new password on primary and secondary System Manager servers for Geographic Redundancy to become operational again.
- Ensure that the two System Manager servers meet the requirements that are defined in “Prerequisites for 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:

      Because 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:
     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 Geographic Redundancy health.

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

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 105
Geographic Redundancy field descriptions on page 116

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.
- Ensure that CLI passwords on primary and secondary System Manager servers do not expire.

  60 days after the System Manager CLI password expires, Geographic Redundancy becomes nonoperational. You must set a new password on primary and secondary System Manager servers for Geographic Redundancy to become operational again.

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:

   Because 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

Geographic Redundancy field descriptions on page 116
Disabling the Geographic Redundancy replication on page 106
Activating the secondary System Manager server on page 108
Changing the TLS version of System Manager on page 1189
Deactivating the secondary System Manager server on page 109
Restoring the primary System Manager server on page 109
Converting the primary System Manager server to the standalone server on page 114
Re-establishing trust for Solution Deployment Manager elements on page 1400

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

Geographic Redundancy field descriptions on page 116
Activating the secondary System Manager server on page 108
Changing the TLS version of System Manager on page 1189
Deactivating the secondary System Manager server on page 109
Restoring the primary System Manager server on page 109
Enabling the Geographic Redundancy replication on page 105

Scenarios of auto-disable for the Geographic Redundancy system

System Manager triggers the auto-disable and 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.

  When the network connectivity is restored, enable the Geographic Redundancy replication.

  For information about the network latency and bandwidth, see “Prerequisites for the Geographic Redundancy setup”.
- If one of the two servers becomes nonoperational, the system triggers auto-disable on the server that is operational.
- If the PostgreSQL database disk partition utilization reaches threshold limit of 75%, System Manager generates a Warning alarm.

  If the PostgreSQL database disk partition utilization reaches threshold limit of 85%, System Manager triggers auto-disable and generates a Critical alarm.

  Note:

  If auto-disable is due to PostgreSQL database disk space issue, contact Avaya Support. Do not enable the Geographic Redundancy until the database disk partition space issue is resolved.

Activating the secondary System Manager server

About this task

- 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.

Before you begin

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

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy** > **GR Health**.
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 the secondary 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.

   Because 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

Geographic Redundancy field descriptions on page 116

Disabling the Geographic Redundancy replication on page 106
Changing the TLS version of System Manager on page 1189
Deactivating the secondary System Manager server on page 109
Restoring the primary System Manager server on page 109
Enabling the Geographic Redundancy replication on page 105

Deactivating the secondary System Manager server

Before you begin

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

Procedure

1. On the System Manager web console, click **Services** > **Geographic Redundancy** > **GR Health**.
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 information, see “Restoring the primary System Manager server”.

Related links

Geographic Redundancy field descriptions on page 116
Disabling the Geographic Redundancy replication on page 106
Activating the secondary System Manager server on page 108
Changing the TLS version of System Manager on page 1189
Restoring the primary System Manager server on page 109
Enabling the Geographic Redundancy replication on page 105

Restoring the primary System Manager server

Before you begin

- Create the snapshot of the primary and secondary System Manager servers.

Note:

Delete the snapshot after the data is successfully restored.

- 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.

Note:

It is recommended to first deactivate secondary System Manager server and then start the **Restore Data** operation. If the Geo Data Restore operation is performed using Secondary Data while Secondary is in active state, then there could be data loss or inconsistency if changes are made on the secondary System Manager server while the Geo Data Restore operation is in progress.

If you choose to retain the primary System Manager database as part of Geo Data Restore then this note does not apply to you.

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.

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**

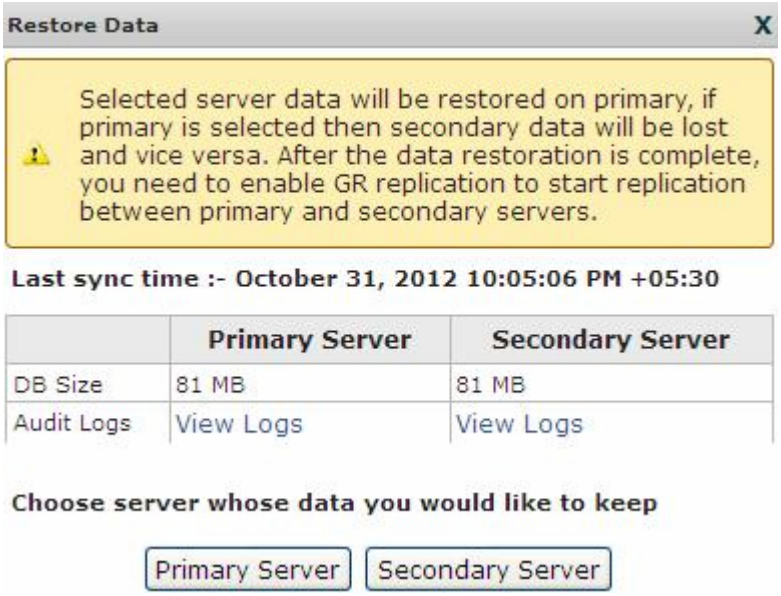
     The system keeps the primary System Manager server data. The data on the secondary System Manager server is lost.

     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**.



System Manager displays the Restore Status dialog box.

System Manager 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 with administrator privilege CLI user credentials.
   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.

- Because 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

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 105
Deactivating the secondary System Manager server on page 109
Geographic Redundancy field descriptions on page 116
Disabling the Geographic Redundancy replication on page 106
Activating the secondary System Manager server on page 108
Changing the TLS version of System Manager on page 1189
Deactivating the secondary System Manager server on page 109
Enabling the Geographic Redundancy replication on page 105

Reconfiguring Geographic Redundancy

Before you begin

- Ensure that the two System Manager servers meet the requirements that are defined in “Prerequisites for the Geographic Redundancy setup”.
- Create the snapshot of the primary and secondary System Manager servers.

  Note:

  Delete the snapshot after the configuration of Geographic Redundancy.
- 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**

     Type the admin user name that you use to log on to the primary System Manager web console.
   - **Primary Server Password**

     Type the admin password that you use to log on to the primary System Manager web console.
   - **Primary Server IP**
   - **Primary Server FQDN**
4. Click **OK**.

   Note:

   Because 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:
     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 Geographic Redundancy health.
   - Log in to the secondary System Manager server as system administrator by using the command line interface and perform the following:
     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 System Manager web console, enable the Geographic Redundancy replication.

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.

Note:

You can also reconfigure secondary System Manager to the standalone server by performing the same steps.

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 105
Geographic Redundancy field descriptions on page 116

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 115
View Profile:HealthMonitor field descriptions on page 889
Edit Profile:HealthMonitor field descriptions on page 889
GR Health field descriptions on page 117

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. To restart the service, type `service systemMonitor restart`.

   The changes take 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.

Name	Description
IP	Displays the IP address of the secondary System Manager server.

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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. • **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.

Prerequisites for configuring disaster recovery

Disaster recovery prerequisites

To configure the disaster recovery for the primary System Manager server, do the following:

1. Set up a new primary System Manager server.
2. Configure CRL download on the primary System Manager server.

   Note:

   By default, CRL is valid only for 7 days. Therefore, you must configure disaster recovery before the expiry date of CRL.
3. Add the trusted certificate of the secondary System Manager server to the new primary System Manager server.

   Note:

   This step is mandatory. Complete this step even if you are replacing the certificates with third-party signed certificates.
4. If the certificate is replaced on the primary server by a third-party signed certificate, then the same certificate type must be replaced on the secondary server by the same third-party CA.

   For example, If a third-party CA replaces *Management Container TLS Service* signed certificate on the primary server, then the same type of certificate must be replaced on the secondary server by the same third-party CA.
5. Install a third-party certificate on both servers on both servers before and after the Geographic Redundancy configuration.
6. Ensure that a third-party CA certificate is added to the trust store of both System Manager servers.
7. The replaced certificate must have a full chain (id certificate ->inter CA (if present) certificate -> root CA certificate) and must contain the correct FQDN/VFQDN in the required places.
8. **Note:**

   Configuring CRL download is mandatory for Geographic Redundancy.

   If the CRL URL for the third-party is not accessible from System Manager, then set **Certificate Revocation Validation** from **BEST_EFFORT** to **NONE** on the **Security** > **Configuration** > **Security Configuration** > **Revocation Configuration** page.

   When you click **Commit**, System Manager displays the following message:

   ```
   Changes are updated successfully. An Application server restart is
   required for changes to take effect. Click Ok to restart it now.
   Click Cancel to restart it later. Web Console would be unavailable
   for 10-15 minutes during a restart.
   ```

Configuring CRL download on the primary System Manager server

Procedure

1. Access the login page of the secondary System Manager server.
2. Copy the CRL of the browser certificate.

   For information about copying the CRL URL, see “Copying the CRL URL.”
3. Replace the vFQDN in the CRL with the IP address of the secondary System Manager server.

   For example, the CRL in the certificate is:

   ```
   http://<vFQDN>/ejbca/publicweb/webdist/certdist?
   cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
   ```

   The new CRL for the certificate will be:

   ```
   http://<ip-address>/ejbca/publicweb/webdist/certdist?
   cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
   ```

   Replace the *<vFQDN>* and *<ip-address>* tags with the respective vFQDN and IP address.

   Note:

   If you installed a third-party certificate on System Manager servers, this step is not required. If third-party certificate, then configure CRL URL of the third-party certificate for CRL download.
4. Log on to the primary System Manager web console.
5. On the System Manager web console, click **Services** > **Security**.
6. In the navigation pane, click **Configuration** > **CRL Download**.
7. On the CRL Download Configuration page, click **Add**.

   System Manager displays the Schedule CRL Download page.
8. In **Job Name**, type the job name.
9. In **Job Frequency**, set the frequency, and recurrence to schedule the job within a few minutes after the CRL addition.

   For more information, see Schedule CRL Download field descriptions.
10. In **Configure CRL Distribution Point**, type the new CRL.
11. Click **Add**, and then click **Commit**.

    Ensure that the job is completed successfully.

Next steps

Add the trusted certificate of the secondary System Manager server to the new primary System Manager server.

Adding the trusted certificate of secondary server to the primary System Manager server

Procedure

1. Log in to the secondary System Manager web console.
2. On the System Manager web console, click **Services** > **Security**.
3. In the navigation pane, click **Certificates** > **Authority**.
4. Click **CA Functions** > **CA Structure & CRLs**.
5. Click **Download PEM file**.
6. Log in to the primary System Manager web console.
7. On the System Manager web console, click **Services** > **Inventory**.
8. In the navigation pane, click **Manage Elements**.
9. On the Manage Elements page, select the System Manager certificate and click **More Actions** > **Manage Trusted Certificates**.
10. On the Manage Trusted Certificates page, click **Add**.
11. Click **Choose File** and select the previously downloaded PEM file from the secondary server.
12. Click **Retrieve Certificate**, and then click **Commit**.

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 105
Restoring the primary System Manager server on page 109
Deactivating the secondary System Manager server on page 109
Disabling the Geographic Redundancy replication on page 106
Activating the secondary System Manager server on page 108

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 information about how to change over to the cold standby server, see *Upgrading Avaya Aura® System Manager*.
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 105
Deactivating the secondary System Manager server on page 109
Disabling the Geographic Redundancy replication on page 106
Activating the secondary System Manager server on page 108
Recovering the primary System Manager server from disaster on page 124

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 105
Deactivating the secondary System Manager server on page 109
Disabling the Geographic Redundancy replication on page 106
Activating the secondary System Manager server on page 108
Recovering the primary System Manager server from disaster on page 124

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 105
Configuring Geographic Redundancy on page 103
Converting the primary System Manager server to the standalone server on page 114

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.

About this task

Important:

During the system recovery of Geographic Redundancy, the active secondary System Manager server copies the data from 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.

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 the Geographic Redundancy setup”.

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, do 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 Chrome, click **Not secure** on the address bar, and then click **Certificate** > **Details** > **Subject Alternative Name**. The first entry for **DNS Name** is the virtual FQDN.
     - On Edge, click **Not secure** on the address bar, and then click **Show certificate symbol** > **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. For Release 7.1 and later, perform the steps provided in the “Disaster recovery prerequisites” section.
7. Log in to the command line interface of the newly created primary System Manager with administrator privilege CLI user credentials, 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 Release 7.1 and later, type `sudo -u admin $MGMT_HOME/geo/bin/rundisasterrecovery.sh -FQDN <SECONDARY_FQDN> -IP <Secondary_Host_IPAddress> -ID admin -PASS <UIPassword>`

Release 6.3.x example: **`$MGMT_HOME/geo/bin/rundisasterrecovery.sh -FQDN psvdbf24.dr.sdr.com -IP 144.235.244.244 -ID systemadmin -PASS System$567`**.

Release 7.1.x example: `sudo -u admin $MGMT_HOME/geo/bin/rundisasterrecovery.sh -FQDN sit2.smgrdev.avaya.com -IP 2a07:2a42:adc0:1d::87 -ID admin -PASS System$675`

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`

8. 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.

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

    The system starts working in the normal operational mode.

Related links

Enabling the Geographic Redundancy replication on page 105
Restoring the primary System Manager server on page 109
Deactivating the secondary System Manager server on page 109
Activating the secondary System Manager server on page 108

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 System Manager Geographic Redundancy feature.

This document provides the procedures required when a primary System Manager is unavailable 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 92

Elements Geographic Redundancy manageability status matrix

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

Element	Version	Geographic Redundancy-enable status	Manage or Unmanage
Avaya Aura® Session Manager	6.3 and later	GR-aware (Auto)	Yes
	6.2 and earlier	GR-unaware	Yes
Communication Manager	6.2 and later	GR-aware (Manual)	Yes
CS 1000	7.5	GR-aware	No
Visualization, Performance and Fault Manager	3.0	GR-aware	-

Table continues…

Element	Version	Geographic Redundancy-enable status	Manage or Unmanage
Avaya Aura® Contact Center	6.3	GR-aware	-
Avaya Breeze® platform	3.0 and later	GR-aware (Auto)	Yes
For information about the Geographic Redundancy terminology, see the “Geographic Redundancy terminology” section. **Note:** The elements that are not listed in this table are GR-unaware.			

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 configuration

Session Manager Release 6.3 and later elements are GR-aware.

In the normal operation mode, all Session Manager Release 6.3 and later 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.

Session Manager 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 switches to an active System Manager that is reachable within the network.

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 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 129
Configuring Session Manager Release 6.2 and earlier during failback on page 129
Problems in managing Session Manager 6.1 or 6.2 using System Manager 6.2 on page 130

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 configuration on page 128

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, use this procedure to switch back the System Manager elements earlier than Release 6.3 to the primary System Manager server and resume normal operation.

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 configuration on page 128

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 configuration on page 128

Communication Manager configuration

Configuring Communication Manager during GR failover

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**.

   You cannot administer the Communication Manager elements that System Manager does not manage.

   The system displays the status of Communication Manager as Unmanaged.
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. **(Optional)** 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 failback if recovery was done using primary System Manager database, 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.
   - During failback if recovery was done using secondary System Manager database, 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**.

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

About this task

Communication Manager Release 6.2 and later have a feature to notify all the changes made outside System Manager, for example, using Communication Manager, System Administration Terminal 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.

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.

During failback, perform the same procedure 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 134
Configuring VxWorks-based CS 1000 servers on page 135
Configuring Linux-based CS 1000 servers on page 135
Limitations to the CS 1000 functionality support on System Manager on page 136

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 134
Alarming on page 1003
TrapListener service on page 1045

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 134

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 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 134

Limitations to the CS 1000 functionality support on System Manager

System Manager server state		CS 1000 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 • Corporate Directory • Registration of the new CS 1000 member • User Management of CS 1000 elements • Starting of Deployment Manager • Starting of Patch Manager	• Authentication (SSO) • Authorization (RBAC) • Starting of Remote Element Managers
Nonoperational	Standby	The primary server is non-operational. Therefore, no functionality is available from the primary server.	• Authentication (SSO) • Authorization (RBAC) • Starting of Remote Element Managers

Table continues…

System Manager server state		CS 1000 functionality support available	
Primary server	**Secondary server**	**From the primary server**	**From the secondary server**
Nonoperational	Active	The primary server is non-operational. 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 134

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 137
License management on page 137

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 137

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 137

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 138

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 the Presence Server element to change the Presence Server System Manager configuration from the primary System Manager to the 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, the 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 the 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 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 138

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.

Note:

Modular Messaging is not supported since December 2015.

Related links

Configuring Messaging in the normal operational mode on page 139
Configuring Messaging when the primary System Manager server is nonoperational on page 140
Configuring Messaging during GR failback on page 141
Configuring Messaging during split network on page 142

Configuring Messaging in the normal operational mode

Before you begin

- Add 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 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. Perform one of the following:
   - If **Must use SSL or encrypted SSL** is selected on the Messaging system, select the **Secured LDAP Connection** check box and set **Port 636** in LDAP Connection Security.
   - If **No encryption required** is selected on the Messaging system, clear the **Secured LDAP Connection** check box and set **Port 389** in LDAP Connection Security.
8. In **Messaging Type**, select one of the following Messaging server types:
   - **AURAMESSAGING**
   - **CMM**
   - **MM**
9. In **Version**, select the Messaging version.

10. Click **Services** > **Inventory** > **Synchronization** > **Messaging System**.
11. Select the required Messaging element, and click **Now**.
12. Perform one of the following:
    - If synchronization is successful, perform the administration task on Messaging.
    - If synchronization fails, check the login details for Messaging.

      To find more information about the cause of the failure, click **Scheduler** > **Completed Jobs**. Select the corresponding Messaging synchronization job, and click **More Actions** > **View Log**.
13. Log on to the secondary System Manager server.
14. On the System Manager web console, click **Services** > **Inventory**.
15. In the navigation pane, click **Manage Elements**.
16. Ensure that the Messaging system added is visible on the Manage Elements page.

Related links

Messaging configuration on page 139

Configuring Messaging when the primary System Manager server is nonoperational

About this task

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

Before you begin

- Add 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 navigation pane, click **Manage Elements**.
6. Select the Messaging system 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 ready to administer and manage Messaging.

Related links

Messaging configuration on page 139

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, skip to 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 server.
   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 ready to administer and manage Messaging.

Related links

Messaging configuration on page 139

Configuring Messaging during split network

About this task

Do not activate primary and secondary System Manager servers except during scenarios where 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 standby mode.

Procedure

1. Log on to the primary and the secondary 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 added as the trusted server, update the login and password details of Messaging for both the 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 synchronization is successful on both System Manager servers, perform the administrative task for Messaging on both System Manager servers.
   - If synchronization fails, check the login details for Messaging.

     To find more information about the cause of the failure, click **Scheduler** > **Completed Jobs**. Select the corresponding Messaging synchronization job, and click **More Actions** > **View Log**.

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

   Note:

   During a split network scenario, you must administer the Messaging system from the primary or the secondary System Manager server. If you simultaneously administer from both System Manager servers, you must run the Messaging System Synchronization job to fetch the changes done from the peer System Manager server on Messaging. Failure to run the job results in the Messaging data on System Manager being inconsistent with the actual data on the Messaging system provisioned from another System Manager.

Related links

Messaging configuration on page 139

Avaya Meetings Server configuration

The Avaya Meetings Server element is GR-unaware. During a failover or split network, you must manually configure SSO on the Avaya Meetings Management console.

Note:

If secondary System Manager is using the same IP or FQDN of the primary System Manager, then you do not need to configure SSO for Avaya Meetings Server.

Configuring SSO for Equinox Conferencing

Exchanging CA certificates between System Manager and Avaya Meetings Management

About this task

If the Avaya Meetings Management CA certificate is not issued by the System Manager CA, perform the following.

Procedure

1. Download the CA PEM file from System Manager.

   For more information, see “Downloading the System Manager PEM certificate”.

   Note:

   If System Manager has more than one CA, import all the CAs into Avaya Meetings Management.
2. Log in to the Avaya Meetings Management administrator portal.
3. To import the CA PEM file into Avaya Meetings Management, click **Settings** > **Security** > **Certificate**.
4. Click **Import**.
5. On the Import certificates dialog box, click **Add** to select the downloaded PEM file, and click **Apply**.
6. Restart Avaya Meetings Management.
7. To download the Avaya Meetings Management CA certificate, click **Settings** > **Security** > **Certificate**.
8. On the Certificates page, click **Conferencing Management Certificate**.
9. On the System Manager web console, click **Services** > **Inventory**.
10. In the navigation pane, click **Manage Elements**.
11. On the Manage Elements page, select the System Manager certificate and click **More Actions** > **Manage Trusted Certificates**.
12. On the Manage Trusted Certificates page, click **Add**.
13. On the Add Trusted Certificates page, click **Import as PEM certificate**.

14. Copy the content of the Avaya Meetings Management CA certificate and paste the content in the text box provided on the Add Trusted Certificates page.
15. Click **Commit**.

Related links

Avaya Meetings Server configuration on page 143
Downloading the System Manager PEM certificate on page 144
Configuring SSO in Avaya Meetings Management on page 144

Downloading the System Manager PEM certificate

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **CA Structure & CRLs**.
4. Click **Download PEM file**.

   The system downloads the `.pem` file on your system.

Related links

Exchanging CA certificates between System Manager and Avaya Meetings Management on page 143

Configuring SSO in Avaya Meetings Management

Before you begin

If the Avaya Meetings Management CA certificate is not issued by the System Manager CA, exchange CA certificates between Avaya Meetings Management and System Manager.

- Download the CA certificate from System Manager and import the certificate into the Avaya Meetings Management console.
- Download the certificate from the Avaya Meetings Management console and add the certificate in to System Manager as a new trusted certificate.

For more information, see “Exchanging CA certificates between System Manager and Avaya Equinox Management”.

Procedure

1. Navigate to `/opt/Avaya/iview/tomcat/webapps/iview/WEB-INF/classes/sso_config/securityServerConfig.properties`, and edit the properties of the file as follows.

```
openssoclient.config.folder=../config
com.iplanet.am.cookie.name=<FQDN of your System Manager?
security.server.fqdn=<FQDN of your System Manager>
```

2. Navigate to `/opt/Avaya/iview/tomcat/config/vcs-core.properties` and add the `vnex.auth.smgr.sso=true` property.

3. Before restarting Tomcat, navigate to `/opt/Avaya/iview/tomcat/config/` and delete the `OpenSSOClient` folder.
4. To restart Tomcat, do one of the following:
   - On the shell, run the **`service avaya.iview restart`** command.
   - On the Avaya Meetings Management console, click **Restart**.

Related links

Avaya Meetings Server configuration on page 143
Exchanging CA certificates between System Manager and Avaya Meetings Management on page 143

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 *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.
- If IP Office has been added to any System Manager previously, then before reusing it, you must erase the IP Office security settings using the **File** > **Advanced** > **Erase Security Settings** page on the IP Office Manager window.

Related links

Configuring IP Office in normal operational mode with SCEP enabled on page 145
Configuring IP Office in normal operational mode with SCEP disabled on page 146
IP Office configuration when the primary System Manager is nonfunctional on page 147
IP Office configuration in the Active-Active scenario on page 147
Alarms on page 147
User management on page 148

Configuring IP Office in normal operational mode with SCEP enabled

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **RA Functions** > **Add End Entity** and add IP Office as an entity and specify all required details.

4. 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**.
5. Log on to the web console of the primary System Manager server.
6. On the System Manager web console, click **Services** > **Inventory**.
7. In the navigation pane, click **Manage Elements**.
8. Click **New**.
9. On the Add IP Office page, provide the name, the IP address, and the valid user name and password for IP Office.
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. Log on to the web console of the secondary System Manager and click **Services** > **Inventory**.
12. 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 145

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 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 145

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 145

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 *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager*.

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 145

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 145

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 145

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.

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 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, click **View** and 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 160

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 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 159

Modifying groups

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.

2. In the 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 162

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 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 164

Deleting groups

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the 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 163

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 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 164

Synchronizing resources for a resource type

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the 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 165

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 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 168

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 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 168

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 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 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

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
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.

Table continues…

Button	Description
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.
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 top-right corner of the page.

Name	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**.

Table continues…

Button	Description
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.
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.

Table continues…

Field	Description
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:

Name	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. • **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.

Table continues…

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 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

Name	Description
Select	The option to select a group.
Name	The groups under which you can create a copy of 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	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.

Table continues…

Button	Description
Selected Group	Moves the selected group to the group that you selected in the **Name** column.
Cancel	Closes the Move Group page and returns to the Group Management page.

Resource Synchronization field descriptions

Name	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 navigation pane, click **Resources**.

Related links

Resources field descriptions on page 168

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 navigation pane, click **Resources**.
3. On the Resources page, select a resource from the list or click **Advanced Search** to search for a resource.
4. Click **Add To New Group**.
5. To add a resource to a new group at root level, do the following:
   a. On the Choose Parent Group page, click **Root**.
   b. On the Create Group page, enter the appropriate information.
   c. Click **Commit**.
6. To add a resource to a new subgroup within a group, do the following:
   a. On the Choose Parent Group page, click a group.

      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.

      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.
   d. Click **Commit**.

Related links

Resources field descriptions on page 168
New Group field descriptions on page 159

Adding resources to a selected group

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the 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 168

Searching for resources

Procedure

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

Name	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.

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

Name	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.

Table continues…

Name	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
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

Name	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 Microsoft Active Directory or other supported directory server administrator roles with System Manager administrator roles. The capability includes system roles and custom roles on System Manager.

Note:

Granular RBAC is not supported for managing Avaya Meetings Server, Web Gateway, and Work Assignment elements by creating custom roles.

Related links

Custom roles on page 176
Built-in roles on page 171

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.

Table continues…

Role	Privileges
System Administrator	Gives the super-user privilege. System Administrator is the single all powerful role. With 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 **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 E-token.
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 E-token. 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.

Table continues…

Role	Privileges
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.
End-User	The administrator assigns this role to the telephony users. **Important:** You cannot log in to System Manager with the End-User role.
Avaya Breeze Admin	Gives read-write access to the Avaya Breeze® platform configuration.
Avaya Breeze Auditor	Gives read-only access to Avaya Breeze® platform logs, configuration information, and audit files. With the Auditor role, you cannot run any command that might provide access to another host.
Avaya Breeze Server Admin	Gives read and write access to all Avaya Breeze® platform management functionality.
Avaya Breeze Service Profile Admin	Gives write access only for Service Profiles.
Avaya Breeze Services Admin	Gives write access only for Service Management.
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.

Table continues…

Role	Privileges
Presence Auditor	Gives read-only access to logs, configuration information, and audit files. With 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.

Table continues…

Role	Privileges
CS1000_Admin2	Provides unrestricted OAM access including security and account administration, and provisioning for all customers on all call server 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

Table continues…

Role	Privileges
Patcher	Gives access to software maintenance functions, such as update and maintenance. You can access the following elements: • All elements of type: Linux Base • 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.

Custom roles

On the Roles page, 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.

Note:

- When a user who is associated with custom role administers various operations on Communication Manager, which is managed by System Manager, then custom role requires permissions for Scheduler and Communication Manager templates along with required Communication Manager admin permissions. Therefore, custom role must have minimum permissions:
  - For on demand job create/view permissions in Scheduler.
  - To view Communication Manager templates.
- If Communication Manager IP address is changed on the **Inventory** > **Manage Elements** page, custom users that have roles for that particular Communication Manager cannot access those Communication Managers.

  For example, the Communication Manager IP Address can be changed on the Manage Elements page for the following reasons:
  - Duplex Communication Manager gets interchanged
  - Communication Manager IP Address has been updated manually

  If Communication Manager IP Address is changed on the Manage Elements page, you must also update the corresponding Communication Manager role mappings.

Viewing user roles

Procedure

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

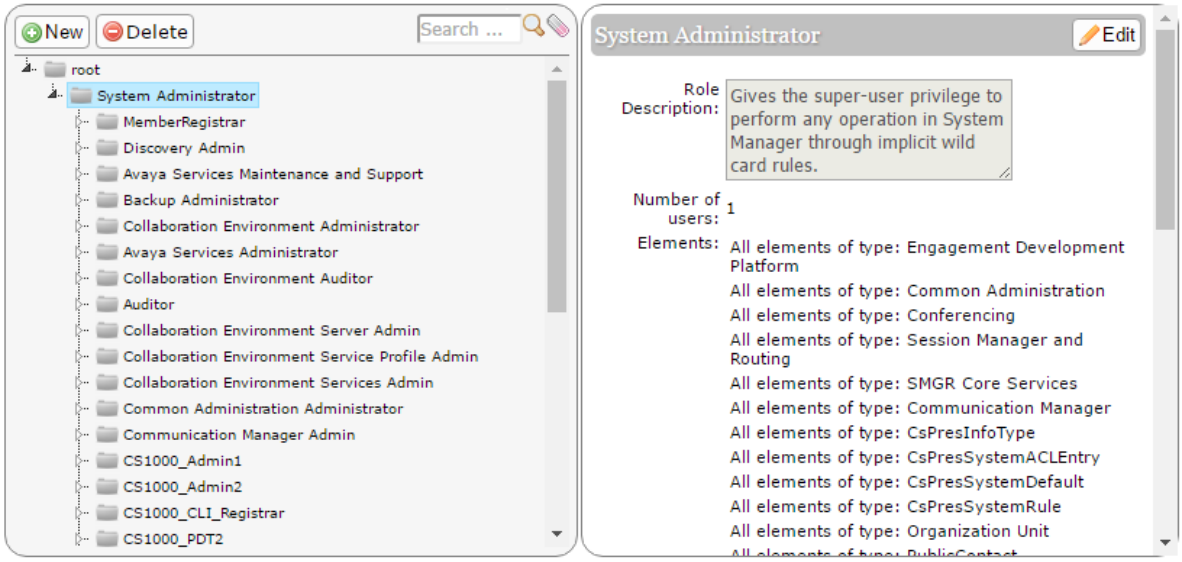
Roles field descriptions on page 184

Adding a custom role

Procedure

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



   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 182
Creating groups on page 151
Assigning resources to a group on page 154
Add Mapping field descriptions on page 186
Add New Role field descriptions on page 185
Mapping permissions by using the template on page 181

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 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 1294

Assigning permissions to access Solution Deployment Manager

About this task

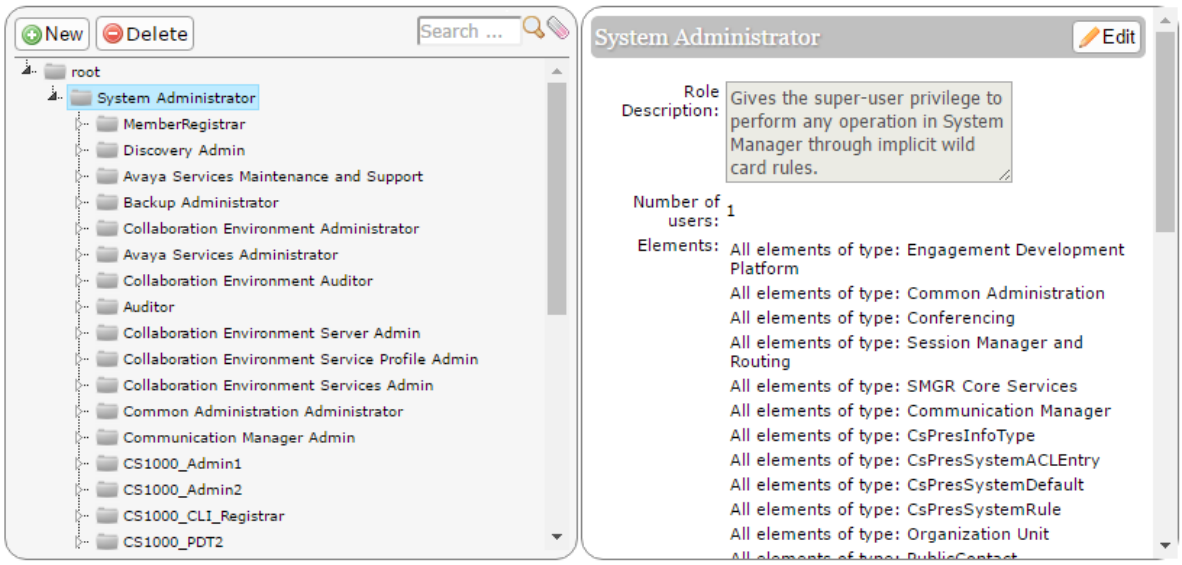
System Manager provides access permissions to Solution Deployment Manager through Role Based Access Control (RBAC) for elements, such as Communication Manager, Session Manager, Branch Session Manager, and IP Office. System Manager defines flexible access privileges for deployment, migration, upgrade, 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 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. 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, select **Solution Deployment Manager**.
9. In the **Element or Resource Instance** field, select **All**.
10. Click **Next**.
11. In Upgrade Management and VM Management, select appropriate permissions, and click **Commit**.

    The user can now access the Solution Deployment Manager links.

    To assign user permissions, select **Users** in **Element or Resource Type**. Select appropriate permissions, and click **Commit**.

Mapping permissions by using the template

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the 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 187

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 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 238
Assigned Users field descriptions on page 186

Unassigning users from role

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the 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 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 187

Editing a custom role

Procedure

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

   Note:

   When a user edits any role assigned to their account and commits the changes in System Manager, the user is logged out immediately and redirected to the login page of System Manager web console.

   For example, if the user `user@domain.com` is logged into System Manager web console and edits one of the roles assigned to their account, the user is logged out of System Manager immediately and redirected to the login page of System Manager web console.

   Note:

   When a user edits a role in System Manager, all other users assigned to that role are logged out after their next action and redirected to the login page of System Manager web console.

   For example, User 1 is assigned the `System Admin role`, while User 2 and User 3 are assigned the `Test role`. If User 1 edits the `Test role`, User 2 and User 3 are

logged out after their next action and redirected to the login page of System Manager web console.

Related links

Mapping permissions by using the template on page 181

Deleting custom roles

Procedure

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

Name	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

Name	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 returns to the Roles page.

Related links

Copying permission mapping for a role on page 182
Creating groups on page 151
Assigning resources to a group on page 154

Role Details field descriptions

Name	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.

Table continues…

Button	Description
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

Name	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 182
Creating groups on page 151
Assigning resources to a group on page 154

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.

Name	Description
User Name	The name of the user that you assign to the role.

Table continues…

Name	Description
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 **Add Mapping** on the Role Details page.

Name	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.

The page displays the following fields when you click **Copy All From** on the Role Details page.

Name	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.

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

Table continues…

Name	Supported range
Coverage Time of Day	1–1000
Off PBX Endpoint Mapping	Off PBX Endpoint Mapping 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

Table continues…

Steps	Action	Implicit permissions that are required
• 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
• 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

Table continues…

Steps	Action	Implicit permissions that are required
	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** > **Switch to Classic View** > **New** page, the system prompts you to enter a qualifier. You can enter the hunt group number, or type `Next`, and click **Add** to add the next available group number.

- 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.

Assigning permissions in User Management

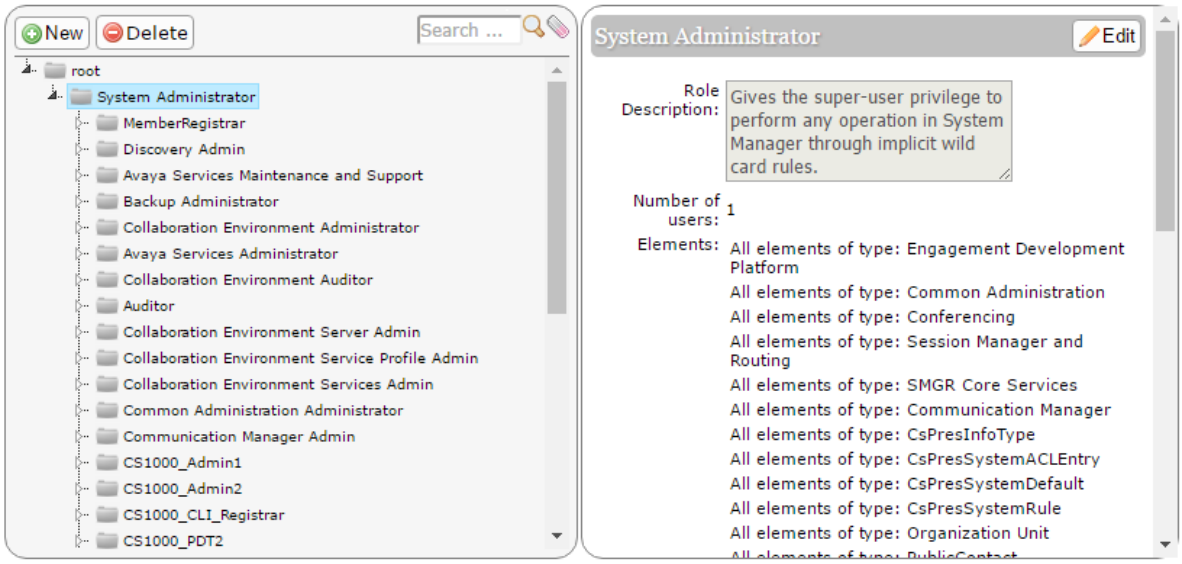
The range feature in endpoints and agents is also applicable in **User Management**. When you assign a range for endpoints and agents, as per the permissions that are defined, you can add, edit, delete, and duplicate only the extensions that are associated with the user. Range is validated when you assign an endpoint extension or an agent extension through the endpoint or agent editor.

Assigning permissions through User Management

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and perform one of the following:
   - 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. 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 **All**.
10. Click **Next**.
11. On the Permission Mapping page, select the **Role Resource Type Action** and **Role Resource Type Attributes**. Enable **Administrative Users**, if required.
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** and **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 • 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

Table continues…

Communication Manager object	Field
	• 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 • 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

Table continues…

Communication Manager object	Field
	• 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 • 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)

Table continues…

Communication Manager object	Field
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.

Endpoints

Range in endpoints

You can assign a range of values in endpoints and add permissions for specific fields in an endpoint. Specify a definite range, comma separated values, or a single value in the endpoints range field.

For example, you can type 5600:6000 to assign permissions for extensions 5000 to 6000. When you use colon (:) 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.

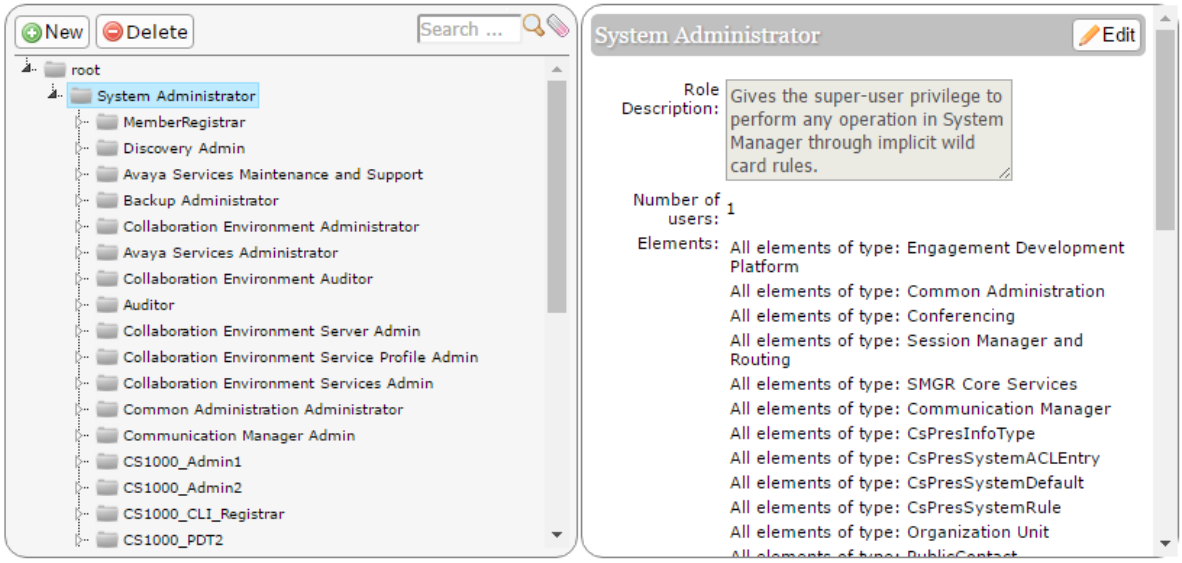
- If you assign a specific endpoint range to a user, you can view, add, delete, edit and duplicate only those endpoints within the specified range.
- You can also assign a specific range to the **COR** and **Coverage Path** fields in endpoints.
- You can manage only those endpoint extensions within the 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

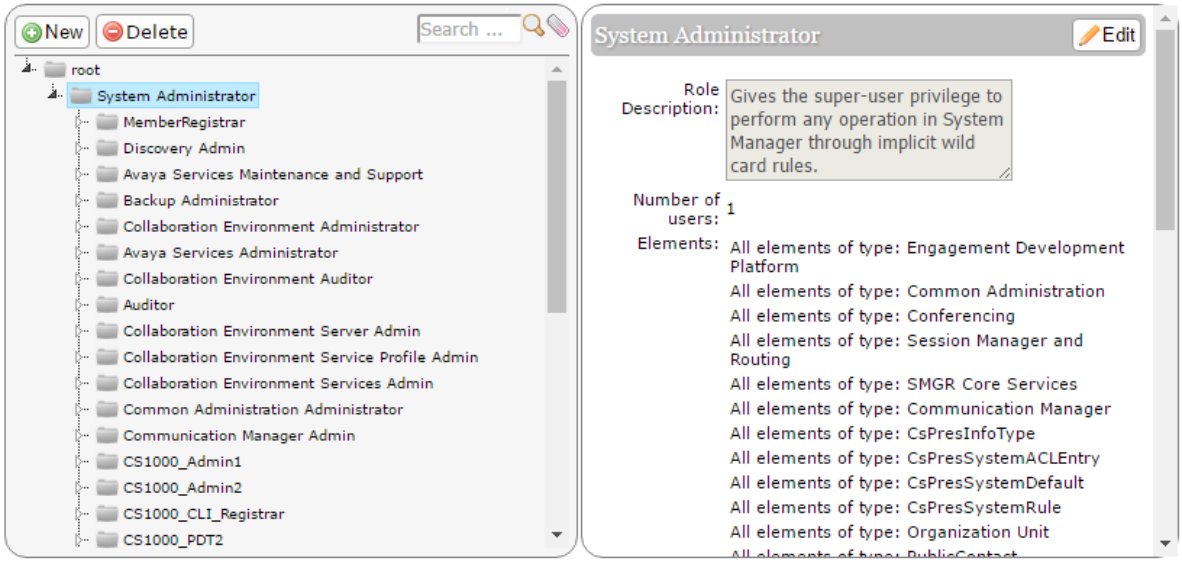
1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and do one of the following:
   - Click **New**
   - Right-click and select **New**

   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. Click **Add Mapping** under **Element/Service Permissions** section.
7. In the **Element or Resource Type** field, click **Communication Manager**.
8. On the Roles page, select an existing role, and do one of the following:
   - 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.



9. On the Add New Role page, type the name and the description for the role.
10. Click **Commit and Continue**.
11. On the Role Details page, in the **Element/Service Permissions** section, click **Add Mapping**.
12. In the **Element or Resource Type** field, click **Communication Manager**.
13. 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.
14. In the **Element or Resource Type** field, click **Communication Manager**.
15. In the **Element or Resource Instance** field, click a Communication Manager instance to which you want to apply this permission.

    When you select **Group Name**, System Manager disables this field.
16. Click **Next**.
17. On the Permission Mapping page, expand the **Endpoints** permission list by clicking on the arrow next to it. 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.
18. 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.
19. Click **Commit**.

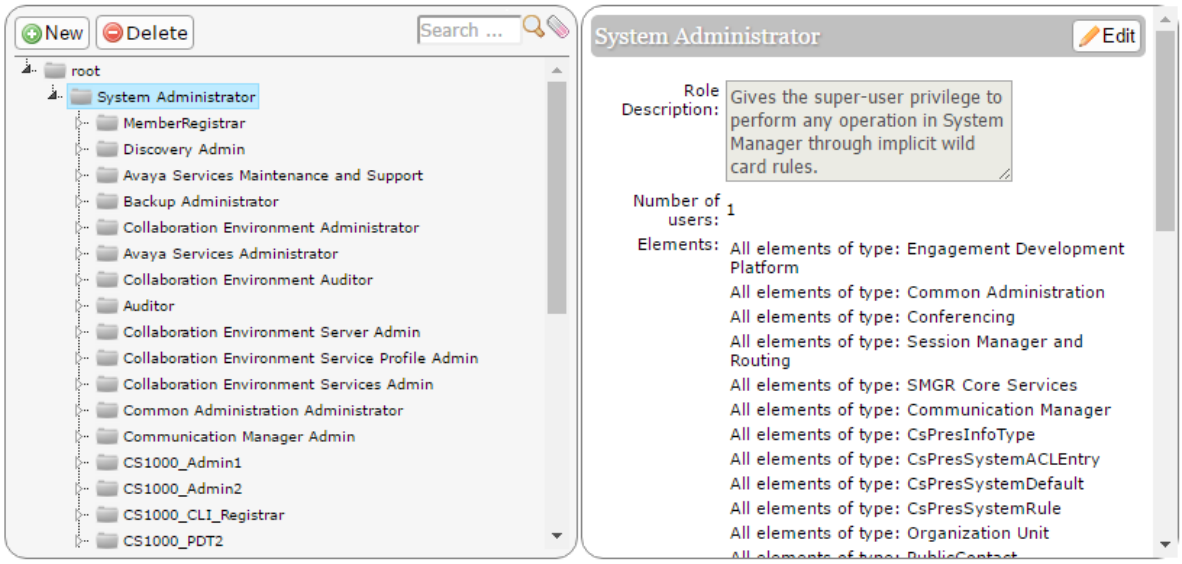
Assigning permissions for fields in endpoints

Field-level RBAC for Communication Manager objects is applicable only for the edit operation.

Procedure

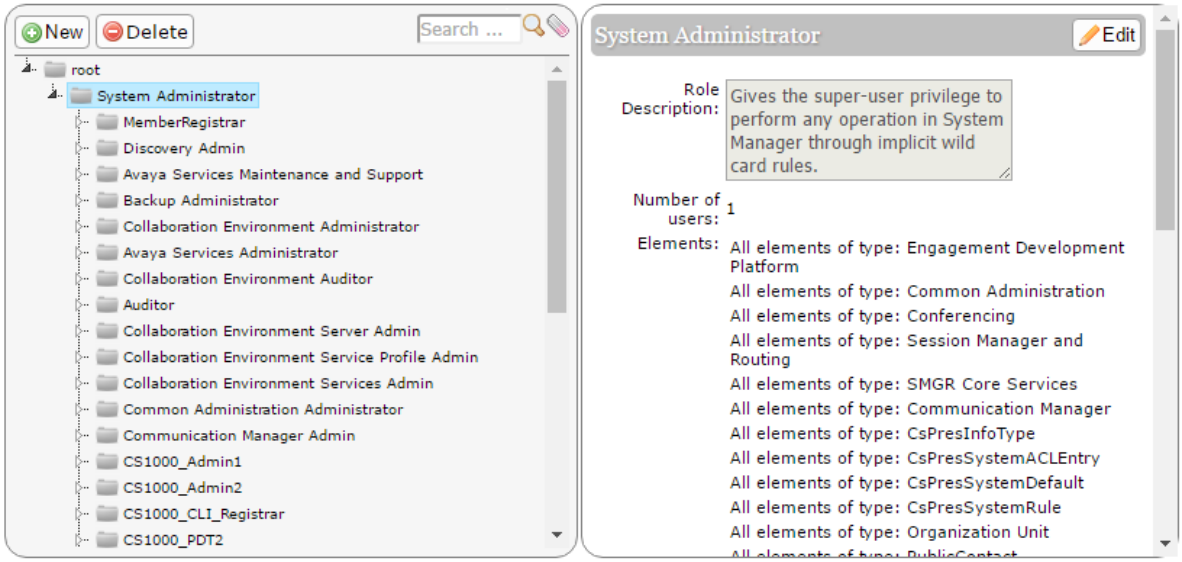
1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and do one of the following:
   - Click **New**
   - Right-click and select **New**

   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. Click **Add Mapping** under **Element/Service Permissions** section.
7. In the **Element or Resource Type** field, click **Communication Manager**.
8. On the Roles page, select an existing role, and do one of the following:
   - 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.



9. On the Add New Role page, type the name and the description for the role.
10. Click **Commit and Continue**.
11. On the Role Details page, in the **Element/Service Permissions** section, click **Add Mapping**.
12. In the **Element or Resource Type** field, click **Communication Manager**.
13. 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.
14. In the **Element or Resource Type** field, click **Communication Manager**.
15. In the **Element or Resource Instance** field, click a Communication Manager instance to which you want to apply this permission.

    When you select **Group Name**, System Manager disables this field.
16. Click **Next**.
17. On the Permission Mapping page, expand **Endpoint Attributes Permission for Edit Operation** and **Endpoint Buttons Permission for Edit Operation** by clicking on the arrow next to it. Select the buttons and attributes that you want to assign to this role.
18. 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.

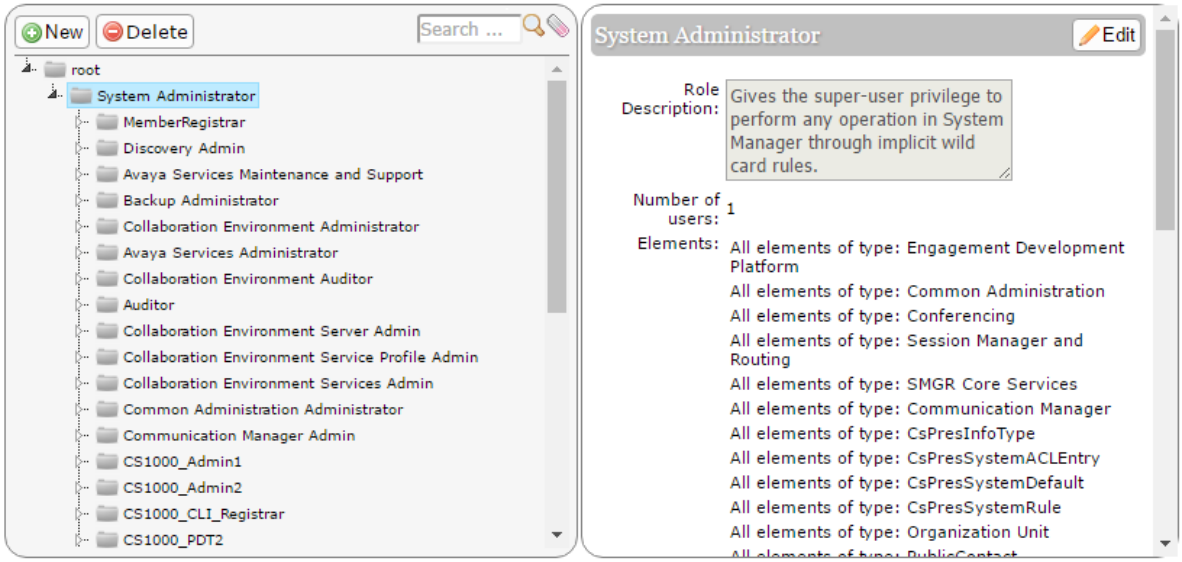
Hunt Group

Assigning range for hunt group

Procedure

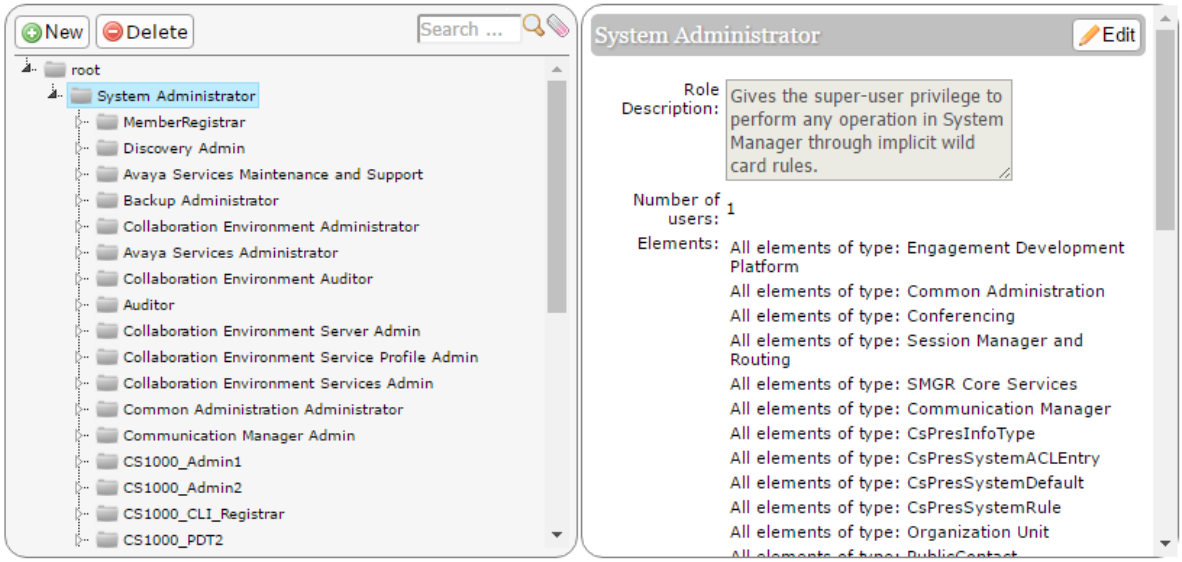
1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and do one of the following:
   - Click **New**
   - Right-click and select **New**

   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. Click **Add Mapping** under **Element/Service Permissions** section.
7. In the **Element or Resource Type** field, click **Communication Manager**.
8. On the Roles page, select an existing role, and do one of the following:
   - 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.



9. On the Add New Role page, type the name and the description for the role.
10. Click **Commit and Continue**.
11. On the Role Details page, in the **Element/Service Permissions** section, click **Add Mapping**.
12. In the **Element or Resource Type** field, click **Communication Manager**.
13. 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.
14. In the **Element or Resource Type** field, click **Communication Manager**.
15. In the **Element or Resource Instance** field, click a Communication Manager instance to which you want to apply this permission.

    When you select **Group Name**, System Manager disables this field.
16. Click **Next**.
17. On the Permission Mapping page, expand the **Hunt Group** permission list by clicking on the arrow next to it. Enter the range you want to specify in the **Group Number Range** and **Group Extension Range** fields.

    You can specify a definite range, enter comma separated values, or * for all extensions.
18. You can also assign operation permissions like **Add**, **Edit**, **Delete**, **List Usage**, and **View**.

    The user can perform only the actions that are assigned in the operation permissions.
19. Click **Commit**.

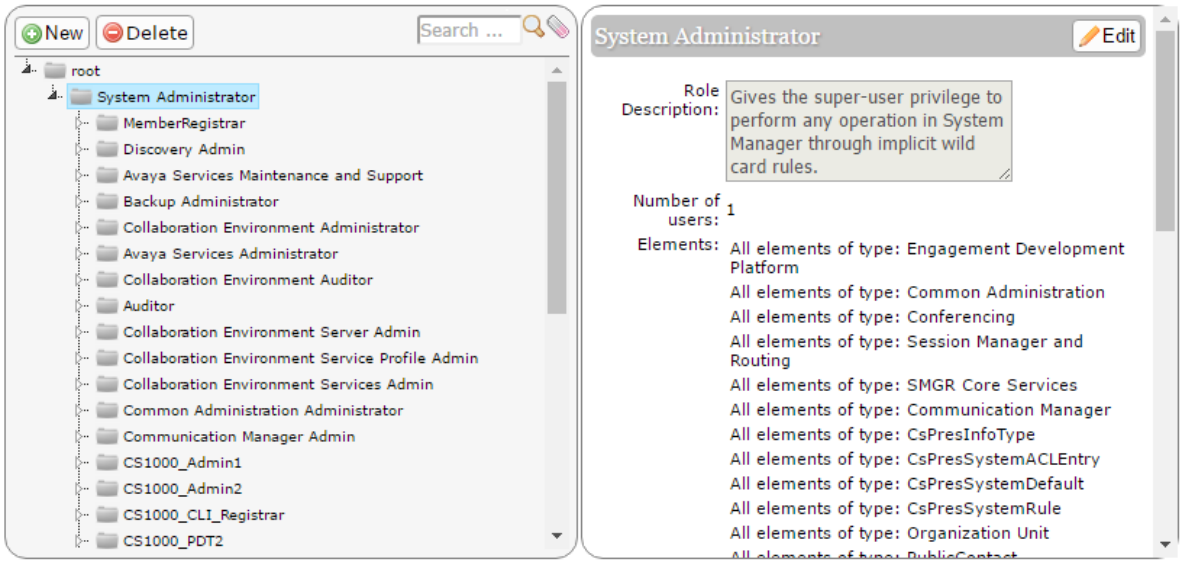
Assigning permissions for fields in hunt group

Field-level RBAC for Communication Manager objects is applicable only for the edit operation.

Procedure

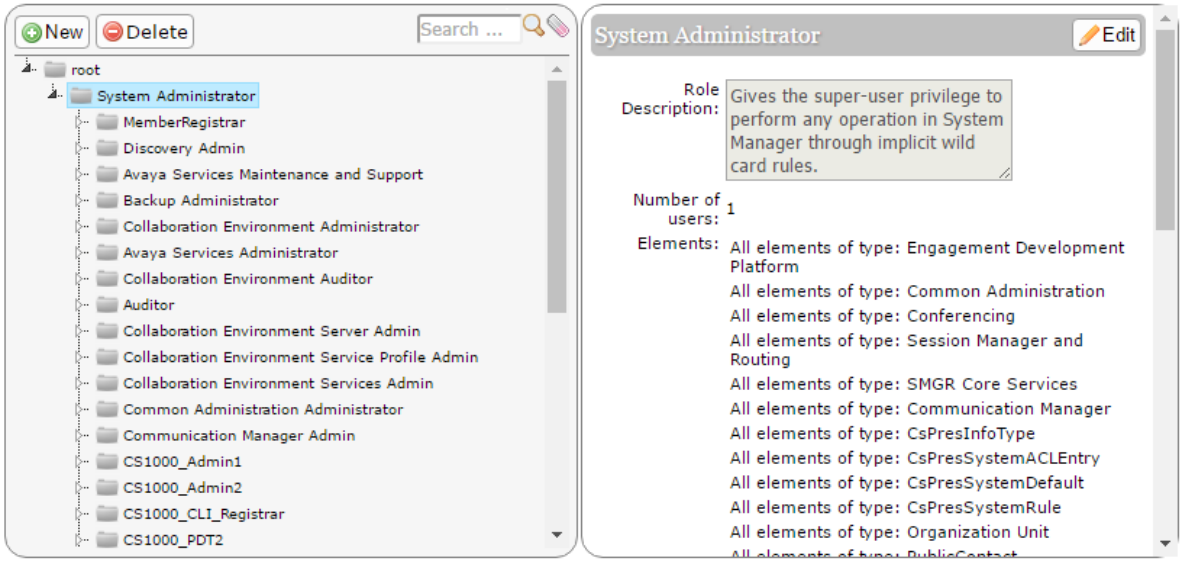
1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and do one of the following:
   - Click **New**
   - Right-click and select **New**

   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. Click **Add Mapping** under **Element/Service Permissions** section.
7. In the **Element or Resource Type** field, click **Communication Manager**.
8. On the Roles page, select an existing role, and do one of the following:
   - 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.



9. On the Add New Role page, type the name and the description for the role.
10. Click **Commit and Continue**.
11. On the Role Details page, in the **Element/Service Permissions** section, click **Add Mapping**.
12. In the **Element or Resource Type** field, click **Communication Manager**.
13. 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.
14. In the **Element or Resource Type** field, click **Communication Manager**.
15. In the **Element or Resource Instance** field, click a Communication Manager instance to which you want to apply this permission.

    When you select **Group Name**, System Manager disables this field.
16. Click **Next**.
17. On the Permission Mapping page, expand the **Hunt Group Attributes Permission for Edit Operation** list by clicking on the arrow next to it. Select the attributes that you want to assign to this role.
18. 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.

Trunk Group

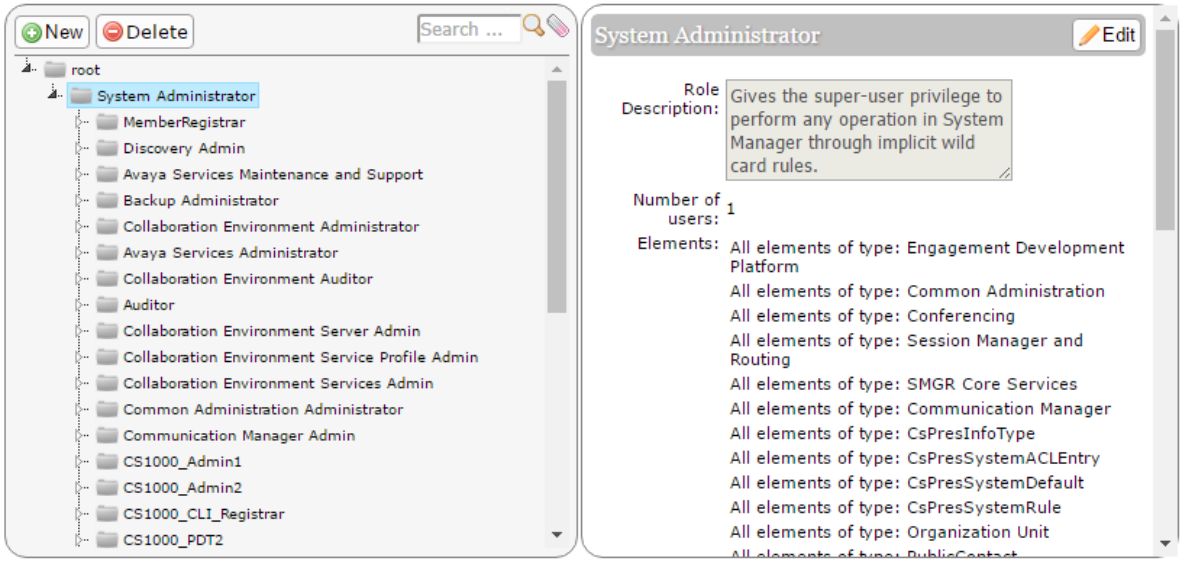
Assigning permissions for fields in trunk group

Field-level RBAC for Communication Manager objects is applicable only for the edit operation.

Procedure

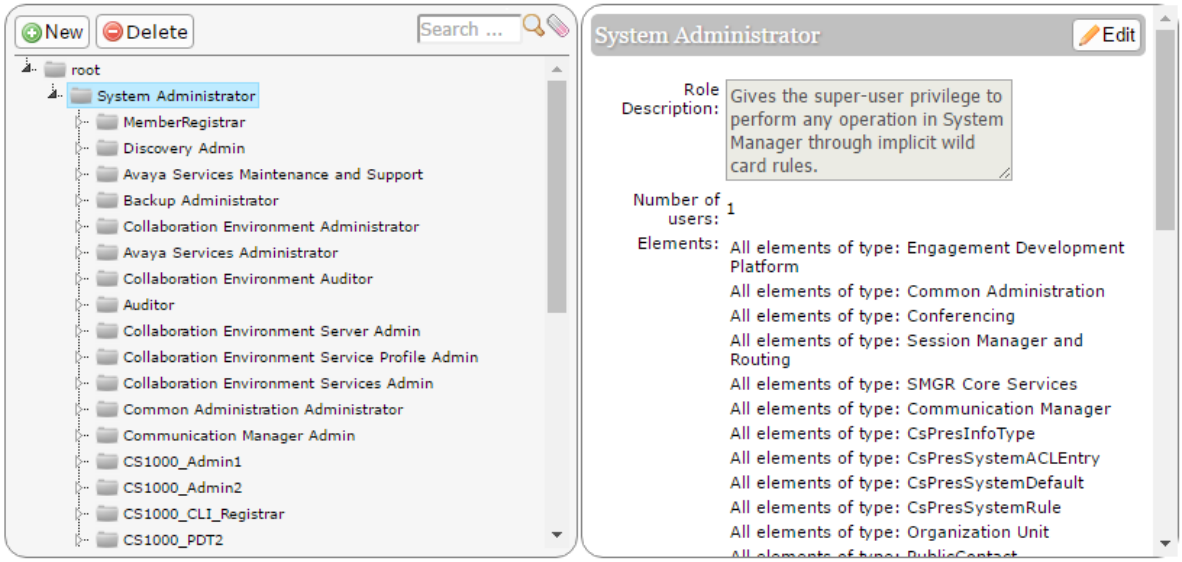
1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and do one of the following:
   - Click **New**
   - Right-click and select **New**

   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. Click **Add Mapping** under **Element/Service Permissions** section.
7. In the **Element or Resource Type** field, click **Communication Manager**.
8. On the Roles page, select an existing role, and do one of the following:
   - 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.



9. On the Add New Role page, type the name and the description for the role.
10. Click **Commit and Continue**.
11. On the Role Details page, in the **Element/Service Permissions** section, click **Add Mapping**.
12. In the **Element or Resource Type** field, click **Communication Manager**.
13. 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.
14. In the **Element or Resource Type** field, click **Communication Manager**.
15. In the **Element or Resource Instance** field, click a Communication Manager instance to which you want to apply this permission.

    When you select **Group Name**, System Manager disables this field.
16. Click **Next**.
17. On the Permission Mapping page, expand the **Trunk Group** permission list by clicking on the arrow next to it. Select the attributes that you want to assign to this role.
18. 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

By using User Management, you can create telephony user and System Manager administrative users.

- **Administrative users:** User who can log in to System Manager, these users must have a role assigned other than the end user role. Based on the role, you can perform the operations on System Manager.
- **Telephony users:** A telephony user in System Manager is defined as a user that has a subscription to one or more Avaya telephony subsystems. A subscription of a user to a Avaya subsystem is represented using Communication Profile of the user.

  A communication profile is used to represent a users subscription to a product specific communication subsystem and contains its specific configuration needs for the user. A communication subsystem is a service or infrastructure that manages the establishment, control, or routing of communication interactions. These can be provided by Avaya products, such as Session Manager and Communication Manager.

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.
- 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
SMGR core services	clone, view, edit, add, and delete

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 the administrator provides, end users can access the Self Provisioning web interface to change or reset 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.

By default, **Self Provisioning Status** is set to **true** so that the end user can change the communication profile password.

There are 2 limits for the Self Provisioning web interface:

- The maximum number of login sessions for the Self Provisioning web interface is 300, 500, and 1000 for System Manager Profiles 2, 3, and 4 respectively.
- The maximum number of concurrent HTTP requests for the Self Provisioning web interface is 75, 125, and 250 for System Manager Profiles 2, 3, and 4 respectively.

For example, if you run System Manager Profile 2, 300 users can login to the Self Provisioning web interface. Once logged in, only 75 users can simultaneously make a change.

Note:

The login sessions and HTTP requests for the Self Provisioning web interface are independent of the main System Manager web interface.

The session time-out is 10 minutes.

Related links

Disabling self provisioning on page 211
Generating the communication profile password from the self provisioning interface on page 211
Changing the communication profile password from the self provisioning interface on page 212

Enabling self provisioning

About this task

Administrator must disable 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 navigation pane, click **Settings** > **SMGR**.
3. On the Edit Profile:SMGR page, set **Self Provisioning Status** to **true**.

4. Click **Commit**.

Disabling self provisioning

About this task

Administrator must disable self provisioning on System Manager so that the end user cannot change the communication profile password.

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the navigation pane, click **Settings** > **SMGR**.
3. On the Edit Profile:SMGR page, set **Self Provisioning Status** to **false**.

   If you set the status to false, the system displays the following message: `The provisioning application is currently disabled. Please contact your system administrator.`

Related links

Generating the communication profile password from the self provisioning interface on page 211
Changing the communication profile password from the self provisioning interface on page 212

Generating the communication profile password from the self provisioning interface

About this task

Use this procedure to reset only the Communication Profile password.

Before you begin

The System Manager administrator must do the following:

- Enable Self Provisioning. For more information, see “Enabling self provisioning”.
- Configure email properties. For more information, see “Configuring email properties”.
- Add the user’s email address in the user profile. For more information, see “User Profile Edit field descriptions”.

Procedure

1. To gain access to the Self Provisioning web interface, on the web browser, type `https://<IP address of System Manager>/selfprovisioning/`.
2. On the Login page, type the user’s Avaya SIP handle and click **Reset Password**.

   Note:

   Avaya SIP handle is in the following format: `handle@domain`.
3. Access the inbox of the email address associated with the provided Avaya SIP handle.

4. In the **Avaya Aura System Manager Password Reset** email, click on the password activation link.

   The system sends a new email with a system generated password.

Next steps

Change the system generated communication profile password. For more information, see “Changing the communication profile password from the self provisioning interface”.

Related links

Disabling self provisioning on page 211
Changing the communication profile password from the self provisioning interface on page 212

Changing the communication profile password from the self provisioning interface

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 message `The Provisioning Application has reached maximum supported load. Please try again after some time.`

Before you begin

The System Manager administrator must Enable Self Provisioning. For more information, see “Enabling self provisioning”.

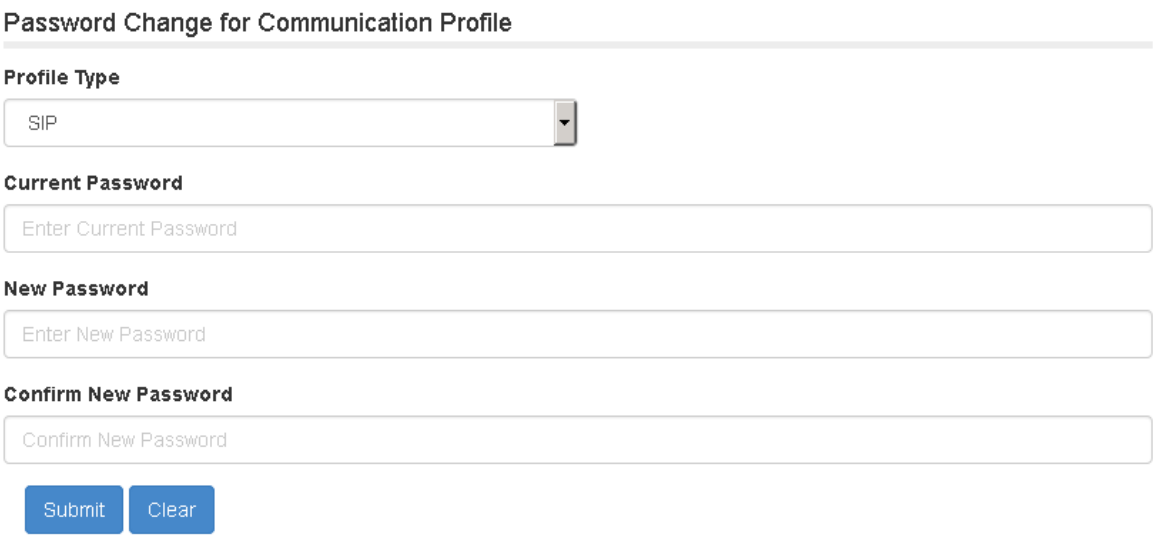
Procedure

1. To gain access to the Self Provisioning web interface, on the web browser, type `https://<IP address of System Manager>/selfprovisioning/`.
2. On the Login page, type the user ID and password and click **Login**.

   Note:

   - Use the communication address as username 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 one of the following:
   - **SIP**
   - **H.323**
   - **Agent**

- **Messaging**



4. Type the current password and the new password, and do one of the following:
   - To clear the values, click **Clear**.
   - To change the password, click **Submit**.

Related links

Disabling self provisioning on page 211
Generating the communication profile password from the self provisioning interface on page 211

Viewing details of a user

Before you begin

You require appropriate permissions.

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, select a user.
3. 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 | <User Name> field descriptions on page 328

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** > **Manage Users**.
2. On the Manage Users page, click **New**.
3. On the User Profile | Add 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)** On the **Identity** tab, in the Basic Info section, 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.
4. 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 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.

Related links

Creating a new user profile using the user provisioning rule on page 214
User Profile | Add field descriptions on page 285

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** > **Manage Users**.
2. On the Manage Users page, click **New**.
3. On the User Profile | Add page, complete the following fields:
   - **User Provisioning Rule**

     You can provide only one user provisioning rule.
   - **Last Name**
   - **First Name**
   - **Login Name**
4. 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 213
User Profile | Add field descriptions on page 285
Results of using the user provisioning rule on page 215

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.

Table continues…

Provisioning method	Scenario	Expected result
	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 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.

Table continues…

Provisioning method	Scenario	Expected result
	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. In bulk import, the user provisioning rule is not mentioned in the XML file.	The system disassociates the user provisioning rule with the user. The communication profiles in the Merge and Replace option with the Complete and Partial Import type remain unchanged.

Table continues…

Provisioning method	Scenario	Expected result
	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.

Table continues…

Provisioning method	Scenario	Expected result
	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. 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** > **Manage Users**.
2. On the Manage Users page, select a user.

   Note:

   At one time, you can edit only one user account.
3. To edit a user account, click one of the following:
   - **Edit**.
   - **View** > **Edit**.
4. On the User Profile | Edit | <User Name> page, do 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)** On the **Identity** tab, in the Basic Info section, 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 | <User Name> 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.

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**.

Note:

When a user edits and commits the changes to their own account in System Manager, the user is logged out immediately and redirected to the login page of System Manager web console.

For example, if a user `user@domain.com` logs in to System Manager web console, edits and commits changes to their user account, the user is logged out immediately and redirected to the login page of System Manager web console.

Related links

User Profile | Edit | <User Name> field descriptions on page 307
Results of using the user provisioning rule on page 215

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. You must add the CS 1000 Endpoint 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** > **Manage Users**.
2. On the Manage Users page, select the user account that you must duplicate.
3. Click **Duplicate**.
4. On the User Profile | Duplicate | <User Name> page, enter the appropriate information.
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**.

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** > **Manage Users**.
2. On the Manage Users page, select one or more users from the table, and click **Delete**.
3. On the User Delete Confirmation page, click **Delete**.

   Note:

   You cannot delete users:

   - With the login name *admin* from the Manage Users page.
   - Synchronized from LDAP.

Related links

Removing the deleted users from the database on page 221

Removing the deleted users from the database

Using this procedure, you can permanently delete a user from the database.

Before you begin

Ensure you have the permission to delete the selected user.

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, click **More Actions** > **Show Deleted Users**.
3. On the Show Deleted Users page, select the users to delete, and click **Delete**.
4. On the User Delete Confirmation page, click **Delete**.

Related links

Removing user accounts on page 221

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** > **Manage Users**.
2. Select one or more users and click **More Actions** > **Bulk Edit Users**.
3. 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.
4. Click **Run Now** or **Schedule**.
5. 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 224

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** > **Manage Users**.
2. Click **More Actions** > **Status of Bulk Edit Users Jobs**.
3. 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.
4. 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** > **Manage Users**.
2. Click **More Actions** > **Status of Bulk Edit Users Jobs**.
3. On the Schedule Bulk Edit of Users page, select one or more bulk edit jobs and click **Delete**.
4. 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.
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 624.
- 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 224.

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	Displays 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 you provide.
Presence/IM Domain	Displays 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 you provide.
Auto Generate Communication Profile Password	The option to automatically generate the communication profile password. If you select the **Auto Generate Communication Profile Password** option, the system disables the **Communication Profile Password** field.
Communication Profile Password	The communication profile password. The field is available only if you enable the communication profile. The password policy is configured on the **Users** > **User Management** > **Communication Profile Password Policy** page. When you provide the communication password value during bulk edit of users, the system overwrites any existing communication profile passwords of the user.
Edit	The link to change the Communication Profile password. When you click the **Edit** link, the system displays the **Confirm Password** field along with the **Generate** and **Cancel** links.

Table continues…

Name	Description
Confirm Password	The communication profile password to reenter for confirmation.
Generate	The option to automatically generate the communication profile password. System Manager sends the generated password to the user, if: • Email configuration properties are set on the **Services** > **Configurations** > **Settings** > **SMGR** page. For more information, see “Configuring email properties”. • **Email Address** is configured on the **Identity** tab.
Cancel	Cancels the password change operation.
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 (+).
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	The option to register an H.323 endpoint and a SIP endpoint together at the same time to the same extension. For more information about the SIP and H.323 dual registration feature, see *Avaya Aura® Communication Manager Feature Description and Implementation* on the Avaya Support website at http://support.avaya.com.

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 223.

Name	Description
Policy	When you enable the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page, the system displays the **Policy** field to select the required policy for the Session Manager communication profile. For more information, see *Administering Avaya Aura® Session Manager*. Based on the policy selection, the system displays the relevant fields. The options are: • **fixed**: When you select this option, the system displays the **Primary Session Manager**, **Secondary Session Manager**, **Third Session Manager**, and **Fourth Session Manager** fields. The default value is **fixed**. • **fixed-region**: When you select this option, the system displays the **Primary Region**, **Secondary Region**, **Third Region**, and **Fourth Region** fields. The system assigns the primary, secondary, third, or fourth region to the Session Manager Communication profile. • **location-region**: When you select this option, the system does not display the **Primary Session Manager** and **Secondary Session Manager** fields and dynamically assigns Session Managers based on the mapping of locations to regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Location to Region Mapping** page. **Note:** If the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page is not enabled, the system displays the **Primary Session Manager** and **Secondary Session Manager** fields similar to the Release 8.1.x and earlier system.
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.

Table continues…

Name	Description
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. This is an optional field. All the four Session Manager values must be unique. For example, if you select the same Session Manager server instance in the **Secondary Session Manager** field as the **Primary Session Manager** field, the system displays the following error message: `The Secondary Session Manager cannot be the same as the Primary Session Manager.`
Third Session Manager	The Session Manager instance that you select as the third Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary or the secondary Session Manager server becomes unavailable. This is an optional field. You must select the value of the Session Manager servers as per the order of display. For example, if you select the third Session Manager value before the secondary Session Manager, the system displays the following error message: `Selection of Session Managers should be as per their order of display. Select Secondary Session Manager before Third Session Manager.`
Fourth Session Manager	The Session Manager instance that you select as the fourth Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary, secondary, or third Session Manager server becomes unavailable. This is an optional field.
Primary Region	The Session Manager region that you select as the primary region. You must select the primary region of the Session Manager server. You can create the regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Session Manager Groups** page. You must select the value of regions as per the order of display. For example, if you select the secondary region value before the primary region, the system displays the following error message: `Selection of regions should be as per their order of display. Select Primary Region before Secondary Region.`

Table continues…

Name	Description
Secondary Region	The Session Manager region that you select as the secondary region. This is an optional field. **Note:** • If you select the same region for the primary and secondary regions, then there must be a minimum of two Session Managers in that region. • If you select 4 different regions, then there must be a minimum of 1 Session Manager in each region. If you select the same region and the region does not have sufficient Session Managers, the system displays the following error message: `<Secondary Region> - <Name_of_the_Region> the assigned regions must contain enough SMs to satisfy the Primary/Secondary/Third/Fourth region selection count.`
Third Region	The Session Manager region that you select as the third region. This is an optional field.
Fourth Region	The Session Manager region that you select as the fourth region. This is an optional field.
Survivability Server	For local survivability, you can specify a survivability server. The server provides survivability communication services to devices associated with a communication profile, when the local connectivity to Session Manager instances in Avaya core is lost. If you select 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. This survivable remote server is resident with the Branch Session Manager selected. 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. After typing a minimum of 3 characters, wait for three seconds to capture the final keyword and fetch the required results.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.

Table continues…

Name	Description
Block New Registration When Maximum Registrations Active	If you select the check box, the system denies any new registrations with Session Manager when an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit. 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 affect the call and keeps that device registered for that call only.
Origination Application Sequence	The application sequence the system invokes when routing 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 invoked when the system routes 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.
Emergency Calling Origination Sequence	The list of application sequences invoked when the system routes emergency calls from this user.
Emergency Calling Termination Sequence	The list of application sequences invoked when the system routes emergency calls to this user.
Home Location	The 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 the IP Address Pattern of any 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** page 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.
Enable Client	The drop-down list of the supported clients. Select the required client.

Communication Profile tab: Avaya Breeze® 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 223.

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. 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 223.

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.

Name	Description
Use Next Available Extension	The option 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.
Sub Type	This field is configured for CS 1000 station types only. You can select the specific set for **Set Type**. On the Manage Endpoint page, **Sub Type** is labeled as **Set**.

Table continues…

Name	Description
System ID	This field is configured for CS 1000 station types only. This field allows you to leave the field blank or enter a string of up to 9 characters. With Release 8.0, more than one station can use the combination of **System ID** and **Terminal Number**. With Release 8.0.1, each station must have a unique combination of **System ID** and **Terminal Number**.
Security Code	The security code for authorized access to the endpoint.
Preferred Handle	Avaya SIP or Avaya E.164 handle 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 **Profile Type**.
Allow H.323 and SIP Endpoint Dual Registration	The option to register an H.323 endpoint and a SIP endpoint together at the same time to the same extension. For more information about the SIP and H.323 dual registration feature, see *Avaya Aura® Communication Manager Feature Description and Implementation* on the Avaya Support website at http://support.avaya.com.

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. For more information, see Create new profile option on page 223.

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 223.

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. • 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 delete the user.

Communication Profile: Avaya 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 223.

Name	Description
System	The Avaya Messaging system to which you add a mailbox.

Table continues…

Name	Description
Refresh	The option to get information about company, departments, and feature groups from Avaya Messaging and save locally on System Manager for future use. You do not require to refresh for every user.
Use Next Available Mailbox	The option to specify if the system must use the next mailbox number to associate with this profile.
Mailbox Range	The range of mailbox numbers assigned to the Avaya Messaging system. **Note:** This option is available only when you select the **Use Next Available Mailbox** check box.
Numeric Password	The numeric password used to log in to the Avaya Messaging system.
Application User Password	The password used to gain access to non-telephone applications, such as Web Client, iLink Pro, iLink Pro Mobile, and iLink Pro Desktop.
Company	The name of the company to which the user belongs.
Department	The department to which the user belongs.
Feature Group	The feature group name that determines the rules for the mailboxes associated with it.
Capability	The type of functionality the user contains. The values are: • **Standard** • **Fax** • **Messaging** • **Collaboration** • **Messaging and Collaboration**
Domain Account Name	The mailbox NT account name for the Avaya Messaging profile. The options are: • **Same as Login Name** • **Admin Specified**
Synchronization User Name	The account name that is used to gain access to the email server, for example, Microsoft Exchange and Google Gmail. The options are: • **Same as Login Name** • **Admin Specified**

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 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 223.

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 Presence Services. This system selects the SIP entity 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 SIP Entity	The Presence Services instance for the user.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with 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 223.

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.

Name	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: Equinox 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 223.

Name	Description
Equinox User Password	The password that is used to log in to the Avaya Workplace Client Management.
Virtual Room Number	The number of a virtual room that is used to create a conference. By default Virtual Room Number serves as Meeting ID when a conference is created. The options are: • **Use Phone Number**: This will use Communication Manager extension. Use this option only if Communication Manager profile is already associated with the user or being associated with the user. • **Auto Generate Virtual Room Number**: Use this option if the system needs to generate the Virtual Room Number automatically.

Button	Description
Run Now	Runs the bulk user edit job immediately.

Table continues…

Button	Description
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 223

Filtering users

About this task

You can apply filter to the following user information:

- First Name
- Surname
- Display Name
- Login Name
- SIP Handle

You can apply one or more filters to view users that match the filter criteria. Table filter works based on “starts with” mechanism.

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, click the **Filter menu** icon displayed next to the column according to which you want to filter.
3. Enter the information for one or more of the following filter criteria:
   - To filter users by the first name, in the **First Name** column, enter the first 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 surname, in the **Surname** column, enter the last name of the user.
   - To filter users by the display name, in the **Display Name** column, enter the display name of the user.
   - 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 (E.164 handle and Avaya SIP Handle) of the user.
4. **(Optional)** To hide the column filters, click **Disable**.

   This action does not clear any filter criteria that you had set.

5. Press Enter from keyboard to apply filters.

   The table displays the users that match the filter criteria.

6. To clear the filter criteria, click the **Clear Filter** icon displayed on the lower-right corner of the table.

User searchable fields

System Manager supports user search for **User Management** objects.

The following table lists the user searchable fields in the search component:

User Management object	Field Names	Supported Actions
User	**User Name**, **First Name**, **Last Name**, **Display Name**, **Endpoint Display Name**, **Login Name**, **Handle**	View, Edit, Delete

Note:

- In the **Search** component, you can find a user match only when the searchable field starts with the search query.
- For handle search, all the handles get concatenated in one string. If you have multiple handles, you can only search using the start of the first handle string.

For information about the search component, see “Search component for Communication Manager objects”.

Searching for users by using Search component

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. In the **Search** component, at the top of the **Manage Users** page, search for users.

Searching for users by using Advanced Search

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, click **Options** > **Advanced Search** on the upper-right corner of the page.
3. In the Criteria section, do the following:
   a. In the first field, select the operator.

      Note:

      This field appears dimmed if there is only one search criteria section.

b. In the second field, select the search criterion.

c. In the third field, enter the condition.

d. In the fourth field, enter the search value.

4. To add another search criterion, click plus (**+**) and repeat Step 3a through Step 3d.

   To delete a search criterion, you must click the **Delete** icon. The system displays this icon when more than one search criterion is available.

5. Click **Apply Filter**.

   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** > **Manage Users**.
2. On the Manage Users 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**.
3. On the User Profile | Edit | <User Name> or User Profile | Add page, click the Membership tab.
4. Click **Assign Roles**.
5. In the Assign Roles section, select the roles.
6. To assign the roles to the selected user, click **Select**.
7. On the User Profile | Edit | <User Name> or User Profile | Add 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** > **Manage Users**.
2. On the Manage Users page, select the users and click **More Actions** > **Assign Roles**.
3. On the Assign Roles page, select the roles from the **Available Roles** section.
4. Click **Commit** to assign the roles to the selected users.

Removing roles from a user

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** > **Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Membership** tab.
4. 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**
5. 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**.
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**.

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** > **Manage Users**.
2. On the Manage Users 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**.
3. On the User Profile | Edit | <User Name> page or the User Profile | Add page, click the **Membership** tab.
4. In the Group Membership section, click **Add To Group**.
5. On the Assign Groups page, select the groups from the **Available Groups** section.
6. Click **Select** to assign the groups to the user.
7. 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

Assigning a user to a group using XML on page 241

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** > **Manage Users**.
2. On the Manage Users page, select the users and click **More Actions** > **Add To Group**.
3. On the Add to Group page, select the groups from the **Available Groups** section.
4. 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** > **Manage Users**.
2. On the Manage Users 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**.
3. On the User Profile | Edit | <User Name> page, click the **Membership** tab.

4. In the Group Membership section, select the groups from which you want to remove the user and click **Remove From Group**.
5. Click **Commit** to save the changes.

Related links

Removing a user from a group using XML on page 242

Assigning a user to a group using XML

Procedure

1. In your XML file, include a portion of the following code, corresponding to the group to which you want to assign the user.

```
<ns9:ipHoteling>false</ns9:ipHoteling>
<ns9:addGroupList>
    <ns9:groupMemData>
        <ns9:groupType>PickupGroupData</ns9:groupType>
        <ns9:groupnumber>1</ns9:groupnumber>
    </ns9:groupMemData>
    <ns9:groupMemData>
        <ns9:groupType>GroupPageData</ns9:groupType>
        <ns9:groupnumber>1</ns9:groupnumber>
    </ns9:groupMemData>
    <ns9:groupMemData>
        <ns9:groupType>CoverageAnswerGroupData</ns9:groupType>
        <ns9:groupnumber>1</ns9:groupnumber>
    </ns9:groupMemData>
    <ns9:groupMemData>
        <ns9:groupType>TermExtGroupData</ns9:groupType>
        <ns9:groupnumber>1</ns9:groupnumber>
    </ns9:groupMemData>
    <ns9:groupMemData>
        <ns9:groupType>HuntGroupData</ns9:groupType>
        <ns9:groupnumber>1</ns9:groupnumber>
    </ns9:groupMemData>
</ns9:addGroupList>
```

2. Save the XML file.
3. Complete the steps in Bulk importing of users on page 377.

Related links

Group types on page 241
Assigning groups to a user on page 239

Group types

Use this table to see the XML code used for each group.

Table 3: Group types table

GUI name	XML corresponding name
Pickup Group	PickupGroupData
Group Page	GroupPageData

Table continues…

GUI name	XML corresponding name
Coverage Answer Group	CoverageAnswerGroupData
Terminating Extension Group	TermExtGroupData
Hunt Group	HuntGroupData
Intercom Group	IntercomGroupData
Coverage Path	CoveragePathData

Related links

Assigning a user to a group using XML on page 241

Removing a user from a group using XML

Procedure

1. In your XML file, include a portion of the following code, corresponding to the group from which you want to remove the user.

```
<ns9:ipHoteling>false</ns9:ipHoteling>
<ns9:removeGroupList>
    <ns9:groupMemData>
        <ns9:groupType>PickupGroupData</ns9:groupType>
        <ns9:groupnumber>1</ns9:groupnumber>
    </ns9:groupMemData>
    <ns9:groupMemData>
        <ns9:groupType>GroupPageData</ns9:groupType>
        <ns9:groupnumber>1</ns9:groupnumber>
    </ns9:groupMemData>
    <ns9:groupMemData>
        <ns9:groupType>CoverageAnswerGroupData</ns9:groupType>
        <ns9:groupnumber>1</ns9:groupnumber>
    </ns9:groupMemData>
    <ns9:groupMemData>
        <ns9:groupType>TermExtGroupData</ns9:groupType>
        <ns9:groupnumber>1</ns9:groupnumber>
    </ns9:groupMemData>
    <ns9:groupMemData>
        <ns9:groupType>HuntGroupData</ns9:groupType>
        <ns9:groupnumber>1</ns9:groupnumber>
    </ns9:groupMemData>
</ns9:removeGroupList>
```

2. Save the XML file.
3. Complete the steps in Bulk importing of users on page 377.

Related links

Removing a user from groups on page 240

Viewing deleted users

About this task

When you remove a user from the Manage Users page by using the **Delete** option, the system temporarily removes and stores the user in the **Deleted Users** table.

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, click **More Actions** > **Show Deleted Users**.

   On the Soft Deleted Users page, the system displays the temporarily deleted users in the Deleted Users table.

Restoring a deleted user

About this task

Use this procedure to restore a user that you deleted by using the **Delete** option on the Manage Users page.

Before you begin

Ensure that you have permission to restore the selected deleted user.

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, click **More Actions** > **Show Deleted Users**.
3. On the Soft Deleted Users page, select the user that you want to restore, and click **Restore**.
4. On the User Restore Confirmation page, click **OK**.
5. 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 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 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 a user address

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, do one of the following:
   - To add an address for 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**.
3. On the Add/Edit Address page, enter the address details.
4. Click **OK** to add the address.
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**.

Related links

Add Address field descriptions on page 246

Editing an address

About this task

Use this procedure to modify the address of a user. Note that you cannot edit a shared address.

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, select a user, and click **Edit** > **Identity** > **Address**.
3. In the **Address** area, select the mailing address that you want to modify and click **Edit**.

   You cannot modify a shared address by using this feature.

4. On the Add/Edit Address page, modify the information.
5. Click **OK**.
6. Click **Commit**.

Deleting an address

About this task

Use this procedure to delete a private mailing address from the database.

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. Do one of the following :
   - If you are on the User Profile | Add page or on the User Profile | Duplicate | <User Name> page and have added an address, then navigate to **Identity** > **Address**.
   - On the Manage Users page, select a user and click **Edit** > **Identity** > **Address**.
3. Select the address that you want to delete and click **Delete**.

   If the address that you delete is a shared address, the system removes the address from the address list of the user, but not from the database
4. 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

Use this procedure to choose a shared address for a user from the common addresses database. You can assign and remove a shared address.

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, do 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**.
3. On the User Profile | Add page or the User Profile | Edit | <User Name> page, click **Identity** > **Address** > **Choose Shared Address**.
4. On the Choose Shared Address page, click one or more shared addresses.

   For a new user, enter valid information in all mandatory fields on all tabs of the User Profile | Add page before you click **Commit**. If you enter invalid information, the system displays an error message.

5. Click **Select**.
6. Click one of the following:
   - **Commit**: To save the changes.
   - **Commit & Continue**: To save the changes and stay on the same page for making further modifications.

Related links

Choose Address field descriptions on page 247

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 610
Adding a shared address on page 610

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 support communication interactions established through Avaya Communication Services. Communication profiles can be associated to the following entities:

- CM Endpoint
- Messaging
- Avaya Messaging
- Session Manager
- CS 1000
- IP Office
- Presence
- Avaya Breeze® platform
- Avaya Meetings Server

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 of the user. A communication

subsystem is a service or infrastructure that manages the establishment and controls or routes the communication interactions.

System Manager supports maximum five communication profile sets for each user. You can add maximum three CM Endpoint profiles and one Messaging profile for each user, and the 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** > **Manage Users**.
2. On the Manage Users page, do one of the following:
   - To create a new user account, click **New**.
   - To add a communication profile to an existing user, select the user and click **Edit**.
3. On the User Profile | Add or the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the communication profile section, click **New**.
5. In the **Name** field, enter the name of the new communication profile.
6. **(Optional)** To mark the profile as default, select the **Default** check box.
7. Click **Done**.
8. Click **Commit**.

Related links

User Profile | Add field descriptions on page 285

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** > **Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **Communication Profile** section, select a profile.
5. Click **Delete**.
6. Click **Commit**.

Result

When you delete a communication profile, System Manager deletes all associated communication addresses.

Creating a new communication address for a communication profile

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, do one of the following :
   - To create a new user account, click **New**.
   - To add a communication profile address to an existing user, select the user and click **Edit**.
3. On the User Profile | Add or User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **Communication Profile** section, select a communication profile.
5. In the **Communication Address** section, click **New**.
6. In the **Type** field, enter a communication protocol.
7. 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, an instant messenger ID, or the SIP address of a SIP-enabled device.
8. Enter the domain name in the field next to **Fully Qualified Address** field.
9. Click **OK**.
10. Click **Commit**.

Related links

User Profile | Edit | <User Name> field descriptions on page 307
User Profile | Add field descriptions on page 285

Modifying the communication address

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **Communication Profile** section, select a profile.
5. In the **Communication Address** section, select a communication address.
6. Click **Edit**.
7. Modify the information in the respective fields.
8. Click **OK**.
9. Click **Commit**.

Related links

User Profile | Edit | <User Name> field descriptions on page 307

User Profile | Add field descriptions on page 285

Deleting a communication address from a communication profile

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **Communication Profile** section, click a communication profile.
5. In the **Communication Address** section, select a communication address from the table.
6. Click **Delete**.
7. Click **Commit**.

Related links

User Profile | Edit | <User Name> field descriptions on page 307
User Profile | Add field descriptions on page 285

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 also administer a third and fourth Session Manager to a communication profile for redundancy service if the policy-based assignment of Session Manager feature is enabled.

You can configure the system to invoke application sequences when routing calls from (origination) or to (termination) 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. The server provides survivability communication services for devices associated with a communication profile, when local connectivity to Session Manager instances in the Avaya 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 251

User Profile | Add field descriptions on page 285

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.

Lync integration simplification

In releases earlier than 7.0, for Lync integration, the administrator had to administer the Presence Services handle of an Avaya Aura® user twice as:

1. Avaya Presence/IM (formerly XMPP) handle
2. Avaya SIP handle

The duplicate administration was required for proper routing of the Lync originated subscription and IM requests.

Starting with Session Manager Release 7.0, the Presence Services handle is administered only once.

To support tighter integration with Microsoft Lync, Session Manager:

- Supports routing rules, configured in System Manager, to deliver Lync Presence/IM traffic to Presence and Avaya Multimedia Messaging as appropriate.
- Recognizes and routes on the Presence/IM handle type.
- Inserts the media type (mtype) parameter in the Route header when routing to SIP entities.

Note:

The Lync server does not connect with a Branch Session Manager in branch locations.

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 profile of a user

With User Profile Management, you can create the CM Endpoint communication profile for a user to create an association between an endpoint and a user.

You can add, view, modify, and delete endpoint profile. You can go to Endpoint Management pages to modify any of the endpoint fields that are not available through User Profile Management.

Login name of endpoint profile

The login name in the Identity section on the User Profile | Add and User Profile | Edit | <User Name> pages is the user name that is associated with the CM Endpoint communication profile. This user name appears in the **User** column in the Endpoint 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.

Note:

Endpoint Display Name and **Localized Display Name** are auto populated while user creation is based on **Last Name** and **First Name**. **Endpoint Display Name** and **Localized Display Name** values get automatically changed if any change is made to **Last Name** and **First Name** value from User Import, Web Console or Web Service operation for user update.

If the **Endpoint Display Name** and **Localized Display Name** are edited manually (not based on Last Name/First Name) during user creation or user edit operation, then these values will never get auto changed even if changes are made to user's **Last Name** and **First Name** from User Import, Web Console or Web Service operation for user update.

Creating CM Endpoint profile

You can create one default or primary Communication Profile for a user. To this default profile, you can add one CM Endpoint profile. You can add a maximum of three CM Endpoint 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** > **Manage Users**.
2. On the Manage Users page, do one of the following:
   - To create a CM Endpoint profile for a new user profile, click **New**.
   - To create a CM Endpoint profile for an existing user, select the user and click **Edit**.
3. Click the **Communication Profile** tab.
4. In the PROFILES section, click the toggle button next to **CM Endpoint Profile**.

   System Manager enables **CM Endpoint Profile** and displays the fields of the CM Endpoint profile.
5. Perform the following:
   a. In the **System** field, select the Communication Manager system to add an endpoint.
   b. In the **Profile Type** field, select **Endpoint**.
   c. In the **Extension** field, type the extension number, and then click the **Editor** button next to the given extension number.
   d. In the **Template** field, select the required template for the endpoint.
   e. In the **Set Type** field, select the required set type for the endpoint.
6. **(Optional)** To delete the endpoint from the communication management device after removing the association between the endpoint and the user, select the **Delete on Unassign 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**.

Related links

User Profile | Add field descriptions on page 285

Viewing the station profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, select a user and click **View**.
3. Click the **Communication Profile** tab.

Modifying the CM Endpoint profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the CM Endpoint Profile section, modify the relevant information in the fields.
5. Do one of the following:
   - To save the changes to the database, click **Commit**.
   - To cancel the action and return to the previous page, click **Cancel**.

Related links

User Profile | Add field descriptions on page 285

Using the automatically generated call routes for SIP routing

About this task

Based on the primary, secondary, third, or fourth Session Manager specified in **Session Manager Communication Profile**, the system automatically determines a route pattern.

Before you begin

In the Communication Manager instance associated with System Manager, do the following:

1. On the Route Pattern page, specify the primary Session Manager.

   Note:

   If Alternate Failover Routing is enabled on Communication Manager, then Route Pattern administration is not required.

2. Select a SIP endpoint.

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. Click **Communication Profile**.
3. In **Session Manager Profile** > **SIP Registration** > **Primary Session Manager**, click a primary Session Manager.

4. In **CM Endpoint Profile**, do the following:
   a. In the **Set Type** field, enter the details of a SIP set type.
   b. Select the **Calculate Route Pattern** check box.

Result

The system automatically generates route patterns for the specified user and for the Session Manager set as the primary Session Manager.

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** > **Manage Users**.
2. On the Manage Users page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **CM Endpoint Profile** section, clear the check box next to the **CM Endpoint Profile** label.
5. 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 an 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** > **Manage Users**.
2. On the Manage Users page, select a user, and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **CM Endpoint Profile** section, clear the check box next to the **CM Endpoint Profile** label.

5. 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

User Profile | Add field descriptions on page 285

Messaging profile administration

Messaging profile of a user

With User Profile Management, you can create the Messaging communication profile for a user to create an association between a subscriber mailbox and a user.

You can add, view, modify, and delete messaging profile. You can go to Subscriber Management pages to modify any of the subscriber fields that are not available through User Profile Management.

Login name of messaging profile

The login name in the Identity section on the User Profile | Add and User Profile | Edit | <User Name> pages is the user name that is associated with the Messaging communication profile. This user name appears in the **User** column in the Subscriber List.

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 Messaging profile

You can create one default or primary Communication Profile for a user. To this default profile, you can add one Messaging profile per user.

Adding a messaging profile for a user

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, perform one of the following steps:
   - If you are creating a messaging profile for a new user profile, click **New**.
   - If you are creating a messaging profile for an existing user, select the user and click **Edit**.
3. Click the **Communication Profile** tab.
4. In the Messaging Profile section, select the check box next to the **Messaging Profile** label.
5. 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.

6. 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

User Profile | Add field descriptions on page 285

Modifying a messaging profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the PROFILES section, click Messaging Profile, and modify the relevant information in the fields.
5. 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

User Profile | Add field descriptions on page 285

Viewing a messaging profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, select a user and click **View**.
3. Click the **Communication Profile** tab.

Result

The Messaging Profile section displays the messaging profile information of the user.

Related links

User Profile | Add field descriptions on page 285

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** > **Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the Messaging Profile tab, clear the check box next to the **Messaging Profile** label.
5. 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** > **Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the Messaging Profile section, clear the check box next to the **Messaging Profile** label.
5. 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 profile administration

CS 1000 profile administration

With User Management, you can create CS 1000 Endpoint Profile to create an association between an endpoint and a user.

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 user to Element Manager.

Related links

Redirecting the CS 1000 user to Element Manager on page 259

Redirecting the CS 1000 user to Element Manager

Before you begin

A user must exist with at least one communication profile.

To create a new user, navigate to **Users** > **User Management** > **Manage Users** > **New**.

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the PROFILES section, click **CS 1000 Endpoint Profile** that you must update and click **Update**.

   The system displays 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.
5. Enter the relevant information and click **Save**.

   The system displays the Manage Users page.

Adding a CS 1000 profile for a user

Before you begin

A user must exist.

To create a new user, navigate to **Users** > **User Management** > **Manage Users** > **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** > **Manage Users**.
2. On the Manage User 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**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. 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.
5. 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 user profile

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. Click **Update**.
5. In the CS 1000 Element Manager window, enter the relevant information in the fields.

   Note:

   In CS 1000 Element Manager, do not update the CPND name. The system maps the CPND name to the System Manager UPM user **Localized Display Name**. Use System Manager UPM to update the CPND name. For more details, see the "Communication profiles synchronization" section.

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 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 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

User Profile | Add field descriptions on page 285

Viewing an IP Office endpoint profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the 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

User Profile | Add field descriptions on page 285

Modifying an IP Office endpoint profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the 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

User Profile | Add field descriptions on page 285

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 navigation pane, click **Manage Users**.
3. On the User Management page, select a user, and do 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 the properties file on page 264

Removing the association between an IP Office endpoint profile and a user from the properties file

About this task

Use the procedure to remove association between an IP Office endpoint profile and a user only when IP Office is unused or corrupted.

Procedure

1. Using putty, navigate to the `$ABG_Home/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 ensure that the user data on IP Office and System Manager is synchronized.
3. Save the properties file.
4. To apply the changes, you must restart the Application server. At the prompt, type `smgr restart`.

   During a restart the System Manager web console will be unavailable for 10-15 minutes.
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 Application server.

Related links

Removing the association between an IP Office endpoint profile and a user on page 263

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 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 266

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 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 268

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 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 269

Deleting contacts from the default contact list

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the 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

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 user, public, or private contact.
Display/Login Name	The unique login name or display name of the contact.
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.

Name	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.

Table continues…

Field	Description
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.
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

About this task

Adding a private contact to a user is a two-step process. First, you add the private contact and then you add the new private contact to the associated contacts. Ensure that you commit your updates after you add the private contact.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the 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 following information in the Contact Details section.
   - Last name
   - First name
   - Middle name
   - Description
   - Company name
   - Localized display name
   - Endpoint display name
   - Language
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**.
11. In the Associated Contacts section, click **New**.

12. On the New Associated Contact page, select the new private contact and click **Add**.
13. 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 277

Modifying details of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the 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 278

Viewing details of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the 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 280

Deleting private contacts of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the 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 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 246

Modifying postal address of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the 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 282

Deleting postal addresses of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the 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 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 247

Adding a contact address for a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the 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 281

Modifying a contact address of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the 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 282

Deleting contact addresses of a private contact

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the 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.

Table continues…

Button	Description
New	Displays the **Add Address** page where you can add a new postal address of the private contact.
Delete	Deletes the selected postal address.
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	Displays the **Edit Address** page. Use this page to modify an existing postal address of the private contact.
New	Displays 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	Displays 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.
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	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 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.
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	Returns 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. • **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 601

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. • **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 602

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.

Name	Description
Select check box	Select the check box for the tenant from the list of tenants to view the organization hierarchy. 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.
Refresh Users	Updates the tenant organization hierarchy. Use this 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

Name	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.

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 in the list.

Button	Description
View	Displays the User Profile | View | <User Name> page where you can view the details of the selected user.
Edit	Displays the User Profile | Edit | <User Name> page where you can modify the details of the selected user.
New	Displays the User Profile | Add page where you can create a new user.

Table continues…

Button	Description
Duplicate	Displays the User Profile | Duplicate | <User Name> 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, 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 selected users.
More Actions > **Export Delta Users**	Displays the Export users page where you can export the added, updated, or deleted user-related data for the specific delta period. **Note:** The permanently deleted users login-names in the delta period are identified on the basis of audit logs of permanently deleted users in the system. Therefore, if you change the Data Retention settings for **LogPurgeRule**, the system might affect the permanently deleted users list in the exported zip file.
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.
Options > **Advanced Search**	Displays fields where you can specify the search criteria for searching a user.
Options > **Clear Filters**	Clears the filter criteria.
Filter menu	You can find the **Filter menu** icon next to the name of each column. Filters the data based on the search criteria.
Select: All	Selects all users in the table.
Select: None	Clears the check box selections.

Table continues…

Button	Description
	Refreshes the user information in the table.

Criteria

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

Name	Description
Criteria	The criteria to search. The options are: • **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 3**: Lists the value for the search criterion. The User Management service retrieves and displays users that match this value.

User Profile | Add field descriptions

Use the User Profile | Add page to create or add 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 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** can be up to 256 characters.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the endpoints. For example, Miller. Typically, the name is in the written or spoken language of the user. **Last Name (Latin Translation)** can be up to 256 characters. **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 and first names change. • Filled, the values remain the same 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** can be up to 256 characters.
First Name (Latin Translation)	The user-preferred first name that the system must display on the endpoints. For example, John. Typically, the name is in the written or spoken language of the user. **First Name (Latin Translation)** can be up to 256 characters.
Middle Name	The middle name of the user, if any. **Middle Name** can be up to 256 characters.
Description	A brief description of the user. **Description** can be up to 1024 characters.

Table continues…

Name	Description
Login Name	The login name of the user. **Login Name** can be up to 256 characters. With Release 8.1.3, the **Login Name** field supports the login name with apostrophe (‘). For example, aine’mars@xyz.com. The following characters are supported: • , • - • _ • ? • % • ! • ~ • * • (•) • = • + • $ • ,, • ; • . • ‘ 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 the login name 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.
Email Address	The email address of the user for receiving email notifications. **Email Address** can be up to 256 characters.

Table continues…

Name	Description
User Type	The authentication type that defines how the system authenticates 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, **User Type** is always Basic. Therefore, the **User Type** field remains invisible in the Excel file.
Password	The password to log in to the System Manager web console. **Password** can be up to 256 characters. **Password** is not a mandatory field for the telephony user.
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. **Localized Display Name** can be up to 256 characters. If you do not provide any value for **Localized Display Name**, System Manager specifies the value as a combination of **First Name** and **Last 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. **Endpoint Display Name** can be up to 256 characters. If you do not provide any value for **Endpoint Display Name**, System Manager specifies the value as a combination of **First Name (Latin Translation)** and **Last Name (Latin Translation)**.
Title Of User	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. **Title Of User** can be up to 256 characters.
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 of the user. For example, 20081234. **Employee ID** can be up to 256 characters.
Department	The department to which the user belongs. For example, Human Resources. **Department** can be up to 256 characters.
Company	The organization where the user works. For example, Avaya LLC **Company** can be up to 256 characters.

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 options 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 to add the address details.
Edit	Displays the Edit Address 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, not for Session Manager and Communication Manager.

Name	Description
Language	The localized language 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 of the user.
Delete	Deletes the localized names that you select for the user.
Add	Adds or edits the localized name of 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 on the **Users** > **User Management** > **Communication Profile Password Policy** page. When you provide the communication password value during bulk edit of users, the system overwrites any existing communication profile passwords of the user. For information about password policy, see “Communication profile password policy”.
Confirm Password	The communication profile password to reenter for confirmation.
Generate	The option to automatically generate the communication profile password. System Manager sends the generated password to the user if you: • Set the email configuration properties on the **Services** > **Configurations** > **Settings** > **SMGR** page. For more information, see “Configuring email properties”. • Configure **Email Address** on the **Identity** tab. By default, the **Generate** link is available for creating a new user account. The **Edit** link is available for modifying user accounts. When you click the **Edit** link, the system displays **Confirm Password** along with the **Generate** and **Cancel** links.
Name	The name of the communication profile that you must select .

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 of adding 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 handle.
Handle	A unique communication address of the user. Communication Manager Release 7.1.2 and later support alphanumeric handles.
Domain	The name of the domain with which the handle is registered.

Button	Description
New	To add a new communication address.
Edit	To edit the information of a selected communication address.
Delete	To delete the selected communication address.

When you click **New** and **Edit** in the Communication Address section, the page displays the following fields that define the communication address of the user:

Name	Description
Type	The type of handle. The options 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 13 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 calendar. • **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 that 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 using which the user can send or receive messages. You must provide a 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
Policy	When you enable the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page, the system displays the **Policy** field to select the required policy for the Session Manager communication profile. For more information, see *Administering Avaya Aura® Session Manager*. Based on the policy selection, the system displays the relevant fields. The options are: • **fixed**: When you select this option, the system displays the **Primary Session Manager**, **Secondary Session Manager**, **Third Session Manager**, and **Fourth Session Manager** fields. The default value is **fixed**. • **fixed-region**: When you select this option, the system displays the **Primary Region**, **Secondary Region**, **Third Region**, and **Fourth Region** fields. The system assigns the primary, secondary, third, or fourth region to the Session Manager Communication profile. • **location-region**: When you select this option, the system does not display the **Primary Session Manager** and **Secondary Session Manager** fields and dynamically assigns Session Managers based on the mapping of locations to regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Location to Region Mapping** page. **Note:** If the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page is not enabled, the system displays the **Primary Session Manager** and **Secondary Session Manager** fields similar to the Release 8.1.x and earlier system.
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.

Table continues…

Name	Description
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. This is an optional field. All the four Session Manager values must be unique. For example, if you select the same Session Manager server instance in the **Secondary Session Manager** field as the **Primary Session Manager** field, the system displays the following error message: `The Secondary Session Manager cannot be the same as the Primary Session Manager.`
Third Session Manager	The Session Manager instance that you select as the third Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary or the secondary Session Manager server becomes unavailable. This is an optional field. You must select the value of the Session Manager servers as per the order of display. For example, if you select the third Session Manager value before the secondary Session Manager, the system displays the following error message: `Selection of Session Managers should be as per their order of display. Select Secondary Session Manager before Third Session Manager.`
Fourth Session Manager	The Session Manager instance that you select as the fourth Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary, secondary, or third Session Manager server becomes unavailable. This is an optional field.
Primary Region	The Session Manager region that you select as the primary region. You must select the primary region of the Session Manager server. You can create the regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Session Manager Groups** page. You must select the value of regions as per the order of display. For example, if you select the secondary region value before the primary region, the system displays the following error message: `Selection of regions should be as per their order of display. Select Primary Region before Secondary Region.`

Table continues…

Name	Description
Secondary Region	The Session Manager region that you select as the secondary region. This is an optional field. **Note:** • If you select the same region for the primary and secondary regions, then there must be a minimum of two Session Managers in that region. • If you select 4 different regions, then there must be a minimum of 1 Session Manager in each region. If you select the same region and the region does not have sufficient Session Managers, the system displays the following error message: `<Secondary Region> - <Name_of_the_Region> the assigned regions must contain enough SMs to satisfy the Primary/Secondary/Third/Fourth region selection count.`
Third Region	The Session Manager region that you select as the third region. This is an optional field.
Fourth Region	The Session Manager region that you select as the fourth region. This is an optional field.
Survivability Server	For local survivability, you can specify a survivability server. The server provides survivability communication services to devices associated with a communication profile, when the local connectivity to Session Manager instances in Avaya core is lost. If you select 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. This survivable remote server is resident with the Branch Session Manager selected. 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. After typing a minimum of 3 characters, wait for three seconds to capture the final keyword and fetch the required results.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.

Table continues…

Name	Description
Block New Registration When Maximum Registrations Active	If you select the check box, the system denies any new registrations with Session Manager when an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit. 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 affect the call and keeps that device registered for that call only.
Origination Application Sequence	The application sequence the system invokes when routing 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 invoked when the system routes 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.
Emergency Calling Origination Sequence	The list of application sequences invoked when the system routes emergency calls from this user.
Emergency Calling Termination Sequence	The list of application sequences invoked when the system routes emergency calls to this user.
Home Location	The 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 the IP Address Pattern of any 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** page 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.
Enable Client	The drop-down list of the supported clients. Select the required client.

Communication Profile tab: Avaya Breeze® 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 Communication Manager Endpoint profile exists for the user.

Name	Description
System	The Communication Manager system on which you add the endpoint. You must select the system.
Profile Type	The type of Communication Manager Endpoint profile that you create. You must select the profile type.
Use Existing Endpoints	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 with this profile. 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.
Endpoint Editor button	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 updates the modified data on the device or database only after you commit the changes on the User Profile | Edit | <User Name> 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.
Set Type	The set type of the endpoint. When you select a template, the system populates the corresponding set types.
Sub Type	This field is configured for CS 1000 station types only. You can select the specific set for **Set Type**. On the Manage Endpoint page, **Sub Type** is labeled as **Set**.
Terminal Number	This field is configured for CS 1000 station types only. You can enter numbers in the following range: 0.0.0.0 to 252.1.15.31. The first digit must be divisible by 4. For example: 0, 4, 8, …, 252.

Table continues…

Name	Description
System ID	This field is configured for CS 1000 station types only. This field allows you to leave the field blank or enter a string of up to 9 characters. With Release 8.0, more than one station can use the combination of **System ID** and **Terminal Number**. With Release 8.0.1, each station must have a unique combination of **System ID** and **Terminal Number**.
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. **Note:** You must clear Local Device Services Data on all Avaya Aura® Web Gateway nodes if you change the value of **Voice Mail Number**.
Preferred Handle	Numeric only handles, SIP handles, or non-SIP handles, that are administered for a user. The **Preferred Handle** field is optional. Select numeric handle for alphanumeric support. By default, the field is blank. If the type of SIP entity is Communication Manager, Session Manager uses the preferred handle 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**.
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 the **Calculate Route Pattern** check box, the system: • Populates the **Sip Trunk** field. • Makes the **Sip Trunk** field read-only.

Table continues…

Name	Description
SIP URI	A unique alphanumeric communication address of the user to make and receive voice or video calls. The **SIP URI** address can be: `<username-projectname>@<xyz.com>`.
Attendant	The option to enable the attendant feature on the endpoint. If you select this check box, you can administer the endpoint as an attendant. When you select the 9641SIP template type from **Template**, the system enables the **Attendant** check box.
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 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 delete the user.

Table continues…

Name	Description
Override Endpoint Name and Localized 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.
Allow H.323 and SIP Endpoint Dual Registration	The option to register an H.323 endpoint and a SIP endpoint together at the same time to the same extension. For more information about the SIP and H.323 dual registration feature, see *Avaya Aura® Communication Manager Feature Description and Implementation* on the Avaya Support website at http://support.avaya.com.

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 customer number of 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	The station profile information updated 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 in 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. The value in the field is valid only if you select the **Use Existing Subscriber on System** check box.
Messaging Editor	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 | <User Name> 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 delete the user.

Communication Profile tab: Avaya Messaging Profile

Name	Description
Officelinx System	The Avaya Messaging system to which you add a mailbox.
Refresh	The option to get information about company, departments, and feature groups from Avaya Messaging and save locally on System Manager for future use. You do not require to refresh for every user.
Mailbox Number	The mailbox number of the subscriber. It should be numeric only.
Numeric Password	The numeric password used to log in to the Avaya Messaging system.
Confirm Numeric Password	The numeric password you retype to confirm.
Application User Password	The password used to gain access to non-telephone applications, such as Web Client, iLink Pro, iLink Pro Mobile, and iLink Pro Desktop.

Table continues…

Name	Description
Confirm Application User Password	The password you retype to confirm.
Company	The name of the company to which the user belongs.
Department	The department to which the user belongs.
Feature Group	The feature group name that determines the rules for the mailboxes associated with it.
Capability	The type of functionality the user contains. The values are: • **Standard** • **Fax** • **Messaging** • **Collaboration** • **Messaging and Collaboration**
Domain Account Name	The mailbox NT account name of the Avaya Messaging profile.
Synchronization User Name	The account name used to gain access to the email server, for example, Microsoft Exchange and Google Gmail.

Note:

Only one-way update is supported for Officelinx elements. If you make any change directly on Officelinx, it does not reflect on System Manager. If you edit the user from System Manager, it overrides the changes you made directly on Officelinx.

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 not 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.

Name	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.

Table continues…

Name	Description
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 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.
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 | <User Name> 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: Equinox Conferencing

Name	Description
Equinox User Password	The Equinox user password.
Virtual Room Number	The virtual room number of the Equinox user.

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

Table continues…

Name	Description
SIP Entity	The option to route the SIP-based messages through Presence Services. This system selects the SIP entity 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 SIP Entity	The Presence Services instance for the user.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with 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: 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 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 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 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 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

Note:

Adding a private contact to a user is a two-step process. First, you add the private contact and then you add the new private contact to the associated contacts. Ensure that you commit your updates after you add the private contact.

Name	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.

Table continues…

Name	Description
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 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 menu	You can find the **Filter menu** icon next to the name of each column. Filters the data based on the search criteria.

Contacts tab: Private Contacts

Note:

Adding a private contact to a user is a two-step process. First, you add the private contact and then you add the new private contact to the associated contacts. Ensure that you commit your updates after you add the private contact.

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 menu	You can find the **Filter menu** icon next to the name of each column. Filters the data based on the search 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.

Related links

Communication profile password policy on page 614

User Profile | Edit | <User Name> field descriptions

Organization

Name	Description
Tenant	The name of the tenant that you 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** can be up to 256 characters.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the endpoints. For example, Miller. Typically, the name is in the written or spoken language of the user. **Last Name (Latin Translation)** can be up to 256 characters. **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 and first names change. • Filled, the values remain the same 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 endpoints. For example, John. Typically, the name is in the written or spoken language of the user. **First Name (Latin Translation)** can be up to 256 characters.
Middle Name	The middle name of the user, if any. **Middle Name** can be up to 256 characters.
Description	A brief description of the user. **Description** can be up to 1024 characters.
Status	The login status of the user
Update Time	The time when the user details were last modified.

Table continues…

Name	Description
Login Name	The login name of the user. **Login Name** can be up to 256 characters. With Release 8.1.3, the **Login Name** field supports the login name with apostrophe (‘). For example, aine’mars@xyz.com. The following characters are supported: • , • - • _ • ? • % • ! • ~ • * • (•) • = • + • $ • ,, • ; • . • ‘ 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 the login name 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.
Email Address	The email address of the user

Table continues…

Name	Description
User Type	The authentication type that defines how the system authenticates 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, **User Type** is always Basic. Therefore, the **User Type** field remains invisible in the Excel file.
Change Password	Displays two new fields: **New Password** and **Confirm Password**.
New Password	The new password to log in to the System Manager web console.
Confirm Password	The password that you reenter for confirmation.
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. **Localized Display Name** can be up to 256 characters. If you do not provide any value for **Localized Display Name**, System Manager specifies the value as a combination of **First Name** and **Last 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. **Endpoint Display Name** can be up to 256 characters. If you do not provide any value for **Endpoint Display Name**, System Manager specifies the value as a combination of **First Name (Latin Translation)** and **Last Name (Latin Translation)**.
Title Of User	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. **Title Of User** can be up to 256 characters.
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 of the user. For example, 20081234. **Employee ID** can be up to 256 characters.
Department	The department to which the user belongs. For example, Human Resources. **Department** can be up to 256 characters.

Table continues…

Name	Description
Company	The organization where the user works. For example, Avaya LLC **Company** can be up to 256 characters.

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. **Department** can be up to 256 characters.
Address Type	The type of address. The options 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 to add the address details.
Edit	Displays the Edit Address 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 language 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 of the user.

Table continues…

Button	Description
Delete	Deletes the localized names that you select for the user.
Add	Adds or edits the localized name of 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 Manager configured in the **Session Manager Communication Profile**.
Sip Trunk	The system makes this field available only for the SIP set type. If you select the **Calculate Route Pattern** check box, the system populates the **Sip Trunk** field, and makes the field read-only.
Allow H.323 and SIP Endpoint Dual Registration	The option to register an H.323 endpoint and a SIP endpoint together at the same time to the same extension. For more information about the SIP and H.323 dual registration feature, see *Avaya Aura® Communication Manager Feature Description and Implementation* on the Avaya Support website at http://support.avaya.com.

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 of adding 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 handle.

Table continues…

Name	Description
Handle	A unique communication address of the user. Communication Manager Release 7.1.2 and later support alphanumeric handles.
Domain	The name of the domain with which the handle is registered.

Button	Description
New	To add a new communication address.
Edit	To edit the information of a selected communication address.
Delete	To delete 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 handle. The options 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 13 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 calendar. • **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 that 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 using which the user can send or receive messages. You must provide a 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
Policy	When you enable the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page, the system displays the **Policy** field to select the required policy for the Session Manager communication profile. For more information, see *Administering Avaya Aura® Session Manager*. Based on the policy selection, the system displays the relevant fields. The options are: • **fixed**: When you select this option, the system displays the **Primary Session Manager**, **Secondary Session Manager**, **Third Session Manager**, and **Fourth Session Manager** fields. The default value is **fixed**. • **fixed-region**: When you select this option, the system displays the **Primary Region**, **Secondary Region**, **Third Region**, and **Fourth Region** fields. The system assigns the primary, secondary, third, or fourth region to the Session Manager Communication profile. • **location-region**: When you select this option, the system does not display the **Primary Session Manager** and **Secondary Session Manager** fields and dynamically assigns Session Managers based on the mapping of locations to regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Location to Region Mapping** page. **Note:** If the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page is not enabled, the system displays the **Primary Session Manager** and **Secondary Session Manager** fields similar to the Release 8.1.x and earlier system.
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.

Table continues…

Name	Description
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. This is an optional field. All the four Session Manager values must be unique. For example, if you select the same Session Manager server instance in the **Secondary Session Manager** field as the **Primary Session Manager** field, the system displays the following error message: `The Secondary Session Manager cannot be the same as the Primary Session Manager.`
Third Session Manager	The Session Manager instance that you select as the third Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary or the secondary Session Manager server becomes unavailable. This is an optional field. You must select the value of the Session Manager servers as per the order of display. For example, if you select the third Session Manager value before the secondary Session Manager, the system displays the following error message: `Selection of Session Managers should be as per their order of display. Select Secondary Session Manager before Third Session Manager.`
Fourth Session Manager	The Session Manager instance that you select as the fourth Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary, secondary, or third Session Manager server becomes unavailable. This is an optional field.
Primary Region	The Session Manager region that you select as the primary region. You must select the primary region of the Session Manager server. You can create the regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Session Manager Groups** page. You must select the value of regions as per the order of display. For example, if you select the secondary region value before the primary region, the system displays the following error message: `Selection of regions should be as per their order of display. Select Primary Region before Secondary Region.`

Table continues…

Name	Description
Secondary Region	The Session Manager region that you select as the secondary region. This is an optional field. **Note:** • If you select the same region for the primary and secondary regions, then there must be a minimum of two Session Managers in that region. • If you select 4 different regions, then there must be a minimum of 1 Session Manager in each region. If you select the same region and the region does not have sufficient Session Managers, the system displays the following error message: `<Secondary Region> - <Name_of_the_Region> the assigned regions must contain enough SMs to satisfy the Primary/Secondary/Third/Fourth region selection count.`
Third Region	The Session Manager region that you select as the third region. This is an optional field.
Fourth Region	The Session Manager region that you select as the fourth region. This is an optional field.
Survivability Server	For local survivability, you can specify a survivability server. The server provides survivability communication services to devices associated with a communication profile, when the local connectivity to Session Manager instances in Avaya core is lost. If you select 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. This survivable remote server is resident with the Branch Session Manager selected. 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. After typing a minimum of 3 characters, wait for three seconds to capture the final keyword and fetch the required results.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.

Table continues…

Name	Description
Block New Registration When Maximum Registrations Active	If you select the check box, the system denies any new registrations with Session Manager when an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit. 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 affect the call and keeps that device registered for that call only.
Origination Application Sequence	The application sequence the system invokes when routing 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 invoked when the system routes 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.
Emergency Calling Origination Sequence	The list of application sequences invoked when the system routes emergency calls from this user.
Emergency Calling Termination Sequence	The list of application sequences invoked when the system routes emergency calls to this user.
Home Location	The 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 the IP Address Pattern of any 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** page 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.
Enable Client	The drop-down list of the supported clients. Select the required client.

Communication Profile tab: Avaya Breeze® 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 Communication Manager 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 Communication Manager Endpoint profile that you create. You must select the profile type.
Use Existing Endpoints	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 with this profile. 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.
Set Type	The set type of the endpoint. 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. **Note:** You must clear Local Device Services Data on all Avaya Aura® Web Gateway nodes if you change the value of **Voice Mail Number**.

Table continues…

Name/Button	Description
Preferred Handle	Numeric only handles, SIP handles, or non-SIP handles, that are administered for a user. The **Preferred Handle** field is optional. Select numeric handle for alphanumeric support. By default, the field is blank. If the type of SIP entity is Communication Manager, Session Manager uses the preferred handle 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**.
SIP URI	A unique alphanumeric communication address of the user to make and receive voice or video calls. The **SIP URI** address can be: `<username-projectname>@<xyz.com>`.
Attendant	The option to enable the attendant feature on the endpoint. If you select this check box, you can administer the endpoint as an attendant. When you select the 9641SIP template type from **Template**, the system enables the **Attendant** check box.

Table continues…

Name/Button	Description
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 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 delete the user.
Override Endpoint Name and Localized 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

Name	Description
System	The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.

Table continues…

Name	Description
Target	The customer number of 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	The station profile information updated 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 in this field. 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. The value in the field is valid only if you select the **Use Existing Subscriber on System** check box.
Messaging Editor	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 | <User Name> 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.

Table continues…

Name	Description
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 delete the user.

Communication Profile tab: Avaya Messaging Profile

Name	Description
Officelinx System	The Avaya Messaging system to which you add a mailbox.
Refresh	The option to get information about company, departments, and feature groups from Avaya Messaging and save locally on System Manager for future use. You do not require to refresh for every user.
Mailbox Number	The mailbox number of the subscriber. It should be numeric only.
Numeric Password	The numeric password used to log in to the Avaya Messaging system.
Confirm Numeric Password	The numeric password you retype to confirm.
Application User Password	The password used to gain access to non-telephone applications, such as Web Client, iLink Pro, iLink Pro Mobile, and iLink Pro Desktop.
Confirm Application User Password	The password you retype to confirm.
Company	The name of the company to which the user belongs.
Department	The department to which the user belongs.
Feature Group	The feature group name that determines the rules for the mailboxes associated with it.
Capability	The type of functionality the user contains. The values are: • **Standard** • **Fax** • **Messaging** • **Collaboration** • **Messaging and Collaboration**
Domain Account Name	The mailbox NT account name of the Avaya Messaging profile.
Synchronization User Name	The account name used to gain access to the email server, for example, Microsoft Exchange and Google Gmail.

Note:

Only one-way update is supported for Officelinx elements. If you make any change directly on Officelinx, it does not reflect on System Manager. If you edit the user from System Manager, it overrides the changes you made directly on Officelinx.

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 not 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.
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 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.
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 | <User Name> 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: Equinox Conferencing

Name	Description
Equinox User Password	The Equinox user password.
Virtual Room Number	The virtual room number of the Equinox user.

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 Presence Services. This system selects the SIP entity 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 SIP Entity	The Presence Services instance for the user.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with 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: 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.

Table continues…

Button	Description
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 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 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 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 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

Note:

Adding a private contact to a user is a two-step process. First, you add the private contact and then you add the new private contact to the associated contacts. Ensure that you commit your updates after you add the private contact.

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 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 menu	You can find the **Filter menu** icon next to the name of each column. Filters the data based on the search criteria.

Contacts tab — Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

Note:

Adding a private contact to a user is a two-step process. First, you add the private contact and then you add the new private contact to the associated contacts. Ensure that you commit your updates after you add the private contact.

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 menu	You can find the **Filter menu** icon next to the name of each column. Filters the data based on the search 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 returns to the User Management or User Profile | View | <User Name> 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 returns to the User Management or User Profile | View | <User Name> page.

User Profile | View | <User Name> field descriptions

Organization

Name	Description
Tenant	The name of the tenant that you 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.

Table continues…

Name	Description
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.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the endpoints. For example, Miller. Typically, the name is in the written or spoken language of the user. **Last Name (Latin Translation)** can be up to 256 characters. **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 and first names change. • Filled, the values remain the same 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 endpoints. For example, John. Typically, the name is in the written or spoken language of the user. **First Name (Latin Translation)** can be up to 256 characters.
Middle Name	The middle name of the user, if any.
Description	A brief description of the user.
Status	The login status of the user.
Update Time	The time when the user details were last modified.

Table continues…

Name	Description
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 the login name in uppercase or lowercase. You cannot edit the **Login Name** field for users with the login name admin.
Email Address	The email address of the user.
Authentication Type	Authentication type defines how the system performs user authentication. The options are: • **Enterprise**: The enterprise authenticates the user login. • **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.

Table continues…

Name	Description
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 on the **Users** > **User Management** > **Communication Profile Password Policy** page. When you provide the communication password value during bulk edit of users, the system overwrites any existing communication profile passwords of the user. For information about password policy, see “Communication profile password policy”.

Table continues…

Name	Description
Generate	The option to automatically generate the communication profile password. System Manager sends the generated password to the user if you: • Set the email configuration properties on the **Services** > **Configurations** > **Settings** > **SMGR** page. For more information, see “Configuring email properties”. • Configure **Email Address** on the **Identity** tab. By default, the **Generate** link is available for creating a new user account. The **Edit** link is available for modifying user accounts. When you click the **Edit** link, the system displays **Confirm Password** along with the **Generate** and **Cancel** links.
Name	The name of the communication profile that you must select .

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 of adding 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

Note:

The system displays the following fields only if a communication profile of the user exists for the product:

Name	Description
Policy	When you enable the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page, the system displays the **Policy** field to select the required policy for the Session Manager communication profile. For more information, see *Administering Avaya Aura® Session Manager*. Based on the policy selection, the system displays the relevant fields. The options are: • **fixed**: When you select this option, the system displays the **Primary Session Manager**, **Secondary Session Manager**, **Third Session Manager**, and **Fourth Session Manager** fields. The default value is **fixed**. • **fixed-region**: When you select this option, the system displays the **Primary Region**, **Secondary Region**, **Third Region**, and **Fourth Region** fields. The system assigns the primary, secondary, third, or fourth region to the Session Manager Communication profile. • **location-region**: When you select this option, the system does not display the **Primary Session Manager** and **Secondary Session Manager** fields and dynamically assigns Session Managers based on the mapping of locations to regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Location to Region Mapping** page. **Note:** If the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page is not enabled, the system displays the **Primary Session Manager** and **Secondary Session Manager** fields similar to the Release 8.1.x and earlier system.
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.

Table continues…

Name	Description
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. This is an optional field. All the four Session Manager values must be unique. For example, if you select the same Session Manager server instance in the **Secondary Session Manager** field as the **Primary Session Manager** field, the system displays the following error message: `The Secondary Session Manager cannot be the same as the Primary Session Manager.`
Third Session Manager	The Session Manager instance that you select as the third Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary or the secondary Session Manager server becomes unavailable. This is an optional field. You must select the value of the Session Manager servers as per the order of display. For example, if you select the third Session Manager value before the secondary Session Manager, the system displays the following error message: `Selection of Session Managers should be as per their order of display. Select Secondary Session Manager before Third Session Manager.`
Fourth Session Manager	The Session Manager instance that you select as the fourth Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary, secondary, or third Session Manager server becomes unavailable. This is an optional field.
Primary Region	The Session Manager region that you select as the primary region. You must select the primary region of the Session Manager server. You can create the regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Session Manager Groups** page. You must select the value of regions as per the order of display. For example, if you select the secondary region value before the primary region, the system displays the following error message: `Selection of regions should be as per their order of display. Select Primary Region before Secondary Region.`

Table continues…

Name	Description
Secondary Region	The Session Manager region that you select as the secondary region. This is an optional field. **Note:** • If you select the same region for the primary and secondary regions, then there must be a minimum of two Session Managers in that region. • If you select 4 different regions, then there must be a minimum of 1 Session Manager in each region. If you select the same region and the region does not have sufficient Session Managers, the system displays the following error message: `<Secondary Region> - <Name_of_the_Region> the assigned regions must contain enough SMs to satisfy the Primary/Secondary/Third/Fourth region selection count.`
Third Region	The Session Manager region that you select as the third region. This is an optional field.
Fourth Region	The Session Manager region that you select as the fourth region. This is an optional field.
Survivability Server	For local survivability, you can specify a survivability server. The server provides survivability communication services to devices associated with a communication profile, when the local connectivity to Session Manager instances in Avaya core is lost. If you select 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. This survivable remote server is resident with the Branch Session Manager selected. 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. After typing a minimum of 3 characters, wait for three seconds to capture the final keyword and fetch the required results.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.

Table continues…

Name	Description
Block New Registration When Maximum Registrations Active	If you select the check box, the system denies any new registrations with Session Manager when an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit. 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 affect the call and keeps that device registered for that call only.
Origination Application Sequence	The application sequence the system invokes when routing 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 invoked when the system routes 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.
Emergency Calling Origination Sequence	The list of application sequences invoked when the system routes emergency calls from this user.
Emergency Calling Termination Sequence	The list of application sequences invoked when the system routes emergency calls to this user.
Home Location	The 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 the IP Address Pattern of any 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** page 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.
Enable Client	The drop-down list of the supported clients. Select the required client.

Communication Profile tab: Avaya Breeze® 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 Communication Manager 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 with this profile. 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. 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. **Note:** You must clear Local Device Services Data on all Avaya Aura® Web Gateway nodes if you change the value of **Voice Mail Number**.
Preferred Handle	Numeric only handles, SIP handles, or non-SIP handles, that are administered for a user. The **Preferred Handle** field is optional. Select numeric handle for alphanumeric support. By default, the field is blank. If SIP entity is of the Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
SIP URI	A unique alphanumeric communication address of the user to make and receive voice or video calls. The **SIP URI** address can be: `<username-projectname>@<xyz.com>`.
Attendant	The option to enable the attendant feature on the endpoint. If you select this check box, you can administer the endpoint as an attendant. When you select the 9641SIP template type from **Template**, the system enables the **Attendant** check box.

Table continues…

Name/Button	Description
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 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 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.

Table continues…

Name	Description
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.
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: Avaya Messaging Profile

Name	Description
Officelinx System	The Avaya Messaging system to which you add a mailbox.
Refresh	The option to get information about company, departments, and feature groups from Avaya Messaging and save locally on System Manager for future use. You do not require to refresh for every user.
Mailbox Number	The mailbox number of the subscriber. It should be numeric only.
Numeric Password	The numeric password used to log in to the Avaya Messaging system.
Confirm Numeric Password	The numeric password you retype to confirm.
Application User Password	The password used to gain access to non-telephone applications, such as Web Client, iLink Pro, iLink Pro Mobile, and iLink Pro Desktop.

Table continues…

Name	Description
Confirm Application User Password	The password you retype to confirm.
Company	The name of the company to which the user belongs.
Department	The department to which the user belongs.
Feature Group	The feature group name that determines the rules for the mailboxes associated with it.
Capability	The type of functionality the user contains. The values are: • **Standard** • **Fax** • **Messaging** • **Collaboration** • **Messaging and Collaboration**
Domain Account Name	The mailbox NT account name of the Avaya Messaging profile.
Synchronization User Name	The account name used to gain access to the email server, for example, Microsoft Exchange and Google Gmail.

Note:

Only one-way update is supported for Officelinx elements. If you make any change directly on Officelinx, it does not reflect on System Manager. If you edit the user from System Manager, it overrides the changes you made directly on Officelinx.

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 not 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.

Table continues…

Name/Button	Description
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 | <User Name> 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.
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: Equinox Conferencing

Name	Description
Equinox User Password	The Equinox user password.
Virtual Room Number	The virtual room number of the Equinox user.

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 Presence Services. This system selects the SIP entity 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.

Table continues…

Name	Description
IM Gateway SIP Entity	The Presence Services instance for the user.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with 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: 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 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 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

Note:

Adding a private contact to a user is a two-step process. First, you add the private contact and then you add the new private contact to the associated contacts. Ensure that you commit your updates after you add the private contact.

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 menu	You can find the **Filter menu** icon next to the name of each column. Filters the data based on the search criteria.

Contacts tab — Private Contacts section

Use this section to add new private contacts, modify and deletes existing contacts.

Note:

Adding a private contact to a user is a two-step process. First, you add the private contact and then you add the new private contact to the associated contacts. Ensure that you commit your updates after you add the private contact.

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 menu	You can find the **Filter menu** icon next to the name of each column. Filters the data based on the search criteria.

Common buttons

Button	Description
Edit	Displays the User Profile | Edit | <User Name> page. Use the User Profile | Edit | <User Name> page to modify the details of the user account.
Done	Closes the User Profile | Edit | <User Name> page and returns to the User Management page.

User Profile | Duplicate | <User Name> field descriptions

Organization

Name	Description
Tenant	The name of the tenant that you 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 endpoints. For example, Miller. Typically, the name is in the written or spoken language of the user. **Last Name (Latin Translation)** can be up to 256 characters. **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 and first names change. • Filled, the values remain the same 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 endpoints. For example, John. Typically, the name is in the written or spoken language of the user. **First Name (Latin Translation)** can be up to 256 characters.
Middle Name	The middle name of the user, if any.
Description	A brief description of 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 the login name in uppercase or lowercase. You cannot edit the **Login Name** field for users with the login name admin.
Email Address	The email address of the user for receiving email notifications. **Email Address** can be up to 256 characters.

Table continues…

Name	Description
User 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.
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.

Table continues…

Button	Description
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 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
Communication Profile Password	The communication profile password. The field is available only if you enable the communication profile. The password policy is configured on the **Users** > **User Management** > **Communication Profile Password Policy** page. When you provide the communication password value during bulk edit of users, the system overwrites any existing communication profile passwords of the user. For information about password policy, see “Communication profile password policy”.
Confirm Password	The communication profile password to reenter for confirmation.

Table continues…

Name	Description
Generate	The option to automatically generate the communication profile password. System Manager sends the generated password to the user if you: • Set the email configuration properties on the **Services** > **Configurations** > **Settings** > **SMGR** page. For more information, see “Configuring email properties”. • Configure **Email Address** on the **Identity** tab. By default, the **Generate** link is available for creating a new user account. The **Edit** link is available for modifying user accounts. When you click the **Edit** link, the system displays **Confirm Password** along with the **Generate** and **Cancel** links.
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 handle. The options 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 13 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 calendar. • **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 that 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 using which the user can send or receive messages. You must provide a 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
Policy	When you enable the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page, the system displays the **Policy** field to select the required policy for the Session Manager communication profile. For more information, see *Administering Avaya Aura® Session Manager*. Based on the policy selection, the system displays the relevant fields. The options are: • **fixed**: When you select this option, the system displays the **Primary Session Manager**, **Secondary Session Manager**, **Third Session Manager**, and **Fourth Session Manager** fields. The default value is **fixed**. • **fixed-region**: When you select this option, the system displays the **Primary Region**, **Secondary Region**, **Third Region**, and **Fourth Region** fields. The system assigns the primary, secondary, third, or fourth region to the Session Manager Communication profile. • **location-region**: When you select this option, the system does not display the **Primary Session Manager** and **Secondary Session Manager** fields and dynamically assigns Session Managers based on the mapping of locations to regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Location to Region Mapping** page. **Note:** If the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page is not enabled, the system displays the **Primary Session Manager** and **Secondary Session Manager** fields similar to the Release 8.1.x and earlier system.

Table continues…

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. It provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. This is an optional field. All the four Session Manager values must be unique. For example, if you select the same Session Manager server instance in the **Secondary Session Manager** field as the **Primary Session Manager** field, the system displays the following error message: `The Secondary Session Manager cannot be the same as the Primary Session Manager.`
Third Session Manager	The Session Manager instance that you select as the third Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary or the secondary Session Manager server becomes unavailable. This is an optional field. You must select the value of the Session Manager servers as per the order of display. For example, if you select the third Session Manager value before the secondary Session Manager, the system displays the following error message: `Selection of Session Managers should be as per their order of display. Select Secondary Session Manager before Third Session Manager.`
Fourth Session Manager	The Session Manager instance that you select as the fourth Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary, secondary, or third Session Manager server becomes unavailable. This is an optional field.

Table continues…

Name	Description
Primary Region	The Session Manager region that you select as the primary region. You must select the primary region of the Session Manager server. You can create the regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Session Manager Groups** page. You must select the value of regions as per the order of display. For example, if you select the secondary region value before the primary region, the system displays the following error message: `Selection of regions should be as per their order of display. Select Primary Region before Secondary Region.`
Secondary Region	The Session Manager region that you select as the secondary region. This is an optional field. **Note:** • If you select the same region for the primary and secondary regions, then there must be a minimum of two Session Managers in that region. • If you select 4 different regions, then there must be a minimum of 1 Session Manager in each region. If you select the same region and the region does not have sufficient Session Managers, the system displays the following error message: `<Secondary Region> - <Name_of_the_Region> the assigned regions must contain enough SMs to satisfy the Primary/Secondary/Third/Fourth region selection count.`
Third Region	The Session Manager region that you select as the third region. This is an optional field.
Fourth Region	The Session Manager region that you select as the fourth region. This is an optional field.

Table continues…

Name	Description
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. **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.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time by 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, the system denies any new registrations with Session Manager when an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit. 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 affect the call and keeps that device registered for that call only.
Origination Application Sequence	The application sequence the system invokes when routing 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 invoked when the system routes 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.
Emergency Calling Origination Sequence	The list of application sequences invoked when the system routes emergency calls from this user.

Table continues…

Name	Description
Emergency Calling Termination Sequence	The list of application sequences invoked when the system routes emergency calls to this user.
Home Location	The 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 the IP Address Pattern of any 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** page 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: Avaya Breeze® 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 Communication Manager 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	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 with this profile. 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.
Set Type	The set type of the endpoint. 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.

Table continues…

Name/Button	Description
Voice Mail Number	The voice mail number of the endpoint. **Note:** You must clear Local Device Services Data on all Avaya Aura® Web Gateway nodes if you change the value of **Voice Mail Number**.
Preferred Handle	Numeric only handles, SIP handles, or non-SIP handles, that are administered for a user. The **Preferred Handle** field is optional. Select numeric handle for alphanumeric support. By default, the field is blank. If SIP entity is of Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
SIP URI	A unique alphanumeric communication address of the user to make and receive voice or video calls. The **SIP URI** address can be: `<username-projectname>@<xyz.com>`.
Calculate Route Pattern	The option to automatically select the route pattern based on the primary or secondary Session Manager configured 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.
Attendant	The option to enable the attendant feature on the endpoint. If you select this check box, you can administer the endpoint as an attendant. When you select the 9641SIP template type from **Template**, the system enables the **Attendant** check box.
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 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. • 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.

Table continues…

Name/Button	Description
Allow H.323 and SIP Endpoint Dual Registration	The option to register an H.323 endpoint and a SIP endpoint together at the same time to the same extension. For more information about the SIP and H.323 dual registration feature, see *Avaya Aura® Communication Manager Feature Description and Implementation* on the Avaya Support website at http://support.avaya.com.

Communication Profile tab - CS1000 Endpoint Profile

Name	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.
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: Avaya Messaging Profile

Name	Description
Officelinx System	The Avaya Messaging system to which you add a mailbox.
Refresh	The option to get information about company, departments, and feature groups from Avaya Messaging and save locally on System Manager for future use. You do not require to refresh for every user.
Mailbox Number	The mailbox number of the subscriber. It should be numeric only.
Numeric Password	The numeric password used to log in to the Avaya Messaging system.
Confirm Numeric Password	The numeric password you retype to confirm.
Application User Password	The password used to gain access to non-telephone applications, such as Web Client, iLink Pro, iLink Pro Mobile, and iLink Pro Desktop.
Confirm Application User Password	The password you retype to confirm.
Company	The name of the company to which the user belongs.
Department	The department to which the user belongs.
Feature Group	The feature group name that determines the rules for the mailboxes associated with it.
Capability	The type of functionality the user contains. The values are: • **Standard** • **Fax** • **Messaging** • **Collaboration** • **Messaging and Collaboration**
Domain Account Name	The mailbox NT account name of the Avaya Messaging profile.
Synchronization User Name	The account name used to gain access to the email server, for example, Microsoft Exchange and Google Gmail.

Note:

Only one-way update is supported for Officelinx elements. If you make any change directly on Officelinx, it does not reflect on System Manager. If you edit the user from System Manager, it overrides the changes you made directly on Officelinx.

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 not 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 | <User Name> 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: Equinox Conferencing

Name	Description
Equinox User Password	The Equinox user password.
Virtual Room Number	The virtual room number of the Equinox user.

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 Presence Services. This system selects the SIP entity 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 SIP Entity	The Presence Services instance for the user.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with 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: 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.

Table continues…

Button	Description
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 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 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	Displays 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	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
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

Note:

Adding a private contact to a user is a two-step process. First, you add the private contact and then you add the new private contact to the associated contacts. Ensure that you commit your updates after you add the private contact.

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	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.
Remove	Removes one or more contacts from the list of the associated contacts.
Filter menu	You can find the **Filter menu** icon next to the name of each column. Filters the data based on the search criteria.

Contacts tab — Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

Note:

Adding a private contact to a user is a two-step process. First, you add the private contact and then you add the new private contact to the associated contacts. Ensure that you commit your updates after you add the private contact.

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	Displays the Edit Private Contact page. Use this page to modify the information of the selected contact.
New	Displays the New Private Contact page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter menu	You can find the **Filter menu** icon next to the name of each column. Filters the data based on the search criteria.

Common buttons

Button	Description
Commit & Continue	Duplicates the user account and retains you on the same page for further modifications.
Commit	Duplicates the user account and takes you to the User Management page.
Cancel	Cancels the operation of modifying the user information and returns 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.
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.
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.
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 import and export user profiles and global settings in bulk. To import data in bulk, you must provide an XML file or an Excel file as input file. System Manager validates any file that you upload during the bulk import operation.

System Manager filters uploaded files based on the file extension and mime type or bytes in the 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, IP Office, Presence, Avaya Breeze® platform, Work Assignment, Avaya Messaging, and Avaya Meetings Server.

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.

Importing and exporting 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 the default.

- Handle. The communication address of the user
- Session Manager profile
- Avaya Breeze® platform profile
- CM Endpoint profile with all attributes of the station communication profile
- CM Agent profile with all attributes.
- Messaging profile
- Avaya Messaging profile
- IP Office Endpoint profile
- CS 1000 Endpoint profile
- Presence profile
- Work Assignment profile
- Avaya Meetings Server profile

- Supports more than one communication profile set.
- Supports the creation, updation, and deletion of the user by using the same Excel file. However, you can only 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 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 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 379
Microsoft Excel data link error on page 373
Examples of bulk import and export of user by using the Excel file on page 370
Hierarchy in communication profile worksheets on page 372

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#secondaryProfile	Session Manager	sm6						Pune	6	false	true

If a Avaya Breeze® 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.

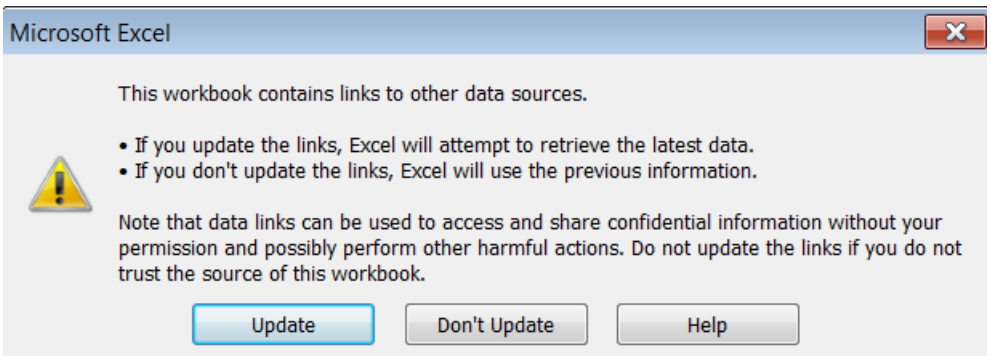
Element	Master worksheet	Child worksheets
Session Manager	Session Manager Profile	None
Communication Manager — Endpoint	CM Endpoint Profile	• Station Site Data • Buttons • Feature Buttons • Expansion Module Buttons • Soft Keys • Display Buttons • Station Abbr Dialing Data • Station Data Module • Station Hot Line Data • Native Name Data
Communication Manager — Agent	CM Agent Profile	• CM Agent LoginId Skills Data • CM Agent Native Name Data

Table continues…

Element	Master worksheet	Child worksheets
Messaging	Messaging Profile	• Messaging MMSpecific • Messaging CMMSpecific • Messaging AAMSpecific
IP Office	IP Office Endpoint Profile	None
CS 1000	CS 1000 Endpoint Profile	None
Avaya Breeze® platform	CE Profile	None
Presence	Presence Profile	None
Work Assignment	Work Assignment Profile	• Work Assignment Resource Details • Work Assignment Agent Attributes
Avaya Messaging	Avaya Messaging Profile	None
Equinox	Equinox Profile	None

Microsoft Excel data link error

Microsoft Excel 2010 displays a data link error.



Related links

Proposed solution on page 373

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 373

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 374

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 404. See Sample XML for bulk import of users with all attributes on page 411 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, 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 404. 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 411 and Sample XML for bulk import of users with all attributes on page 411.

- XML schema definition for partial import of users: See XML Schema Definition for partial import of user attributes on page 419. 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 421.

To delete bulk users, a separate XML schema definition is defined. See XML Schema Definition for bulk deletion of users on page 423. For a sample XML that conforms to delete bulk users XML schema definition, see Sample XML for bulk deletion of users on page 424.

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.

Bulk importing of users

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. On the Import users page, in the **Select File** field, type the complete path of the file or click **Browse** to locate and select a file.
5. Select one of the following error configuration options:
   - **Abort on first error**
   - **Continue processing other records**
6. For the XML file type, click **Complete** in the import type.

   If you select the Excel file type, the system does not display the import type option.

7. 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.

8. 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.

9. Click **Import**.

   If you use the default configurations option **Importing Users** > **Add Users** in the database, the system imports the next user record even if the import user operation encounters an error while importing a user record. The system logs an error. Skip import of users that already exist in the database. The system schedules the import job to run immediately.

   Note:

   The operations, Communication Manager synchronization and bulk import of users, must not overlap in time. When bulk import of users is in progress and if Communication Manager synchronization starts, the records that are in process fail. When synchronization is complete, the remaining bulk import records process successfully. You must reimport the records that fail to import during synchronization.

Related links

Attribute details defined in Import user XSD on page 521
Attribute details defined in Delete User XSD on page 532
Attribute details defined in the CM Endpoint profile XSD on page 533
Attribute details defined in the Messaging communication profile XSD on page 563
Attribute details defined in the Session Manager communication profile XSD on page 572
Downloading the Excel template file on page 379
Microsoft Excel data link error on page 373

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 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.

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, IP Office, Presence, Avaya Breeze® platform, Work Assignment, Avaya Messaging, and Avaya Meetings Server.

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 404.

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 any administrative role. For security reasons, the system does not export the **Password** fields to the XML file. Therefore, import of users with any administrative role fails, if the password is not provided.

To import users with any administrative role, in the XML file for the users, add the following XML tag after the `<username>` tag:

```
<userPassword> provide password for user </userPassword>
```

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.

Bulk export users directory

The bulk export users zip files are stored in the `/var/avaya/bulkadministration/export/` directory. The total file size of exported zip files is monitored as per the value of the **max_bulk_export_files_directory_size_allowed** property in the `$MGMT_HOME/bulkadministration/exportutility/config/bulkexportconfig.properties` directory. The default file size for bulk export user is 1-GB. You can change the file size value for bulk export user to maximum 2-GB.

The system runs the check for the total size of the files in the `/var/avaya/bulkadministration/export/` directory on a daily basis. If the file size is greater than **max_bulk_export_files_directory_size_allowed**, the system automatically deletes the oldest files to make the size less than or equal to **max_bulk_export_files_directory_size_allowed**.

Note:

If there is only one file in `/var/avaya/bulkadministration/export/`, the system does not deletes the file.

Exporting users in bulk from web console

About this task

With bulk export you can export the delta of users for a specified period of time. Delta users are the added, updated, or deleted users for the specified period of time. This feature is useful for performing bulk export of the entire System Manager user database that can be used with the external applications. This feature enables you to export only the users that have changed during the defined interval.

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.
- Increasing number of users per file in bulk export configuration beyond verified default limit consumes system resources. It results in degrading system performance and can cause system crash.

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.

- **More Actions** > **Export Delta Users** to export the delta of users for a specified period of time.

The system displays the Export Users page.

3. In the Export File Type Options section, in **Select Export File Types**, click **Xml**, **Excel** or both.

   Note:

   Select at least one option. If you do not select a file type, and click **Export**, the export operation does not start. The page displays the message `Export File Type/Types Not Selected. Select Export File Types Xml or Excel or Both`.

   If you select only **Excel**, the system automatically clears the **Contacts** check box in **User Attribute Options** because excel file does not support importing and exporting user contacts. The page also displays a message `Excel file does not support contacts` beside the **Contacts** check box.

4. **(Optional)** 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”.

5. In the Delta Period Options section, from **Select the delta period**, select the delta period to generate the file for the delta of users.

   The Delta Period Options section is available only if you select the **Export Delta Users** option.

   For more information, see “Export Users field descriptions”.

   For example, if you select the delta period as **One Week**, schedule the job with the **Run immediately** option, and export file type as both XML and Excel, then the exported zip file contains the following:

   - An `XML` file with added or updated users in last one week.
   - An `Excel` file with added or updated users in last one week.
   - A deleted users `.txt` file only if there are any permanently deleted users in the specified delta period.

6. 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.

7. Click **Export** to complete the export operation.

   The system exports the user data to the XML and Excel file.

8. 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 page, clear the **Contacts** check box 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

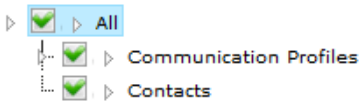
Bulk export of users on page 380
List of XML Schema Definitions and sample XMLs for bulk import on page 403
exportUpmGlobalsettings.sh command on page 399
Attribute details defined in Import user XSD on page 521
Attribute details defined in Delete User XSD on page 532
Attribute details defined in the CM Endpoint profile XSD on page 533
Attribute details defined in the Messaging communication profile XSD on page 563
Attribute details defined in the Session Manager communication profile XSD on page 572
Export Users field descriptions on page 384
Downloading the Excel template file on page 379
Microsoft Excel data link error on page 373
Bulk importing of users on page 377

Export Users field descriptions

Export File Type Options

Name	Description
Select Export File Types	The file type to which you want to export the users. The options are: • **Xml** • **Excel** • **Both**. You can select **Xml** and **Excel**. **Note:** Select at least one option. If you do not select a file type, and click **Export**, the export operation does not start. The page displays the message `Export File Type/Types Not Selected. Select Export File Types Xml or Excel or Both`. If you select only **Excel**, the system automatically clears the **Contacts** check box in **User Attribute Options** because excel file does not support importing and exporting user contacts. The page also displays a message `Excel file does not support contacts` beside the **Contacts** check box.

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. • **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.

Delta Period options

The Delta Period Options section is available only if you select the **Export Delta Users** option.

Name	Description
Select the delta period	Following are the delta period options: • **One Day**: is exact past one day from current system date and time for run immediately or exact past one day from scheduled job time. • **One Week**: is exact past one week from current system date and time for run immediately or exact past one week from scheduled job time. • **One Month**: is exact past one month from current system date and time for run immediately or exact past one month from scheduled job time. **Note:** The system creates the `XML` and `Excel` file even if there are no added or updated users in the specified delta period. If there are no added or updated users in the specified delta period then the `XML` and `Excel` files contain zero users data. However, the system creates the `.txt` file only if there are any permanently deleted users in the specified delta period.

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. **Note:** If you select the **Export All Users** or **Export Delta Users** option, and select the **Schedule Job** as **Schedule later**, the system displays the **Recurrence** and **Range** fields.
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.

Table continues…

Name	Description
Recurrence	Following are the options: • **Execute task one time only**: The job is executed only once at the specified scheduled start time. • **Tasks are repeated**: The options are **Daily**, **Weekly**, and **Monthly**. The job is repeated as per the selection. **Note:** If you select the **Tasks are repeated**, the system enables the **Range** field. **Note:** The delta period selected for the **Export Delta Users** option for scheduled or recurring jobs will consider the exact delta period past to the exact start date and time of execution of the scheduled jobs. For example, if a delta export job is scheduled to run on December 17, 2017 at 2:00 p.m. with the delta period of **One Day**, then the delta of users is identified from December 16, 2017 from 2.00 p.m. For recurrence jobs, if a job is configured to run multiple times then the last exported zip file with the name `<Scheduled Job Name>.zip` will be available on the Export Users page for download. However, the previously exported zip files will be stored in the `/var/avaya/bulkadministration/export/` directory with the name `<Scheduled Job_Date_time_In_UTC>.zip`. Where *Date_time_In_UTC* is the date and time in UTC when the file was last-updated or created in the last run of the job. For example, if the admin started a recurring job at 18 Dec 2017 14:32:26 UTC to run for say 3 recurrences daily then after the completion of all 3 recurrences there will be 3 files available in the `/var/avaya/bulkadministration/export/` directory with following names: `users_1503066729239_18-Dec-2017_14:32:37_UTC.zip`, `users_1503066729239_19-Dec-2017_14:32:32_UTC.zip`, and `users_1503066729239.zip`.
Range	Following are the options: • **No End Date**: The job has no end date and executed as per the selection in the **Tasks are repeated** field. • **End After Occurrences**: The job is executed as per the selection in the **Tasks are repeated** field for the number of occurrences specified in **End After Occurrences**. • **End By Date**: The job is executed and the recurrence ends when the end date is reached.

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.

Configuring the maximum file size for automatically removing the exported zip files from the bulk export users directory

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.

2. From the `$MGMT_HOME/bulkadministration/exportutility/config` location, open the `bulkexportconfig.properties` file.
3. In the `bulkexportconfig.properties` file, change the value of **max_bulk_export_files_directory_size_allowed**.

   Do not enter the decimal value for the file size. The default file size for bulk export user is 1-GB. You can change the file size value for bulk export user to maximum 2-GB.

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 419. For a sample XML file for import of user, see Sample XML for partial import of users on page 421.

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 375
List of XML Schema Definitions and sample XMLs for bulk import on page 403

Attribute details defined in Import user XSD on page 521
Attribute details defined in Delete User XSD on page 532
Attribute details defined in the CM Endpoint profile XSD on page 533
Attribute details defined in the Messaging communication profile XSD on page 563
Attribute details defined in the Session Manager communication profile XSD on page 572
Configuration options for bulk import of users on page 389

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 404. Partial import type uses a different XML schema definition, for more information, see XML Schema Definition for partial import of user attributes on page 419.

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.

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 any administrative role. For security reasons, the system does not export the **Password** fields to the XML file. Therefore, import of users with any administrative role fails, if the password is not provided.

  To import users with any administrative role, in the XML file for the users, add the following XML tag after the <username> tag:

  ```
  <userPassword> provide password for user </userPassword>
  ```

  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 has 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:
   a. 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.

   b. In the **Date** field, type the date.

      You can use the calendar icon to select a date.

c. In the **Time** field, type the time in the HH:MM:SS format.

d. 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 509. For sample XML file for import global settings, see Sample XML for bulk import of global setting records on page 516.

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 509.

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 519. For a sample XML conforming to delete bulk global settings XML schema definition, see Sample XML for bulk deletion of users on page 424.

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 375
List of XML Schema Definitions and sample XMLs for bulk import on page 403
Bulk import of global user settings on page 397

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 509.

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.

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

Scheduling a global user settings import job

About this task

System Manager supports scheduling of bulk import jobs from the System Manager web 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. In the **Date** field, type the date.

   You can use the calendar icon to select a date.

c. In the **Time** field, type time in the HH:MM:SS format.

d. In 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 section contains the XML Schema Definition and sample XML snippets for bulk import of users, global setting records, elements, endpoint profiles, Messaging profiles, CS 1000 profiles, IP Office profiles, agent profiles, Session Manager profiles, Presence profiles, Avaya Breeze® platform, Work Assignment, Avaya Messaging, and Avaya Meetings Server profiles.

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 <
- Ampersand character (&) as &
- Greater-than character (>) as >
- Double-quote character (") as "
- Apostrophe or single-quote character (') as '

If you copy the XML schema from the document, take care of the line breaks.

If you are using the Import User operation and you want to edit buttons on the Communication Manager endpoint, ensure that the XML file for the buttons matches the configuration on the endpoint.

For example, for the J179 settype, the following are supported:

- buttons tag: 8 main buttons
- featureButtons tag: 16 feature buttons
- expansionModuleButtons tag: 72 expansion module buttons (3 button modules and 24 buttons on each button module)

In this J179 scenario, you should only configure the following number of buttons for each button type:

- <number> value for <buttons> tag can have a value between 1 to 8
- <number> value for <featureButtons> tag can have a value between 1 to 16
- <number> value for <expansionModuleButtons> tag can have a value between 1 to 72

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="0" />

      <!--  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>
                <!--
              Flag to enable/disable the offline Call Logging feature for the SIP users
                     -->
          <xsd:element name="enabledisablecalllog" minOccurs="0">
                <xsd:simpleType>
                      <xsd:restriction base="xsd:boolean" />
                  </xsd:simpleType>
          </xsd:element>

          <!-- Name of the Emergency Termination Application Sequence (optional)
               - administered under
                  Session Manager / Application Configuration / Emergency Application
Sequences -->
          <xsd:element name="emergencyTerminationAppSequence" type="xsd:string"
minOccurs="0" />

          <!-- Name of the Emergency Origination Application Sequence (optional)
               - administered under
                 Session Manager / Application Configuration / Emergency Application
Sequences -->
          <xsd:element name="emergencyOriginationAppSequence" type="xsd:string"
minOccurs="0" />

            <!-- Policy Type (required only when policy based SM assignment global
settings is enabled) -->
      <xsd:element name="policyType" type="xsd:string" default="fixed" minOccurs="0" />

       <!-- Name of the third Session Manager -->
      <xsd:element name="thirdSM" type="xsd:string" minOccurs="0" />

       <!-- Name of the fourth Session Manager -->
      <xsd:element name="fourthSM" type="xsd:string" minOccurs="0" />

        <!-- Name of the primary fixed-region (mandatory only in case of fixed-region
policy type minimum occurance is kept zero but is validated in AsmComProfDataRules, as
this field is not applicable in case of fixed policy type ) -->
      <xsd:element name="primaryFixedRegion" type="xsd:string" minOccurs="0" />

        <!-- Name of the secondary fixed-region (applicable only in case of fixed-
region policy type, optional) -->
      <xsd:element name="secondaryFixedRegion" type="xsd:string" minOccurs="0" />

      <!-- Name of the third fixed-region (applicable only in case of fixed-region
policy type, optional) -->
      <xsd:element name="thirdFixedRegion" type="xsd:string" minOccurs="0" />

       <!-- Name of the fourth fixed-region (applicable only in case of fixed-region
policy type, optional) -->
      <xsd:element name="fourthFixedRegion" type="xsd:string" minOccurs="0" />
      <xsd:element name="thirdPartyClient" type="xsd:string" minOccurs="0" />
    </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 LLC 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>
<!-- Profile Settings for 96X1SIP & 96X1SIPCC Phones only -->
<xs:complexType name="xmlProfileSettings">
    <xs:sequence>
        <!-- Call Settings Options -->
```

```
        <!-- Phone Screen on Calling -->
        <xs:element name="phoneScreenCalling" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="No"/>
                    <xs:enumeration value="Yes"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Redial -->
        <xs:element name="profileRedial" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="List"/>
                    <xs:enumeration value="One Number"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Dialing Option -->
        <xs:element name="dialingOption" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Editable"/>
                    <xs:enumeration value="On-hook"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Headset Signaling -->
        <xs:element name="headsetSignaling" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Disabled"/>
                    <xs:enumeration value="Switchhook and Alerts"/>
                    <xs:enumeration value="Switchhook only"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Audio Path -->
        <xs:element name="audioPath" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Speaker"/>
                    <xs:enumeration value="Headset"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Screen & Sound Options Section -->
        <!-- Button Clicks -->
        <xs:element name="buttonClicks" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="On"/>
                    <xs:enumeration value="Off"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Phone Screen -->
        <xs:element name="phoneScreen" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
```

```
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Half"/>
                    <xs:enumeration value="Full"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Background Logo -->
        <xs:element name="backgroundLogo" type="xs:string" maxOccurs="1"
minOccurs="0" />

        <!-- Personalized Ringing -->
        <xs:element name="personalizedRinging" type="xs:string" maxOccurs="1"
minOccurs="0" />

        <!-- Call Pickup Indication -->
        <xs:element name="callPickUpIndication" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="None"/>
                    <xs:enumeration value="Audible"/>
                    <xs:enumeration value="Visual"/>
                    <xs:enumeration value="Both"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Show Quick Touch Panel -->
        <xs:element name="touchPanel" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="0"/>
                    <xs:enumeration value="1"/>
                    <xs:enumeration value="2"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>


        <!-- Language & Region Section -->
        <!-- User Preferred Language -->
        <xs:element name="userPreferredLanguage" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="English"/>
                    <xs:enumeration value="Hebrew"/>
                    <xs:enumeration value="Brazilian Portuguese"/>
                    <xs:enumeration value="Canadian French"/>
                    <xs:enumeration value="German"/>
                    <xs:enumeration value="Parisian French"/>
                    <xs:enumeration value="Latin American Spanish"/>
                    <xs:enumeration value="Castilian Spanish"/>
                    <xs:enumeration value="Italian"/>
                    <xs:enumeration value="Dutch"/>
                    <xs:enumeration value="Russian"/>
                    <xs:enumeration value="Traditional Chinese"/>
                    <xs:enumeration value="Japanese"/>
                    <xs:enumeration value="Korean"/>
                    <xs:enumeration value="Arabic"/>
                    <xs:enumeration value="Polish"/>
                    <xs:enumeration value="Turkish"/>
                    <xs:enumeration value="Thai"/>
                    <xs:enumeration value="Chinese"/>
                  </xs:restriction>
            </xs:simpleType>
```

```
        </xs:element>

        <!-- Time Format -->
        <xs:element name="timeFormat" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="12 Hour"/>
                    <xs:enumeration value="24 Hour"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Advanced Options - Presence Integration Section -->
        <!-- Away Timer -->
        <xs:element name="awayTimer" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="On"/>
                    <xs:enumeration value="Off"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Away Timer Value -->
        <xs:element name="awayTimerValue" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:int">
                    <xs:minInclusive value="5" />
                    <xs:maxInclusive value="999" />
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:sequence>
</xs:complexType>

<!--  GroupMembershipData to be set -->
<xs:complexType name="xmlStationGroupMememberShipData">
    <xs:sequence>
        <xs:element name="groupMemData" type="csm:xmlGroupMemData"
maxOccurs="unbounded" minOccurs="0" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlGroupMemData">
    <xs:sequence>
        <xs:element name="groupType" type="xs:string" maxOccurs="1"
minOccurs="1" />
        <xs:element name="groupnumber" type="xs:string" maxOccurs="1" minOccurs="1" />
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlStationdonotSharePortwithUnnamedRegistrationData">
    <xs:sequence>
       <xs:element name="donotSharePortwithUnnamedRegistration" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
    </xs:sequence>
</xs:complexType>
</xs:schema>
```

Sample XML for bulk import of 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 Definition for bulk import of Avaya Breeze® 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 Avaya Breeze® platform endpoint 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 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>
```

Sample XML for bulk import of Work Assignment profiles

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:ns2="http://xml.avaya.com/schema/import_ce"
xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ns4="http://xml.avaya.com/schema/
import_mem_officelinx" xmlns:ns5="http://xml.avaya.com/schema/import1"
xmlns:ns6="http://xml.avaya.com/schema/import_csm_mm" xmlns:ns7="http://
xml.avaya.com/schema/import_workassignment" xmlns:ns8="http://xml.avaya.com/schema/
import_sessionmanager" xmlns:ns9="http://xml.avaya.com/schema/presence"
xmlns:ns10="http://xml.avaya.com/schema/import_csm_cm" xmlns:ns11="http://xml.avaya.com/
schema/import_mmcs" xmlns:ns12="http://xml.avaya.com/schema/import_csm_b5800"
xmlns:ns13="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>
        <UserProvisionRules>
            <UserProvisionRuleName>My UPR Equi</UserProvisionRuleName>
        </UserProvisionRules>
        <authenticationType>basic</authenticationType>
        <description></description>
        <displayName>bbb, aaa</displayName>
        <displayNameAscii>bbb, aaa</displayNameAscii>
        <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>aaa</givenName>
        <givenNameAscii>aaa</givenNameAscii>
        <honorific></honorific>
        <loginName>aaa@avaya.com</loginName>
        <employeeNo></employeeNo>
        <department></department>
        <organization></organization>
        <middleName></middleName>
        <preferredLanguage>it_IT</preferredLanguage>
        <source>local</source>
        <status>provisioned</status>
        <surname>bbb</surname>
        <surnameAscii>bbb</surnameAscii>
        <timeZone>(-12:0)International Date Line West</timeZone>
        <userName>aaa</userName>
        <userPassword></userPassword>
        <commPassword></commPassword>
        <roles>
            <role>End-User</role>
        </roles>
        <ownedContactLists>
            <contactList>
                <name>list-aaa_avaya.com</name>
                <isPublic>false</isPublic>
                <contactListType>general</contactListType>
            </contactList>
        </ownedContactLists>
        <commProfileSet>
            <commProfileSetName>Primary</commProfileSetName>
            <isPrimary>true</isPrimary>
            <handleList>
                <handle>
                    <handleName>aaa@avaya.com</handleName>
                    <handleType>uca</handleType>
                </handle>
            </handleList>
            <commProfileList>
                <commProfile xsi:type="ns7:WorkAssignmentCommProfXML" xmlns:ns7="http://
xml.avaya.com/schema/import_workassignment">
                    <commProfileType>UCA</commProfileType>
                    <ns7:strategyName>Skill Level</ns7:strategyName>
                    <ns7:workAssignmentResourceDetails>
                        <ns7:associatedHandleName>aaa@avaya.com</
ns7:associatedHandleName>
                        <ns7:accountName>aaa</ns7:accountName>
                        <ns7:accountAddress>aaa@avaya.com</ns7:accountAddress>
                        <ns7:sourceName>avaya.com</ns7:sourceName>
                        <ns7:sourceAddress></ns7:sourceAddress>
                        <ns7:channelAttribute>Voice</ns7:channelAttribute>
                    </ns7:workAssignmentResourceDetails>
                </commProfile>
            </commProfileList>
        </commProfileSet>
```

```
    </tns:user>
</tns:users>
```

XML Schema Definition for bulk import of Avaya Messaging profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:smgr="http://xml.avaya.com/schema/import" elementFormDefault="qualified"
    targetNamespace="http://xml.avaya.com/schema/import_mem_officelinx">

    <xs:import namespace="http://xml.avaya.com/schema/import"
        schemaLocation="userimport.xsd" />

    <xs:complexType name="xmlOfficelinxProfile">
        <xs:complexContent>
            <xs:extension base="smgr:xmlCommProfileType">
                <xs:sequence>
                    <xs:element type="xs:string" name="officelinxName" maxOccurs="1" />
                    <xs:element type="xs:long" name="mailBoxNumber" maxOccurs="1" />
                    <xs:element type="xs:string" name="numericPassword" maxOccurs="1"
minOccurs="0" />
                    <xs:element type="xs:string" name="applicationUserPassword"
maxOccurs="1" minOccurs="0" />
                    <xs:element type="xs:string" name="company" maxOccurs="1"
minOccurs="0" />
                    <xs:element type="xs:string" name="department" maxOccurs="1"
minOccurs="0" />
                    <xs:element type="xs:string" name="featureGroup" maxOccurs="1"
minOccurs="0" />
                    <xs:element type="xs:string" name="capability" maxOccurs="1"
minOccurs="0" />
                    <xs:element type="xs:string" name="domainAccountName" maxOccurs="1"
minOccurs="0" />
                    <xs:element type="xs:string" name="synchronizationUserName"
maxOccurs="1" minOccurs="0" />
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>

</xs:schema>
```

Sample XML for bulk import of Avaya Messaging profiles

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:ns2="http://xml.avaya.com/schema/import_ce"
xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ns4="http://xml.avaya.com/schema/
import_mem_officelinx" xmlns:ns5="http://xml.avaya.com/schema/import1"
xmlns:ns6="http://xml.avaya.com/schema/import_csm_mm" xmlns:ns7="http://
xml.avaya.com/schema/import_workassignment" xmlns:ns8="http://xml.avaya.com/schema/
import_sessionmanager" xmlns:ns9="http://xml.avaya.com/schema/presence"
xmlns:ns10="http://xml.avaya.com/schema/import_csm_cm" xmlns:ns11="http://xml.avaya.com/
schema/import_mmcs" xmlns:ns12="http://xml.avaya.com/schema/import_csm_agent"
xmlns:ns13="http://xml.avaya.com/schema/import_csm_b5800" xmlns:ns14="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>pp7, pp7</displayName>
        <displayNameAscii>pp7, pp7</displayNameAscii>
        <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>pp7</givenName>
        <givenNameAscii>pp7</givenNameAscii>
```

```
        <honorific></honorific>
        <loginName>pp7@avaya.com</loginName>
        <employeeNo></employeeNo>
        <department></department>
        <organization></organization>
        <middleName></middleName>
        <preferredLanguage>sv</preferredLanguage>
        <source>local</source>
        <status>provisioned</status>
        <surname>pp7</surname>
        <surnameAscii>pp7</surnameAscii>
        <userName>pp7</userName>
        <userPassword></userPassword>
        <commPassword></commPassword>
        <roles>
            <role>End-User</role>
        </roles>
        <ownedContactLists>
            <contactList>
                <name>list-pp7_avaya.com</name>
                <isPublic>false</isPublic>
                <contactListType>general</contactListType>
            </contactList>
        </ownedContactLists>
        <commProfileSet>
            <commProfileSetName>Primary</commProfileSetName>
            <isPrimary>true</isPrimary>
            <commProfileList>
                <commProfile xsi:type="ns4:xmlOfficelinxProfile" xmlns:ns4="http://
xml.avaya.com/schema/import_mem_officelinx">
                    <commProfileType>officelinx</commProfileType>
                    <ns4:officelinxName>Officelinx-Pune</ns4:officelinxName>
                    <ns4:mailBoxNumber>198</ns4:mailBoxNumber>
                    <ns4:numericPassword/>
                    <ns4:applicationUserPassword/>
                    <ns4:company>1</ns4:company>
                    <ns4:department>14</ns4:department>
                    <ns4:featureGroup>1</ns4:featureGroup>
                    <ns4:capability>1</ns4:capability>
                    <ns4:domainAccountName>pp7@avaya.com</ns4:domainAccountName>
                    <ns4:synchronizationUserName>pp7@avaya.com</
ns4:synchronizationUserName>
                </commProfile>
            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema Definition for bulk import of Equinox 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/
import_scopia" elementFormDefault="qualified" xmlns:abc="http://xml.avaya.com/schema/
import_scopia">
<xsd:import namespace="http://xml.avaya.com/schema/import"
            schemaLocation="userimport.xsd"/>
<xsd:complexType name="ScopiaCommProfileType">
    <xsd:complexContent>
        <xsd:extension base="one:xmlCommProfileType" >
            <xsd:sequence>
                <xsd:element name="scopiaUserId" type="xsd:string" minOccurs="0"/>
                <xsd:element name="password" type="xsd:string"/>
                <xsd:element name="vrNumber" type="xsd:string" minOccurs="0"/>
                <xsd:element name="needVR" type="xsd:boolean" minOccurs="0"/>
```

```
                <xsd:element name="virtualRoomId" type="xsd:string" minOccurs="0"/>
            </xsd:sequence>
        </xsd:extension>
    </xsd:complexContent>
 </xsd:complexType>
</xsd:schema>
```

Sample XML for bulk import of Equinox profiles

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:ns2="http://xml.avaya.com/schema/import_ce"
xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ns4="http://xml.avaya.com/schema/
import_mem_officelinx" xmlns:ns5="http://xml.avaya.com/schema/import1"
xmlns:ns15="http://xml.avaya.com/schema/import_scopia" xmlns:ns6="http://xml.avaya.com/
schema/import_csm_mm" xmlns:ns7="http://xml.avaya.com/schema/import_workassignment"
xmlns:ns8="http://xml.avaya.com/schema/import_sessionmanager" xmlns:ns9="http://
xml.avaya.com/schema/presence" xmlns:ns10="http://xml.avaya.com/schema/import_csm_cm"
xmlns:ns11="http://xml.avaya.com/schema/import_mmcs" xmlns:ns12="http://xml.avaya.com/
schema/import_csm_b5800" xmlns:ns13="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>Firstname, Lastname</displayName>
        <displayNameAscii>Firstname, Lastname</displayNameAscii>
        <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>Lastname</givenName>
        <givenNameAscii>Lastname</givenNameAscii>
        <honorific></honorific>
        <loginName>abc@avaya.com</loginName>
        <employeeNo></employeeNo>
        <department></department>
        <organization></organization>
        <middleName></middleName>
        <preferredLanguage>pl</preferredLanguage>
        <source>local</source>
        <status>provisioned</status>
        <surname>Firstname</surname>
        <surnameAscii>Firstname</surnameAscii>
        <userName>abc</userName>
        <userPassword></userPassword>
        <commPassword>12345</commPassword>
        <roles>
            <role>End-User</role>
        </roles>
        <ownedContactLists>
            <contactList>
                <name>list-abc_avaya.com</name>
                <isPublic>false</isPublic>
                <contactListType>general</contactListType>
            </contactList>
        </ownedContactLists>
        <commProfileSet>
            <commProfileSetName>Primary</commProfileSetName>
            <isPrimary>true</isPrimary>
            <commProfileList>
                <commProfile xsi:type="ns15:ScopiaCommProfileType" xmlns:ns15="http://
xml.avaya.com/schema/import_scopia">
                    <commProfileType>scopiaProfile</commProfileType>
                    <ns15:scopiaUserId>1654</ns15:scopiaUserId>
                    <ns15:password>1111</ns15:password>
                    <ns15:vrNumber>6985001</ns15:vrNumber>
```

```
                    <ns15:needVR>true</ns15:needVR>
                    <ns15:virtualRoomId>16582</ns15:virtualRoomId>
                </commProfile>
            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

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>
<!-- Profile Settings for 96X1SIP & 96X1SIPCC Phones only -->
<xs:complexType name="xmlProfileSettings">
    <xs:sequence>
```

```
        <!-- Call Settings Options -->
        <!-- Phone Screen on Calling -->
        <xs:element name="phoneScreenCalling" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="No"/>
                    <xs:enumeration value="Yes"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Redial -->
        <xs:element name="profileRedial" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="List"/>
                    <xs:enumeration value="One Number"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Dialing Option -->
        <xs:element name="dialingOption" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Editable"/>
                    <xs:enumeration value="On-hook"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Headset Signaling -->
        <xs:element name="headsetSignaling" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Disabled"/>
                    <xs:enumeration value="Switchhook and Alerts"/>
                    <xs:enumeration value="Switchhook only"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Audio Path -->
        <xs:element name="audioPath" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Speaker"/>
                    <xs:enumeration value="Headset"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Screen & Sound Options Section -->
        <!-- Button Clicks -->
        <xs:element name="buttonClicks" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="On"/>
                    <xs:enumeration value="Off"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Phone Screen -->
        <xs:element name="phoneScreen" maxOccurs="1" minOccurs="0" >
```

```
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Half"/>
                    <xs:enumeration value="Full"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Background Logo -->
        <xs:element name="backgroundLogo" type="xs:string" maxOccurs="1"
minOccurs="0" />

        <!-- Personalized Ringing -->
        <xs:element name="personalizedRinging" type="xs:string" maxOccurs="1"
minOccurs="0" />

        <!-- Call Pickup Indication -->
        <xs:element name="callPickUpIndication" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="None"/>
                    <xs:enumeration value="Audible"/>
                    <xs:enumeration value="Visual"/>
                    <xs:enumeration value="Both"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Show Quick Touch Panel -->
        <xs:element name="touchPanel" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="0"/>
                    <xs:enumeration value="1"/>
                    <xs:enumeration value="2"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>


        <!-- Language & Region Section -->
        <!-- User Preferred Language -->
        <xs:element name="userPreferredLanguage" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="English"/>
                    <xs:enumeration value="Hebrew"/>
                    <xs:enumeration value="Brazilian Portuguese"/>
                    <xs:enumeration value="Canadian French"/>
                    <xs:enumeration value="German"/>
                    <xs:enumeration value="Parisian French"/>
                    <xs:enumeration value="Latin American Spanish"/>
                    <xs:enumeration value="Castilian Spanish"/>
                    <xs:enumeration value="Italian"/>
                    <xs:enumeration value="Dutch"/>
                    <xs:enumeration value="Russian"/>
                    <xs:enumeration value="Traditional Chinese"/>
                    <xs:enumeration value="Japanese"/>
                    <xs:enumeration value="Korean"/>
                    <xs:enumeration value="Arabic"/>
                    <xs:enumeration value="Polish"/>
                    <xs:enumeration value="Turkish"/>
                    <xs:enumeration value="Thai"/>
                    <xs:enumeration value="Chinese"/>
                  </xs:restriction>
```

```
            </xs:simpleType>
        </xs:element>

        <!-- Time Format -->
        <xs:element name="timeFormat" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="12 Hour"/>
                    <xs:enumeration value="24 Hour"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Advanced Options - Presence Integration Section -->
        <!-- Away Timer -->
        <xs:element name="awayTimer" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="On"/>
                    <xs:enumeration value="Off"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Away Timer Value -->
        <xs:element name="awayTimerValue" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:int">
                    <xs:minInclusive value="5" />
                    <xs:maxInclusive value="999" />
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:sequence>
</xs:complexType>

<!--  GroupMembershipData to be set -->
<xs:complexType name="xmlStationGroupMememberShipData">
    <xs:sequence>
        <xs:element name="groupMemData" type="csm:xmlGroupMemData"
maxOccurs="unbounded" minOccurs="0" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlGroupMemData">
    <xs:sequence>
        <xs:element name="groupType" type="xs:string" maxOccurs="1"
minOccurs="1" />
        <xs:element name="groupnumber" type="xs:string" maxOccurs="1" minOccurs="1" />
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlStationdonotSharePortwithUnnamedRegistrationData">
    <xs:sequence>
       <xs:element name="donotSharePortwithUnnamedRegistration" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
    </xs:sequence>
</xs:complexType>
</xs:schema>
```

XML Schema for CS 1000 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/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 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:Annex1Support>false</csm:Annex1Support>
                  <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 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>
```

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	The options are: • BASIC • ENTERPRISE
description	A description of the user. A human readable description of this user instance.	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
loginName	The unique login name that you provide for the user. The format for the login name is username@domain. The login name is an alphanumeric value and supports the ASCII characters “_”, “.”, and “-“.	Mandatory	
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	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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	The options are: • 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 this user record. The format of this field must be a IP Address/ Port or a name representing an enterprise LDAP or Avaya.	Optional	User Management populates the source field with the name of the file.
sourceUserKey	The key of the user from the source system. If the source is an Enterprise Active Directory server, the key is objectGUID.	Optional	By default, the value is none.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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	The options are: 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	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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:** While using the suggested **timeZone** values, consider daylight saving time (DST) and summer time adjustments. Typically, you add 1 hour to the offset. **Note:** In the import xml files, make the following changes while using specific characters: • less-than character (<) as < < • ampersand character (&) as & • greater-than character (>) as > • double-quote character (") as " • apostrophe or single-quote character (') as '	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 (-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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			(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 (+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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			(+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	
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	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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	The options 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	
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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 CommProfile uniqueness constraint include type, commprofile_set_id.	Optional	A user has a default commprofile set.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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	The options are: • 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 Manager system 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	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 respectively.
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 endpoint to a series of telephones.	Optional	
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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 patterns for incoming calls. For virtual endpoints, 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
Message Lamp Extension messageLampExt	The Message Lamp Extension associated with the current extension.	Mandatory	
muteButtonEnabled	Select to enable the mute button on the endpoint.		

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 Telecommuter/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	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Survivable GK Node Name survivableGkNodeName	Survivable GK Node Name identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the H.248 gateways. When 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).	Optional	Valid Entry Usage: Valid IP node name, any valid, previously-administered IP node name.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 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.	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. 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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 calls failed. Select true if LWC Reception is audix.	Optional	Boolean
activeStationRinging	Active endpoint ringing	Optional	Valid entries: • single • continuous • if-busy-single • silent

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 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	Optional	Valid entries: as-needed permanent

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	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 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.		

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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. 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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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. 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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			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 Softphone to the PSAP. 4. Option - Option allows the user to select the option (extension, block, or cesid) that the user selected during registration.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 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	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	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	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 transferred or conferenced has. If that attempt fails, Optional Boolean Communication Manager selects the first idle appearance coverageMsgRetrieval.	Optional	Boolean
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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			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.
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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 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.	Optional	
audibleMessageWaiting	Provides audible message waiting	Optional	Boolean

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 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	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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.
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	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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.
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	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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** • 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.	Optional	
Name	This is a Native Name Data field.	Mandatory	Max length 27
enableReachStaDomainControl Enable Reachability for Domain Control SIP Stations	The system enables Reachability on SIP endpoint.	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			If you select **Calculate Route Pattern** check box, the system: • Populates the **Sip Trunk** field • Makes **Sip Trunk** field read-only.
		Optional	
phoneScreenCalling 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.		
profileRedial Redial	The field to select the redial options.		
dialingOption Dialing Option	The field to specify the dialing options.		
headsetSignaling Headset Signaling	The field that defines a headset signaling profile.		
audioPath Audio Path	The field to set the phone to go off-hook when you make an on-hook call.		
buttonClicks Button Clicks	The field to activate or deactivate the standard button click sound.		
phoneScreen Phone Screen	The field to configure the phone screen width.		
backgroundLogo Background Logo	The option to set a customized background logo. The **Default** value sets the built-in Avaya logo.		
personalizedRinging Personalized Ringing	The option to set a personalized ring tone for an incoming call.		
callPickUpIndication Call Pickup Indication	The option to set ring tones to alert you about an incoming call.		

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
touchPanel Show Quick Touch Panel	The options to display **Quick Touch Pane**l on the phone.		
userPreferredLanguage User Preferred Language	The option to configure the user preferred language.		
timeFormat Time Format	The option to configure the time format to be displayed on the phone screen.		
awayTimer Away Timer	The option to enable the automatic away timer for presence indication.		
awayTimerValue Away Timer Value	The option to specify a value for the automatic **Away Timer**.		

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 mailbox number is to be used.	Optional	
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	

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
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 extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.	Optional	Valid values 0 to 9 number values of length 10

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
Time Zone timezone	This is the time zone for Avaya Aura® Messaging time subscribers.	Optional	Time zone in the StandardizedName format. For example, America/Phoenix. The field applies to Avaya Aura® Messaging 6.3 and later only. **Note:** If the value is not in the standardized name format, the system sets the Avaya Aura® Messaging subscriber time zone to the System Manager server time zone.
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 (]).

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
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	
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	

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
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. 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.

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
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. Specifies whether a subscriber can receive messages, email 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.	Optional	

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
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 a subscriber. Entries in this field are for convenience and are not used by the messaging system.		Max length 51
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

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
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 Communication Manager Messaging 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 extension as the account code.	Optional	
coveringExtension	This is field of Communication Manager Messaging 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.

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
miscellaneous1	This is field of Communication Manager Messaging 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 Communication Manager Messaging 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 Communication Manager Messaging 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 Communication Manager Messaging data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.	Optional	Max length 11

Attribute details defined in the Session Manager communication profile XSD

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Policy policyType	When you enable the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page, the system displays the **Policy** field to select the required policy for the Session Manager communication profile. Based on the policy selection, the system displays the relevant fields. The options are: • **fixed** • **fixed-region** • **location-region** **Note:** If the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page is not enabled, the system displays the **Primary Session Manager** and **Secondary Session Manager** fields similar to Release 8.1.x and earlier system.		-

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Primary Session Manager primarySM	When the policy type is **fixed**, the system displays this field. The name of the Session Manager instance 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	When the policy type is **fixed**, the system displays this field. 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	-
Third Session Manager thirdSM	When the policy type is **fixed**, the system displays this field. The Session Manager instance you select as the third Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary or the secondary Session Manager server becomes unavailable.	Optional	-

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Fourth Session Manager fourthSM	When the policy type is **fixed**, the system displays this field. The Session Manager instance you select as the fourth Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary, secondary, or third Session Manager server becomes unavailable.	Optional	-
Primary Region primaryFixedRegion	When you select the **fixed-region** policy type, the system displays this field. The Session Manager region you select as the primary region. You must select the primary region of the Session Manager server.	Mandatory	-
Secondary Region secondaryFixedRegion	When you select the **fixed-region** policy type, the system displays this field. The Session Manager region you select as the secondary region.	Optional	-
Third Region thirdFixedRegion	When you select the **fixed-region** policy type, the system displays this field. The Session Manager region you select as the third region.	Optional	-

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Fourth Region fourthFixedRegion	When you select the **fixed-region** policy type, the system displays this field. The Session Manager region you select as the fourth region.	Optional	-

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 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	Optional	-

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	resident with Branch Session Manager.		
Max. Simultaneous Devices maxSimultaneousDevices	The maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.	The default value is 1.	
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 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.		-

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Origination Application Sequence originationAppSequence	An Application Sequence 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 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 Manager must be the same in both the sequences.	Optional	-
Enable Centralized Call History enabledisablecalllog	The option to enable the call history feature for SIP users.	Optional	-

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Emergency Calling Origination Sequence emergencyOriginationAppSequence	The list of application sequences invoked when the system routes emergency calls from this user.	Optional	-
Emergency Calling Termination Sequence emergencyTerminationAppSequence	The list of application sequences invoked when the system routes emergency calls to this user.	Optional	-
Home Location homeLocation	The home location that you set from **Routing** > **Locations** page to support user mobility. 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** page to administer the Conference Factory Sets.	Optional	-
Enable Client thirdPartyClient	Name of third party client	Optional	Must be a string

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: executive, desktop_user_with_video, desktop_user_no_video, desktop_user_low_priority, guest_user_no_video, event_1000, event_2000, event_3000.	Mandatory	-
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.	-

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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 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.	Mandatory if the User Template supports 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**. If a file type does not match, System Manager displays an error message.

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.
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.
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.

Table continues…

Name	Description
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**.
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.

Table continues…

Name	Description
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. If a file type does not match, System Manager displays an error message.

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.
% 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	Returns to the **User Management** page.
Cancel	Cancels the import operation and 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.
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	Returns 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 4: 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>` ... `</givenName>`	First name of the user.
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 588

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 5: 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 6: 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.

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 7: Mapping of Session Manager Communication Profile elements

UI field	Description	XML tag	Possible value

Policy	When you enable the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page, you can specify the required policy for the Session Manager communication profile.
	The options are:
	• **fixed**:
	When you specify this option, provide the values for the **Primary Session Manager**, **Secondary Session Manager**, **Third Session Manager**, and **Fourth Session Manager** fields.
	The default value is **fixed**.
	• **fixed-region**:
	When you specify this option, provide the values to the **Primary Region**, **Secondary Region**, **Third Region**, and **Fourth Region** fields.
	The system assigns the primary, secondary, third, or fourth region to the Session Manager Communication profile.
	• **location-region**: When you specify this option, the system performs the dynamic assignment of Session
		`<sm:policyType>`
		...
		`</sm:policyType>`
			• **fixed**
			• **fixed-region**
			• **location-region**

Table continues…

UI field	Description	XML tag	Possible value
	Manager based on the mapping of locations to regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Location to Region Mapping** page. **Note:** If the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page is not enabled, specify the **Primary Session Manager** and **Secondary Session Manager** fields similar to the Release 8.1.x and earlier system.		

Primary Session Manager	Specifies the name of the primary Session Manager instance used as the home server for a communication profile.	`<sm:primarySM>`
		...
		`</sm:primarySM>`
			Enter the name of Session Manager.

Secondary Session Manager	Specifies the name of the secondary Session Manager instance used to provide continued service to SIP devices associated with this communication profile when the primary Session Manager is unavailable.	`<sm:secondarySM>`
		...
		`</sm:secondarySM>`
			Enter the name of Session Manager.

Table continues…

UI field	Description	XML tag	Possible value

Third Session Manager	Specifies the name of the third Session Manager instance used to provide continued service to SIP devices associated with this communication profile when the primary or the secondary Session Manager server becomes unavailable.	`<sm:thirdSM>`
		...
		`</sm:thirdSM>`
			Enter the name of Session Manager.

Fourth Session Manager	Specifies the name of the fourth Session Manager instance used to provide continued service to SIP devices associated with this communication profile when the primary, secondary, or third Session Manager server becomes unavailable.	`<sm:fourthSM>`
		...
		`</sm:fourthSM>`
			Enter the name of Session Manager.

Primary Region	When you specify the **fixed-region** policy type, this field indicates the primary region of the Session Manager server.	`<sm:primaryFixedRegion>`
		...
		`</sm:primaryFixedRegion>`
			Enter the name of region.

Secondary Region	When you specify the **fixed-region** policy type, this field indicates the secondary region of the Session Manager server.	`<sm:secondaryFixedRegion>`
		...
		`</sm:secondaryFixedRegion>`
			Enter the name of region.

Third Region	When you specify the **fixed-region** policy type, this field indicates the third region of the Session Manager server.	`<sm:thirdFixedRegion>`
		...
		`</sm:thirdFixedRegion>`
			Enter the name of region.

Fourth Region	When you specify the **fixed-region** policy type, this field indicates the fourth region of the Session Manager server.	`<sm:fourthFixedRegion>`
		...
		`</sm:fourthFixedRegion>`
			Enter the name of region.

Table continues…

UI field	Description	XML tag	Possible value

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>`	

Emergency Origination Application Sequence	Specifies the emergency application sequence that is invoked when calls are routed from this user.	`<sm:emergencyOriginationAppSequence>`
		...
		`</sm:emergencyOriginationAppSequence>`	

Emergency Termination Application Sequence	Specifies the emergency application sequence that is invoked when calls are routed to this user.	`<sm:emergencyTerminationAppSequencee>`
		...
		`</sm:emergencyTerminationAppSequence>`	

Survivability Server	Specifies 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.	`<sm:survivabilityServer>`
		...
		`</sm:survivabilityServer>`
			The name of a Branch Session Manager, but can be any non-CM SIP Entity.

Max. Simultaneous Devices	Specifies the maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.	`<sm:maxSimultaneousDevices>`
		...
		`</sm:maxSimultaneousDevices>`
			The value is an integer between 1 and 10. The default value is 1.

Table continues…

UI field	Description	XML tag	Possible value

Block New Registration When Maximum Registrations Active	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 endpoint cannot register with Session Manager The endpoint does not have the SIP service.	`<sm:blockNewRegistrationWhenMaxActive>`
		...
		`</sm:blockNewRegistrationWhenMaxActive>`
			true or false
			The default value is false.

Home Location	Specifies the routing home location.	`<sm:homeLocation>`
		...
		`</sm:homeLocation>`
			The name of the Home Location.

Conference Factory Set	Specifies the conference factory set to enable media capability-based call routing to the Conferencing SIP entities.	`<sm:confFactorySet>`
		...
		`</sm:confFactorySet>`
			The name of the conference factory set.

Enable Centralized Call History	Specifies the option to enable the call history feature for SIP users.	`<sm:enabledisablecallog>`
		...
		`</sm:enabledisablecallog>`
			enable or disable

Enable Client	Specifies the drop-down list of supported third party clients.	`<sm:thirdPartyClient>`
		...
		`</sm:thirdPartyClient>`
			ZOOM, Avaya Cloud Office Hybrid or blank

The following is the mapping of CM Endpoint Profile elements with the corresponding user interface fields.

Table 8: 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 on page 377

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 590

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** > **Public Contacts**.
2. On the Public Contacts page, click **New**.
3. 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.

4. In the **Postal Address** area, click **New** to add postal address of the contact.
5. 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.
6. Click **Commit** to create a new public contact.

Related links

New Public Contact field descriptions on page 606

Modifying details of a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Public Contacts**.
2. On the Public Contacts page, click **Edit**.
3. On the Edit Public Contact page, modify the information of the contact.
4. 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 604

Deleting public contacts

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Public Contacts**.
2. On the Public Contacts page, select one or more contacts.
3. Click **Delete**.
4. 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** > **Public Contacts**.
2. 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 602

Adding a postal address for a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Public Contacts**.
2. 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**.
3. Click **New** in the **Postal 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 postal address for the public contact.
6. On the New Public Contact or Edit Public Contact page, click **Commit**.

Related links

Add Address field descriptions on page 246

Modifying postal address of a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Public Contacts**.
2. On the Public Contacts page, select a public contact and click **Edit**.
3. On the Edit Public Contact page, select an address from the Postal Address section.
4. Click **Edit**.
5. On the Edit Address page, modify the information in the respective fields.

   The fields marked with an asterisk are mandatory. You must enter valid information in these fields.

6. Click **Add** to save the modified address.

Related links

Add Address field descriptions on page 246

Deleting the postal addresses of a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Public Contacts**.
2. On the Public Contacts page, select a public contact and click **Edit**.
3. Select an address from the table in the Postal Address section, and click **Delete**.
4. 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** > **Public Contacts**.
2. Click **Choose Shared Address**.
3. On the Choose Address page, select one or more shared addresses.
4. Click **Select** to add the selected addresses for the public contact.
5. Click **Commit**.

Adding a contact address of a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Public Contacts**.
2. Click **New** in the **Contact Address** area.
3. On the Add Address page, enter the appropriate information in the respective fields.

   Enter a valid information in these fields.
4. Click **Add** to create a new contact address for the public contact.
5. On the New Public Contact page, click **Commit**.

Related links

Add Address field descriptions on page 281

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** > **Public Contacts**.
2. On the Public Contacts page, select a public contact and click **Edit**.
3. On the Edit Public Contact page, modify the information in the Contact Details, Postal Address, and Contact Address 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.
4. Click **Commit**.

Related links

Edit Address field descriptions on page 282

Deleting the contact address of a public contact

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Public Contacts**.
2. On the Public Contacts page, select a public contact and click **Edit**.

   If you are on the New Public Contact page, follow Step 4.
3. In the **Contact Address** area, select one or more addresses from the list and click **Delete**.
4. Click **Commit** to save the changes.

View Public Contact field descriptions

Contact Details

Name	Description
Last Name	The last name of the contact.

Table continues…

Name	Description
Last Name (Latin Translation)	The user-preferred last name that the system must display on the endpoints. For example, Miller. Typically, the name is in the written or spoken language of the user. **Last Name (Latin Translation)** can be up to 256 characters. **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 and first names change. • Filled, the values remain the same 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 endpoints. For example, John. Typically, the name is in the written or spoken language of the user. **First Name (Latin Translation)** can be up to 256 characters.
Middle Name	The middle name of the contact.
Description	Displays a brief description of 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.

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 600

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 endpoints. For example, Miller. Typically, the name is in the written or spoken language of the user. **Last Name (Latin Translation)** can be up to 256 characters. **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 and first names change. • Filled, the values remain the same 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 endpoints. For example, John. Typically, the name is in the written or spoken language of the user. **First Name (Latin Translation)** can be up to 256 characters.
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.

Table continues…

Name	Description
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	Displays the **Edit Address** page. Use this page to add a new postal address of the public contact.
New	Displays 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	Displays 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	Displays the **Edit Address** page. Use this page to edit a contact address of the public contact.

Table continues…

Button	Description
New	Displays 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 599

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 endpoints. For example, Miller. Typically, the name is in the written or spoken language of the user. **Last Name (Latin Translation)** can be up to 256 characters. **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 and first names change. • Filled, the values remain the same 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 endpoints. For example, John. Typically, the name is in the written or spoken language of the user. **First Name (Latin Translation)** can be up to 256 characters.
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	Displays the **Edit Address** page. Use this page to add a new postal address of the public contact.
New	Displays 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	Displays 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	Displays the **Edit Address** page. Use this page to edit a contact address of the public contact.
New	Displays 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 598

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

Use this procedure to choose a shared address for a user from the common addresses database. You can assign and remove a shared address.

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, do 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**.
3. On the User Profile | Add page or the User Profile | Edit | <User Name> page, click **Identity** > **Address** > **Choose Shared Address**.
4. On the Choose Shared Address page, click one or more shared addresses.

For a new user, enter valid information in all mandatory fields on all tabs of the User Profile | Add page before you click **Commit**. If you enter invalid information, the system displays an error message.

5. Click **Select**.
6. Click one of the following:
   - **Commit**: To save the changes.
   - **Commit & Continue**: To save the changes and stay on the same page for making further modifications.

Related links

Choose Address field descriptions on page 247

Adding a shared address

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Shared Addresses**.
2. On the Shared Address page, click **New**.
3. On the Add Address page, enter the appropriate information.
4. 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** > **Shared Addresses**.
2. On the Shared Address page, select an address and click **Edit**.
3. On the Edit Address page, modify the information in the fields.
4. 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** > **Shared Addresses**.

2. 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 610
Adding a shared address on page 610

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. • **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 602

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.

Table continues…

Name	Description
Province	Displays the full name of the province.
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	Displays the Add Address page. Use this page to add an address.
Edit	Displays 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 613

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.

Name	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**:

Name	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 password has the following requirements:

- Passwords must contain 6 to 25 characters. The default value is 14.
- Passwords must contain a combination of the following characters: a-z, A-Z, 0-9, {, }, |, (,), <, >, ,, /, ., =, [,], ^, _ ,@, !, $, %, &, -, +, ", :, ?, `, or ;
- Passwords must contain at least one each of the following characters:
  - A lowercase letter
  - An uppercase letter
  - A number
  - A special character

- Password can contain maximum of 2 consecutive characters. The valid values are from 1 through 5. The default value is 2.
- Password can contain maximum number of 4 consecutive characters from the same character type. The valid values are from 1 through 5. The default value is 4.

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 the communication profile on page 615
Communication Profile Password Policy field descriptions on page 616
User Profile | Add field descriptions on page 285

Editing the password policy for the communication profile

Procedure

1. On the System Manager web console, click **Users** > **User Management** > **Communication Profile Password Policy**.
2. On the Communication Profile Password Policy page, do the following:
   a. On the **Aging Policy** tab, select the **Enforce password aging policy** check box, and modify the required fields.
   b. On the **History Policy** tab, select the **Enforce policy against previously used passwords** check box, and type the value in the **Previous passwords blocked** field.
   c. On the **Strength Policy** tab, select the **Enforce password content standards** check box, and modify the required fields.

   For information about the fields, see “Communication Profile Password Policy field descriptions”.
3. Click **Commit**.

   System Manager saves the changes to the password policy for the communication profile password.

Related links

Communication Profile Password Policy field descriptions on page 616

Communication Profile Password Policy field descriptions

Aging Policy

Name	Description
Enforce password aging policy	The option to enable or disable the password aging policies. By default, the password aging policy is disabled. To enforce the password aging policies, select the check box. If you clear the check box, the password aging policy is not applicable. **Note:** If the password policy is disabled earlier and you enable it then all users whose password now match the criteria are asked to change their password.
Expiration period	The maximum number of days to maintain the password. The default value is 60 days. The valid values are from 1 through 365 days.
Expiration warning	The number of days for password expiry prior to which the password expiration warning message must be sent to the user. The valid values are from 1 through 15 days. The default value is 10 days.
Minimum age for password change	The minimum number of days for password age. The valid values are from 0 through 7 days. The default value is 1 day. Ensure that the expiration period is greater than the minimum password age.
Enable expired password change	If this is enabled, you can change the password after it expires. If this is disabled, only the system administrator can change the password. When you log in with the system administrator-provided password, you must change the password.

History Policy

Name	Description
Enforce policy against previously used passwords	The option to enable or disable the password policy against previously used passwords. By default, the password policy against previously used passwords is disabled. To enforce the password policy against previously used passwords, select the check box. If you clear the check box, the password policy against previously used passwords is not applicable.
Previous passwords blocked	The number of latest passwords that the system maintains in history. You cannot reset your password to these values. The valid values are from 1 through 15. From Release 8.1.3, the default value is 10. For earlier release system, the default value is 6.

Strength Policy

Name	Description
Enforce password content standards	The option to enable or disable the password content standards. By default, the password content standards is disabled. To enforce the password content standards, select the check box. If you clear the check box, the password content standards is not applicable.
Minimum total length	The minimum number of characters to use in the password. The password can be of 6 to 25 characters. From Release 8.1.3, the default value is 14. For earlier release system, the default value is 8.
Minimum by character Type: Lower case	The minimum number of lowercase characters to use in the password. The default value is 1.
Minimum by character Type: Upper case	The minimum number of uppercase characters to use in the password. The default value is 1.
Minimum by character Type: Numeric case	The minimum number of numeric characters to use in the password. The default value is 1.
Minimum by character Type: Special case	The minimum number of special characters to use in the password. The default value is 1.
Maximum repeated consecutive characters	The maximum number of repeated consecutive characters. The valid values are from 1 through 5. The default value is 2. For example, if the maximum repeated consecutive characters value is set to 2: • Valid password is: Buildd123$ • Invalid password is: Builddd123$
Maximum consecutive characters from same character type	The maximum number of consecutive characters from the same character type. The valid values are from 1 through 5. The default value is 4. For example, if the maximum repeated consecutive characters of the same character type is set to 4: • Valid password is: Build123$ • Invalid password is: Build12345$

Button	Description
Commit	Saves all the changes on the Communication Profile Password Policy page.
Cancel	Cancels the changes and returns to the previous page.

Chapter 8: Managing user provisioning rules

User Provisioning Rule

System Manager provides 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 a 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

The administrator can assign only one user provisioning rule to any 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
- Directory 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
SMGR core services	clone, view, edit, add, and delete

Capabilities and guidelines of user provisioning rules

Capabilities of user provisioning rules

The user provisioning rule is a template that is used 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 while creating the user. User provisioning rules cannot be used after they are applied. After you create a user by using 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 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 by using the user provisioning rule. You can assign only one communication profile to a user provisioning rule.

  Note:

  When you define user provisioning rule with elements data in the **Communication Profile** section, and later if you change value for Session Manager, Communication Manager Templates, and Messaging elements, then you must update the existing user provisioning rule with latest element data.

  If the user provisioning rule and communication profile data are available from the 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 from the user provisioning rule.

- After you create the user by using the user provisioning rule, you can modify values of an existing communication profile by using one of the following System Manager user provisioning interfaces:
  - System Manager native user interface
  - Web Services API
  - Bulk import and export

- Global Endpoint Change Editor

Also, you can add another communication profile by using a different user provisioning rule.

- Whenever a user provisioning rule is used while creating or updating a user, the administrator should not manually remove any communication profile.

Guidelines for upgrading Communication Manager and Messaging elements

1. Before upgrading the Communication Manager and Messaging elements to major Release 6.3.x and later, note down the Communication Manager and Messaging templates associated with user provisioning rule in System Manager.
2. Once the Communication Manager or Messaging element is upgraded, then templates associated with old release of Communication Manager and Messaging will get unlinked for existing user provisioning rule. Therefore, after upgrading Communication Manager and Messaging elements:
   a. Create custom templates for the current release of Communication Manager and Messaging.
   b. Update existing user provisioning rule with newly created custom templates or default templates of Communication Manager and Messaging as per the user provisioning rule guidelines.

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
   - Avaya Breeze® 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 with administrator privilege credentials.
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, do 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 appropriate information.
   c. On the **Organization** tab, enter the appropriate information.

   For more information, see “User Provisioning Rule field descriptions”.
5. Click **Commit** to save the changes.

Related links

New User Provisioning Rule field descriptions on page 624

Modifying the user provisioning rule

Before you begin

Create a user provisioning rule.

Procedure

1. Log on to System Manager with administrator privilege credentials.
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, click one of the following:
   - **Edit**.
   - **View** > **Edit**.
5. On the Edit User Provisioning Rule page, do 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.

c. On the **Organization** tab, modify the appropriate information.

6. Click **Commit**.

Related links

New User Provisioning Rule field descriptions on page 624

Viewing the user provisioning rule

Before you begin

Create a user provisioning rule.

Procedure

1. Log on to System Manager with administrator privilege credentials.
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

New User Provisioning Rule field descriptions on page 624

Creating a duplicate user provisioning rule

About this task

You can create a new user provisioning rule by duplicating the information from an existing user provisioning rule.

Procedure

1. Log on to System Manager with administrator privilege credentials.
2. On the System Manager web console, click **Users** > **User Provisioning Rule**.
3. On the User Provisioning Rules page, click the user provisioning rule.
4. Click **Duplicate**.
5. On the Duplicate User Provisioning Rule page, do the following:

   a. On the **Basic** tab, change the appropriate information.

b. On the **Communication Profile** tab, change the communication profile information as appropriate.

c. On the **Organization** tab, change the appropriate information.

For more information, see “User Provisioning Rule field descriptions”.

6. Click **Commit**.

Related links

New User Provisioning Rule field descriptions on page 624

Deleting a user provisioning rule

Procedure

1. Log on to System Manager with administrator privilege credentials.
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**.

   System Manager:

   - Removes the selected user provisioning rule.
   - Disassociates the user provisioning rule from the user if you have already provided the user provisioning rule for the user.

Related links

New User Provisioning Rule field descriptions on page 624

User Provisioning Rules field descriptions

Name	Description
Name	The name of the user provisioning rule.
SIP Domain	The name of the configured SIP domain name.
Description	The description of the user provisioning rule.

Button	Description
View	Displays the View User Provisioning Rule page with details of the user provisioning rule that you selected.

Table continues…

Button	Description
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 selected user provisioning rule.
Duplicate	Duplicates the selected user provisioning rule.
Select	Selects a user provisioning rule in the table. The options are: • **All**: To select all user provisioning rules in the table. • **None**: To clear the selections.

Icon	Name	Description
	Refresh	Refreshes the user provisioning rule information in the table.

New User Provisioning Rule field descriptions

Basic

Name	Description
User Provisioning Rule Name	Displays the name of the user provisioning rule.
Description	A description of the user provisioning rule.
SIP Domain	Displays 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 you provide.
Presence/IM Domain	Displays 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 you provide.

Table continues…

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 on the **Users** > **User Management** > **Communication Profile Password Policy** page. When you provide the communication password value during bulk edit of users, the system overwrites any existing communication profile passwords of the user. For information about password policy, see “Communication profile password policy”.
Confirm Password	The communication profile password to 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 a maximum of 13 digits. Usually, the numbers are written with a plus (+) as the prefix. The system populates the phone number 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 the telephone number or Avaya E.164 handle. The default is plus (+).
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:

Name	Description
Policy	When you enable the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page, the system displays the **Policy** field to select the required policy for the Session Manager communication profile. For more information, see *Administering Avaya Aura® Session Manager*. Based on the policy selection, the system displays the relevant fields. The options are: • **fixed**: When you select this option, the system displays the **Primary Session Manager**, **Secondary Session Manager**, **Third Session Manager**, and **Fourth Session Manager** fields. The default value is **fixed**. • **fixed-region**: When you select this option, the system displays the **Primary Region**, **Secondary Region**, **Third Region**, and **Fourth Region** fields. The system assigns the primary, secondary, third, or fourth region to the Session Manager Communication profile. • **location-region**: When you select this option, the system does not display the **Primary Session Manager** and **Secondary Session Manager** fields and dynamically assigns Session Managers based on the mapping of locations to regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Location to Region Mapping** page. **Note:** If the **Enable Policy Based Assignment of Session Managers** field on the **Elements** > **Session Manager** > **Global Settings** page is not enabled, the system displays the **Primary Session Manager** and **Secondary Session Manager** fields similar to the Release 8.1.x and earlier system.
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.

Table continues…

Name	Description
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. This is an optional field. All the four Session Manager values must be unique. For example, if you select the same Session Manager server instance in the **Secondary Session Manager** field as the **Primary Session Manager** field, the system displays the following error message: `The Secondary Session Manager cannot be the same as the Primary Session Manager.`
Third Session Manager	The Session Manager instance that you select as the third Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary or the secondary Session Manager server becomes unavailable. This is an optional field. You must select the value of the Session Manager servers as per the order of display. For example, if you select the third Session Manager value before the secondary Session Manager, the system displays the following error message: `Selection of Session Managers should be as per their order of display. Select Secondary Session Manager before Third Session Manager.`
Fourth Session Manager	The Session Manager instance that you select as the fourth Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary, secondary, or third Session Manager server becomes unavailable. This is an optional field.
Primary Region	The Session Manager region that you select as the primary region. You must select the primary region of the Session Manager server. You can create the regions on the **Elements** > **Session Manager** > **Session Manager Administration** > **Groups** > **Session Manager Groups** page. You must select the value of regions as per the order of display. For example, if you select the secondary region value before the primary region, the system displays the following error message: `Selection of regions should be as per their order of display. Select Primary Region before Secondary Region.`

Table continues…

Name	Description
Secondary Region	The Session Manager region that you select as the secondary region. This is an optional field. **Note:** • If you select the same region for the primary and secondary regions, then there must be a minimum of two Session Managers in that region. • If you select 4 different regions, then there must be a minimum of 1 Session Manager in each region. If you select the same region and the region does not have sufficient Session Managers, the system displays the following error message: `<Secondary Region> - <Name_of_the_Region> the assigned regions must contain enough SMs to satisfy the Primary/Secondary/Third/Fourth region selection count.`
Third Region	The Session Manager region that you select as the third region. This is an optional field.
Fourth Region	The Session Manager region that you select as the fourth region. This is an optional field.
Survivability Server	For local survivability, you can specify a survivability server. The server provides survivability communication services to devices associated with a communication profile, when the local connectivity to Session Manager instances in Avaya core is lost. If you select 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. This survivable remote server is resident with the Branch Session Manager selected. 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. After typing a minimum of 3 characters, wait for three seconds to capture the final keyword and fetch the required results.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.

Table continues…

Name	Description
Block New Registration When Maximum Registrations Active	If you select the check box, the system denies any new registrations with Session Manager when an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit. 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 affect the call and keeps that device registered for that call only.
Origination Application Sequence	The application sequence the system invokes when routing 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 invoked when the system routes 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.
Emergency Calling Origination Sequence	The list of application sequences invoked when the system routes emergency calls from this user.
Emergency Calling Termination Sequence	The list of application sequences invoked when the system routes emergency calls to this user.
Home Location	The 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 the IP Address Pattern of any 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** page 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.
Enable Client	The drop-down list of the supported clients. Select the required client.

Communication Profile tab: Avaya Breeze® 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 Communication Manager Endpoint profile exists for the user.

Name	Description
Use Next Available Extension	The option 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.
Sub Type	This field is configured for CS 1000 station types only. You can select the specific set for **Set Type**. On the Manage Endpoint page, **Sub Type** is labeled as **Set**.
System ID	This field is configured for CS 1000 station types only. This field allows you to leave the field blank or enter a string of up to 9 characters. With Release 8.0, more than one station can use the combination of **System ID** and **Terminal Number**. With Release 8.0.1, each station must have a unique combination of **System ID** and **Terminal Number**.
Security Code	The security code for authorized access to the endpoint.
Preferred Handle	Avaya SIP or Avaya E.164 handle 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 **Profile Type**.
Allow H.323 and SIP Endpoint Dual Registration	The option to register an H.323 endpoint and a SIP endpoint together at the same time to the same extension. For more information about the SIP and H.323 dual registration feature, see *Avaya Aura® Communication Manager Feature Description and Implementation* on the Avaya Support website at http://support.avaya.com.

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.

Table continues…

Name	Description
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: 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.
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 delete the user.

Communication Profile tab: Avaya Messaging Profile

Name	Description
System	The Avaya Messaging system to which you add a mailbox.
Refresh	The option to get information about company, departments, and feature groups from Avaya Messaging and save locally on System Manager for future use. You do not require to refresh for every user.
Use Next Available Mailbox	The option to specify if the system must use the next mailbox number to associate with this profile.

Table continues…

Name	Description
Mailbox Range	The range of mailbox numbers assigned to the Avaya Messaging system. **Note:** This option is available only when you select the **Use Next Available Mailbox** check box.
Numeric Password	The numeric password used to log in to the Avaya Messaging system.
Application User Password	The password used to gain access to non-telephone applications, such as Web Client, iLink Pro, iLink Pro Mobile, and iLink Pro Desktop.
Company	The name of the company to which the user belongs.
Department	The department to which the user belongs.
Feature Group	The feature group name that determines the rules for the mailboxes associated with it.
Capability	The type of functionality the user contains. The values are: • **Standard** • **Fax** • **Messaging** • **Collaboration** • **Messaging and Collaboration**
Domain Account Name	The mailbox NT account name for the Avaya Messaging profile. The options are: • **Same as Login Name** • **Admin Specified**
Synchronization User Name	The account name that is used to gain access to the email server, for example, Microsoft Exchange and Google Gmail. The options are: • **Same as Login Name** • **Admin Specified**

Communication Profile tab: IP Office Endpoint Profile

Name	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.

Table continues…

Name	Description
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 Presence Services. This system selects the SIP entity 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 SIP Entity	The Presence Services instance for the user.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with 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: Equinox Profile

Name/Button	Description
Equinox User Password	The password that is used to log in to the Avaya Workplace Client Management.

Table continues…

Name/Button	Description
Virtual Room Number	The number of a virtual room that is used to create a conference. By default Virtual Room Number serves as Meeting ID when a conference is created. The options are: • **Use Phone Number**: This will use Communication Manager extension. Use this option only if Communication Manager profile is already associated with the user or being associated with the user. • **Auto Generate Virtual Room Number**: Use this option if the system needs to generate the Virtual Room Number automatically.

Organization

Name/Button	Description
Tenant	The tenant of the user created by the user provisioning rule.
Site	The work site of the user created by the user provisioning rule.
Department	The department of the user created by the user provisioning rule.
Team	The team of the user created by the user provisioning rule.

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

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 element that you import.

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 Subscriber 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**, leave the **Name** field blank, and 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

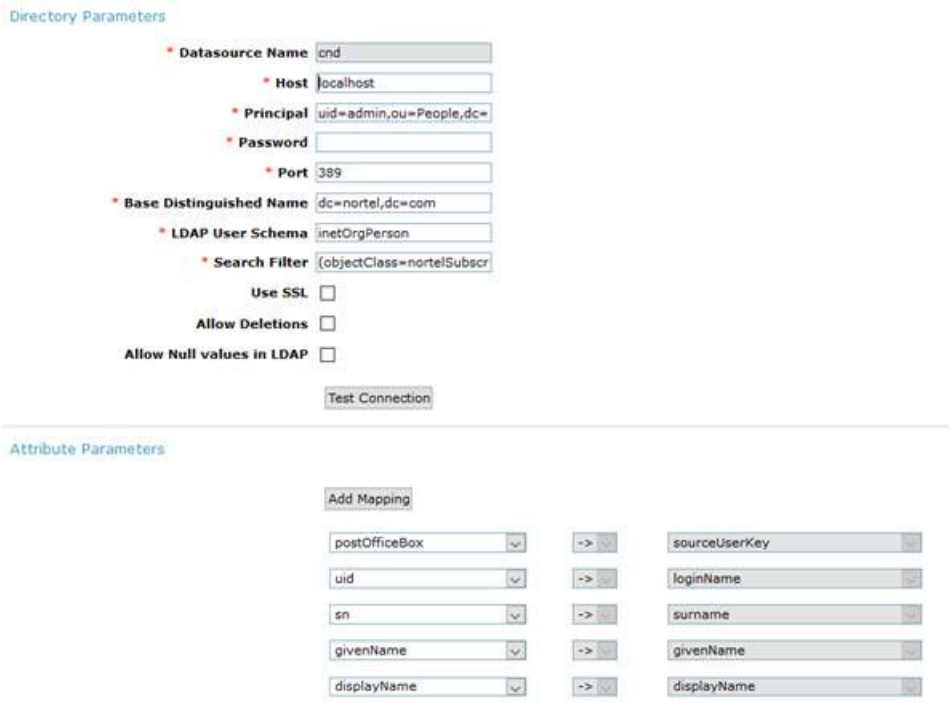
Before you begin

- 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 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.



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 84
Adding the synchronization datasource on page 75
Subscriber Manager datasource parameters and attributes on page 639

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>*
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
Allow Null values in LDAP	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.

Table continues…

Subscriber Manager attribute	User Management attribute	Import Type	Description
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.
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 element that are being imported. For information on profile synchronization, see Synchronizing CS 1000 profiles.

Related links

Bulk importing of users on page 377
Exporting users in bulk from web console on page 381

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 synchronize 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 636
Preparing the Subscriber Manager user data for import to User Management on page 636

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 637
Subscriber Manager datasource parameters and attributes on page 639
Importing the Subscriber Manager user data to User Management on page 637
Subscriber Manager datasource parameters and attributes on page 639

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 640
Exporting the user data and creating the user profile on page 640

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 636
Preparing the Subscriber Manager user data for import to User Management on page 636

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 637
Subscriber Manager datasource parameters and attributes on page 639
Importing the Subscriber Manager user data to User Management on page 637
Subscriber Manager datasource parameters and attributes on page 639

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 640
Exporting the user data and creating the user profile on page 640

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 and
- Avaya Aura® Messaging 6.0 and later

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 or Modular Messaging from the list of messaging systems, and then click **New**, the system displays the Add Subscriber page with the first Messaging or Modular Messaging in context.

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.

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.

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.

Table continues…

Name	Description
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 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 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.
Reset or **Clear**	Clears all changes.
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

Important:

The **Elements** > **Communication Manager** > **Cluster Management** page and all the screens and options are for future use.

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 pop 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, Communication 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

Table continues…

Communication Manager object	Searchable fields	Supported Actions
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

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** > **Synchronization** > **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
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

Table continues…

Group	Communication Manager objects
Network	Automatic Alternate Routing Analysis Automatic Alternate Routing Digit Conversion Automatic Route Selection Analysis Automatic Route Selection Digit Conversion Automatic Route Selection Toll Cluster Session Manager 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 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.

Export function of Communication Manager objects

When you export the selected object or all objects, System Manager exports the objects in an excel sheet.

Note the following points:

- The Excel sheet has hyperlink limit of 65530. If the hyperlinks in the exported excel sheet exceeds from the provided limit, System Manager stops adding new hyperlinks. To maintain consistency, the font size is same for the text where hyperlink is applicable and even if hyperlink is not added.
- The Excel sheet has row limit of 1048576. If this limit is reached while exporting data on any sheet, System Manager creates a new file and continues exporting the data in the new Excel sheet. Once all data is exported, all the excel files are merged in a zip. So, if there are more than one Excel files then the Export Job list provides link to the zip file. Otherwise, System Manager provides the direct excel download.

Related links

Adding Communication Manager objects on page 660
Editing Communication Manager objects on page 661
Viewing Communication Manager objects on page 661
Deleting Communication Manager objects on page 661
Filtering Communication Manager objects on page 662

Adding Communication Manager objects

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. Select the Communication Manager object.
3. Select one or more 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 one or more 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 one or more 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 one or more 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 one or more 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 navigation pane, click **Call Center** > **Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. From **Template**, select the template.
7. In **Login ID**, perform one of the following:
   - Type the extension number.
   - Click the **Display Extension Ranges** link to select the extension number from the available extension ranges.
8. Complete the New Agent page and click **Commit**.

Related links

Agents field descriptions on page 668

Viewing agent data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Agents**.
3. Select one or more 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 668

Editing agent data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Agents**.
3. Select one or more 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 668

Deleting agents

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Agents**.
3. Select one or more 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 668

Adding agents in bulk

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Agents**.
3. Select one or more 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 668

Editing agent data in bulk

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Agents**.
3. Select one or more 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 668

Deleting agents in bulk

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Agents**.
3. Select one or more 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.

Exporting selected agent

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the **Agent List**, select the agent you want to export.
6. Click **More Actions** > **Export Selected Agents**.

   The system displays the **Export AgentLoginIds** page.
7. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
8. Click **Export**.

   System Manager displays the status of the exported job in the **Status** column of the Export Jobs List section.

Exporting all agents

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Export All Agents**.

   The system displays the **Export All AgentLoginIds** page.
6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

   System Manager displays the status of the exported job in the **Status** column of the Export Jobs List section.

Importing agents

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Import Agents**.

   The system displays the **Import CM Objects** page.
6. In the **Select a file** field, click **Browse** to select the required excel file.
7. In the **Select Error Configuration** field, select one of the following.

   The default option is **Continue processing other records**.

   - **Abort on first error**
   - **Continue processing other records**
8. In the **If a matching record already exists** field, select one of the following:

   The default option is **Skip**.

   - **Skip**
   - **Merge**
   - **Delete**
9. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.

10. Click **Import**.

    System Manager displays the status of the imported job in the **Status** column of the Import Jobs List section.

Downloading Excel Template

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Download Excel Template**.
6. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and click **OK**.

   System Manager saves the file on your local computer.

Agents field descriptions

If you change the value of the fields from the systemparameters features screen of Communication Manager, agents must log out and log back in for the change to be reflected.

Name	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.
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.

Table continues…

Name	Description
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. • 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 Agent Considered Idle (MIA)	To include agents who are in the AUX mode in the Most Idle Agent (MIA) queue. Communication Manager counts the time in AUX as idle time. The options are: • **System**: Communication Manager uses the system-wide field settings. • **Yes**: Communication Manager keeps or places agents in the MIA queue while they are in AUX work. • **No**: Communication Manager excludes AUX agents from the MIA queue while they are in AUX work. The **No** value matches the legacy Communication Manager functionality.

Table continues…

Name	Description
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 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*.
Check skill TNs to match agent TN	The skill tenant number to match the tenant number.
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	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.

Table continues…

Name	Description
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.
Hears Service Observing Tone	When you enable the **(SA8569) - No Service Observing Tone Heard by Agent** field on the Special Application form, the system enables the **Hears Service Observing Tone** field.
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.
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. 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 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…

Name	Description
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. • **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	To remove an agent from the MIA queue for all splits or skills that the agent is available in when the agent answers a call from any assigned splits or skills. The options are: • **System** • **Yes** • **No**
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.
MWI Served User Type	This field is available for Communication Manager Release 7.1.3.6 and Release 8.1.2 and later. However, System Manager Release 8.1.2 displays this field on the Agent add/edit page if you select Communication Manager Release 7.1 and later. If the **MWI Served User Type** field is administered on System Manager and Communication Manager Release does not have the value in this field, you can create Agent but the system operations will be unaffected. Controls the auditing of a served user's message waiting indicator (MWI). The options are: • **None**: The served user's MWI is not audited. The user's MWI is not audited if the user is not served by an fp-mwi, qsig-mwi, or sip-adjunct message center. • **fp-mwi**: The agent is a served user of an fp-mwi message center. • **qsig-mwi**: The agent is a served user of a qsig-mwi message center. • **sip-adjunct**: Use this option to audit the user's MWI.

Table continues…

Name	Description
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 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*.

Table continues…

Name	Description
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**. **Note:** Values entered in this field are not echoed to the screen.

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 the 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 the 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).
- Disk/Flash Memory as vVAL in H.248 Media Gateways.
- Disk or content store on Avaya Aura® Media Server or also can be sourced from an internet source if using Avaya Aura® MS.

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

While scheduling backup or backing up all jobs from the List Announcement page, if the backup size is:

- Greater than 1 GB, the system does not schedule the job and displays an error.
- Less than 1 GB or if system estimates that the backup size is exceeding 1 GB limit while executing the job, the scheduled job fails with error: `Used size has exceeded the maximum allowed size. Consider removing the old backups.`

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.

Note:

When Avaya Aura® Media Server is used for announcement operations, such as Add, Delete, Broadcast, Backup or Download, only Avaya Aura® Media Server IPv4 addresses are supported. System Manager ignores Avaya Aura® Media Server IPv6 addresses if configured for those operations.

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. 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**: Indicates that the announcement does not play if a port is not available. This is the default value. • **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. • **bargein**: 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.

Table continues…

Name	Description
Live Stream Source	Indicates if the announcement is played live from an external source or from an audio file. After you configure the announcement with Live Stream Source type, play once to ensure that the live streaming feature works correctly. When you deactivate the Release 10.2.x patch, the system runs on Release 10.2.x system and sets the **Live Stream Source** feature to `n`. Therefore, you must install and activate the new Release 10.2.x patch immediately to prevent the system processes from running on the Release 10.2.x system. You must also set the value of the **Live Stream Source** feature to `y`.
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 navigation pane, click **Call Center** > **Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select **New**.
6. On the New Announcement page, complete the fields and click **Commit**.

   For more information, see “Announcements field descriptions”.

Related links

Announcements field descriptions on page 684

Editing an announcement

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more 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 684

Viewing an announcement

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more 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 684

Deleting an announcement

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more 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 navigation pane, click **Call Center** > **Announcements**.
3. Select one or more 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 684

Backing up announcements

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more 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 684

Backing up all announcements

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more 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 navigation pane, click **Call Center** > **Announcements**.
3. Select one or more 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 684

Restoring announcements

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Restore**.
6. Select one or more 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 684

Restoring all announcements

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more 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 navigation pane, click **Call Center** > **Announcements**.
3. Select one or more 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 684

Broadcasting announcements

About this task

You can upload an audio file on multiple media sources using the **Broadcast** operation. The media sources can be Media Servers, Media Gateways, or VAL Board. You can also transfer audio files from one board to the other of the same Communication Manager or boards (VAL Board, Media Gateway, or Media Server) of another Communication Manager.

Uploading audio files to media servers is done using a SOAP request. System Manager uses FTP or SCP for Media Gateway and FTP or SFTP for VAL Board. The transfer protocol for Media Gateway or VAL Board can be configured from File Transfer Settings. FTP is the default protocol for file transfer on VAL Board and Media Gateway.

With Release 8.1.1, you can upload more than one audio file (.wav) with a single click by using the **Browse** option of the **Select Announcement File** field.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Do one of the following:
   - To transfer an audio file from one audio source to another:
     a. Select the announcement that you want to broadcast from the Announcement list.
     b. Click **More Actions** > **Broadcast**.
   - To upload an audio file from your computer and broadcast it to audio sources:
     a. Click **More Actions** > **Broadcast**.
     b. On the Broadcast Announcements page, in **Select Announcement File**, click **Browse**.

c. In the File Upload dialog box, select one or more audio files from your local computer.

System Manager displays the uploaded audio files (.wav) with file name on the Broadcast Announcements page.

Note:

If you remove one of the uploaded audio files using the browse option, the system removes all the files that were uploaded together.

6. In the Select Destination for Broadcasting Announcements section, select the destination VAL source, which includes media servers too.
7. Do one of the following:
   - Click **Now** to immediately broadcast the announcement files to various VAL boards on voice system or media servers.
   - Click **Schedule** to schedule a broadcast operation later.

   On the Job Scheduler page, you can set a later time to broadcast the announcement files to various VAL boards on voice system or media servers.

Related links

Announcements field descriptions on page 684
Using File Transfer Settings on page 682
Announcements field descriptions on page 684

Using File Transfer Settings

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more 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 684

Using List Usage Extension

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more 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 684

Filtering the Announcements list

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the 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 navigation pane, click **Call Center** > **Announcements**.
3. Select one or more 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	A valid extension number for the announcement. Extension numbers must not include punctuation.
Source	The field that 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.
Type	The type of announcement. The options are: • **Integ-mus**. Integrated music type. • **Integ-rep**. Integrated repeating type. • **Integrated**. A special integrated announcement circuit pack stored internally. Use this for general announcements and VDN of Origin Announcements.
Protected	The field to set the protection mode for an integrated announcement. The options are: **y**: The recording is protected, and you cannot delete or change it through a telephone session or FTP. **n**: You can change or delete the recording if you have the corresponding console permissions.

Table continues…

Name	Description
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.
Tenant Number	The tenant partition number of the announcement. Valid entries include 1 to 100.
Queue	The announcement queue or barge-in. The options are: • **no**: Indicates that the announcement is not played if a port is unavailable. This is the default value. • **yes**: Indicates that the request is placed in a queue when all ports on the circuit pack are busy. The announcement is played when a port becomes available. Most call center applications use this setting. • **bargein**: Indicates that you can connect callers to the announcement at any time while the announcement is being played. With n or y, the caller is always connected to the beginning of the announcement.
Live Stream Source	The option to stream music on hold live from an external source. **Live Stream Source** is available only when the **Type** is **Integ-mus** or **Integ-rep**. You can select **Live Stream Source** only when: • Queue is set to **bargein.** • **Source** is set to Media Server. If you select **Live Stream Source**, the system changes the **Protected** field to Y, which is noneditable. When you deactivate the Release 10.2.x patch, the system runs on Release 10.2.x system and sets the **Live Stream Source** feature to `n`. Therefore, you must install and activate the new Release 10.2.x patch immediately to prevent the system processes from running on the Release 10.2.x system. You must also set the value of the **Live Stream Source** feature to `y`. **Note:** After you configure the announcement with Live Stream Source type, play once to ensure that the live streaming feature works correctly.
Size	The size of the audio file in kilobytes.
Timestamp	The date and time the audio file was created or modified. This value changes each time you upload the audio file.

Audio File Information

Name	Description
Use Unused Wave File	To use an audio file that has not been used yet.
Upload Audio File	To upload an audio file by browsing to the file you want to upload.

More Actions

Name	Description
Broadcast	Displays the Broadcast Announcements page. You can broadcast the announcements from the Announcement list. After the broadcast operation is completed, files are deleted from the SCP server.
File Transfer Settings	Displays the Audio File Transfer Settings page.
Compact Flash Configuration	Displays the Compact Flash Configuration page.

More Actions in Audio Groups

Name	Description
File Name	Specifies the filename of the audio file. The filename can be up to 27 characters and must be alphanumeric.
File Size	Specifies 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)

Table continues…

Name	Description
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. **Note:** SCP file transfer on gateways, works only with SNMPv3 – MD5 and DES combination.
Local SCP Server	System Manager acts as a SCP server.
SCP Server IP Address	When you select **Local SCP Server**, the system auto populates the **SCP Server IP Address** field with IP Address of System Manager.
SCP User Name	The SCP server user name. If you use **Local SCP Server**, type the System Manager CLI user name.
SCP Password	The SCP server password. If you use **Local SCP Server**, type the System Manager CLI password.
Confirm SCP Password	Confirm the SCP server password. If you use **Local SCP Server**, re-type the System Manager CLI password.
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.
Clear	Clears all the entries.
Edit	Edits 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 in 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 navigation pane, click **Call Center** > **Audio Group**.
3. Select one or more 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 690

Editing an audio group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Audio Group**.
3. Select one or more 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 690

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 690

Deleting an audio group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Audio Group**.
3. Select one or more 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 navigation pane, click **Call Center** > **Audio Group**.
3. Select one or more 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 690

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 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 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 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.
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.

Holiday Table

Holiday Table List

Holiday Table List displays all the Holiday Table details under the selected Communication Manager. 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 Holiday Table List.

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

Name	Description
Number	The extension number of the holiday table Number.
Name	The name associated with the holiday table.
System	The name of the Communication Manager associated with the holiday table.

Exporting all Holiday Table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager** > **Call Center** > **Holiday Table**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. Click **More Actions** > **Export All Holiday Table**.

   The system displays the **Export Holiday Table** page.
5. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
6. Click **Export**.

Exporting selected holiday table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager** > **Call Center** > **Holiday Table**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. From the **Holiday Table List**, select the holiday table number you want to export.
5. Click **More Actions** > **Export Selected Holiday Table**.

   The system displays the **Export Holiday Table** page.
6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

Importing holiday table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager** > **Call Center** > **Holiday Table**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. Click **More Actions** > **Import Holiday Table**.

   The system displays the **Import CM Objects** page.
5. In the **Select a file** field, select the required excel file and click **Browse**.
6. Select one of the following in the **Select Error Configuration** field.

   Default value is **Continue processing other records**.

   - **Abort on first error**
   - **Continue processing other records**
7. Select one of the following in the **If a matching record already exists** field.

   Default value is **Skip**.

   - **Skip**
   - **Merge**
   - **Delete**
8. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
9. Click **Import**.

Downloading Excel Template

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager** > **Call Center** > **Holiday Table**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. Click **More Actions** > **Download Excel Template**.
5. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and click **OK**.

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 selected Communication Manager. 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.
Destination Number	Indicates the number for **Destination**.
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 navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select one or more 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 navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select one or more 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 navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select one or more 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 navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select one or more 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.

Exporting Selected Vector Directory Number

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select one or more 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 export.
6. Click **More Actions** > **Export Selected VDN**.

   The system displays the **Export VDN** page.
7. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
8. Click **Export**.

Exporting all Vector Directory Numbers

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Export All VDN**.

   The system displays the **Export VDN** page.
6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

Importing Vector Directory Numbers

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Import VDN's**.

   The system displays the **Import CM Objects** page.
6. In the **Select a file** field, select the required excel file and click **Browse**.
7. Select one of the following in the **Select Error Configuration** field.

   Default value is **Continue processing other records**.

   - **Abort on first error**
   - **Continue processing other records**
8. Select one of the following in the **If a matching record already exists** field.

   Default value is **Skip**.

   - **Skip**
   - **Merge**
   - **Delete**
9. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
10. Click **Import**.

Downloading Excel Template

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Vector Directory Number**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Download Excel Template**.
6. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and click **OK**.

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 navigation pane, click **Call Center** > **Vector Routing Table**.
3. Select one or more 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 699

Viewing Vector Routing Table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Vector Routing Table**.
3. Select one or more 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 699

Editing Vector Routing Table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Vector Routing Table**.
3. Select one or more 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 699

Deleting Vector Routing Table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Vector Routing Table**.

3. Select one or more 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 699

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.
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.

Service Hours Tables

Service Hours Table List

Service Hours Table displays all the Service Hours Table details under the selected Communication Manager. 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 Service Hours Table.

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

Name	Description
Number	The extension number of the service hours table Number.
Location	The location associated with the service hours table.
Description	The description associated with the service hours table .
System	The name of the Communication Manager associated with the service hours table.

Exporting all Service Hours Table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager** > **Call Center** > **Service Hours Tables**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. Click **More Actions** > **Export All Service Hours**.

   The system displays the **Export Service Hours Table** page.
5. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
6. Click **Export**.

Exporting selected service hours table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager** > **Call Center** > **Service Hours Tables**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. From the **Service Hours Table List**, select the service hours table number you want to export.
5. Click **More Actions** > **Export Selected Service Hours**.

   The system displays the **Export Service Hours Table** page.
6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

Importing service hours table

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager** > **Call Center** > **Service Hours Tables**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. Click **More Actions** > **Import Service Hours**.

   The system displays the **Import CM Objects** page.
5. In the **Select a file** field, select the required excel file and click **Browse**.
6. Select one of the following in the **Select Error Configuration** field.

   Default value is **Continue processing other records**.

   - **Abort on first error**
   - **Continue processing other records**
7. Select one of the following in the **If a matching record already exists** field.

   Default value is **Skip**.

   - **Skip**
   - **Merge**
   - **Delete**
8. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.

9. Click **Import**.

Downloading Excel Template

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager** > **Call Center** > **Service Hours Tables**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. Click **More Actions** > **Download Excel Template**.
5. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and click **OK**.

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.

Name	Description
Coverage Path Number	The coverage path that is being administered.
Coverage Path Description	The name for the coverage path. Accepts alphanumeric characters and must contain at least one alphabetical and one numeric character.
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 navigation pane, click **Coverage** > **Coverage Path**.
3. Select one or more 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 705

Viewing a Coverage Path

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Coverage** > **Coverage Path**.
3. Select one or more 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 705

Editing a Coverage Path

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Coverage** > **Coverage Path**.
3. Select one or more 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 705

Deleting a Coverage Path

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Coverage** > **Coverage Path**.

3. Select one or more 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 705

Exporting selected Coverage Path

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Coverage** > **Coverage Path**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In **Coverage Path List**, select the coverage path that you want to export.
6. Click **More Actions** > **Export Selected Coverage Paths**.

   The system displays the **Export Coverage Paths** page.
7. In the **Schedule Job** field, click one of the following:
   - **Run immediately**
   - **Schedule later**
8. Click **Export**.

Exporting all Coverage Paths

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Coverage** > **Coverage Path**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Export All Coverage Paths**.

   The system displays the **Export All Coverage Paths** page.
6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

Importing Coverage Paths

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Coverage** > **Coverage Path**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Import Coverage Paths**.

   The system displays the **Import CM Objects** page.
6. In the **Select a file** field, select the required excel file and click **Browse**.
7. Select one of the following in the **Select Error Configuration** field.

   Default value is **Continue processing other records**.

   - **Abort on first error**
   - **Continue processing other records**
8. Select one of the following in the **If a matching record already exists** field.

   Default value is **Skip**.

   - **Skip**
   - **Merge**
   - **Delete**
9. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
10. Click **Import**.

Downloading Excel Template

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Coverage** > **Coverage Path**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Download Excel Template**.
6. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and click **OK**.

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     Description: Admin12345
     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: 1
                All?            n               n
 DND/SAC/Goto Cover?            y               y
   Holiday Coverage?            n               n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
Point1: ________________         Point2: ________________
Point3: ________________         Point4: ________________
Point5: ________________         Point6: ________________
```

Coverage Path Number

The coverage path being administered.

Coverage path description

The name for the coverage path. Accepts alphanumeric characters and must contain at least one alphabetical and one numeric character.

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.

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.
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.

Table continues…

Valid Entry	Usage
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.

Table continues…

Name	Description
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 navigation pane, click **Coverage** > **Coverage Time-of-day**.
3. Select one or more 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 712

Viewing Coverage Time-of-day

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Coverage** > **Coverage Time-of-day**.
3. Select one or more 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 712

Editing Coverage Time-of-day

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Coverage** > **Coverage Time-of-day**.
3. Select one or more 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 712

Deleting Coverage Time-of-day

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Coverage** > **Coverage Time-of-day**.
3. Select one or more 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 712

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.

Synchronize CM Data and Configure Options / Element Cut-Through field descriptions

Synchronize CM Data/Launch Element Cut Through

Name	Description
Element Name	The name of Communication Manager.
FQDN/IP Address	The fully qualified domain name or the IP address of Communication Manager.

Table continues…

Name	Description
Last Sync Time	The time when Communication Manager was last synchronized with the Communication Manager database. On the standalone System Manager, the last synchronization time zone is that of the System Manager. On the Geographic Redundancy-enabled System Manager, the last synchronization time zone is that of the local system.
Last Translation Time	The time when the last translation of Communication Manager has been saved. The last translation time zone is always that of the Communication Manager.
Sync Type	The type of synchronization. The options are: • Initialization • Incremental
Sync Status	The status of synchronization. The options are: • Completed • In progress • Failed
Type	The type of Communication Manager.
Location	The daylight saving time displayed to set the area code for each location.
Software Version	The software version of Communication Manager.
CM Notification	The **CM Notification** is enabled or not while adding a Communication Manager system in System Manager.
CM State	The state of the Communication Manager system. The options are: • **Managed** • **Unmanaged**

Synchronize CM Data options

Name	Description
Initialize data for selected devices	Initializes the data synchronization for selected device.
Incremental Sync data for selected devices	Executes the incremental data synchronization for selected device.
Execute 'save trans all' for selected devices	Executes the command for saving all the translation for selected device.
Audit	Audits the data for selected device.

Button	Description
Now	Executes the selected action immediately.

Table continues…

Button	Description
Schedule	Displays the Job Scheduler page to schedule the data synchronization at a specific time.
Launch Element Cut Through	Displays the Element Cut Through page.
View Audit Report	Displays the Audit Report page.
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 view, edit, and delete endpoints and other 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 J129/J169/J169CC/J179/J179CC J139/J159/J189/J189CC B199 **Note:** • Communication Manager Release 8.0.1 and later internally maps the Avaya B199 Conference Phone conference phones with 9630SIP set types. • You can administer Avaya B199 Conference Phone conference phones from the System Manager user interface only.
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, K2500, CallrID, and virtual
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:

- From Release 10.2 and later, the CS1k-IP, CS1k-IPCC, CS1k-ana, CS1k-39xx, CS1k-1col, and CS1k-2col set types are not supported.
- The set types supported vary 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 navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. From **Template**, select the template based on the set type you want to add.

   The system auto populates the **Port** and **Set Type** fields.
7. In **Extensions**, perform one of the following:
   - Type the extension number.
   - Click the **Display Extension Ranges** link to select the extension number from the available extension ranges.
8. 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**, **Button Assignment**, **Profile Settings**, and **Group Membership** 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.

   Note:

   If you need to delete and add the same endpoint within seconds, for example, when running an automation script, ensure to leave a minimum of 10 second gap between deleting and adding an endpoint.

If the endpoint is deleted and added immediately without any delay, the Notify Sync feature might cause the endpoint to not display in System Manager.

Related links

New Endpoint / Template field descriptions on page 743

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 navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more 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

New Endpoint / Template field descriptions on page 743

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 navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more 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

New Endpoint / Template field descriptions on page 743

Viewing an endpoint

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more 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

New Endpoint / Template field descriptions on page 743

Deleting an endpoint

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more 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.

   Note:

   If you need to delete and add the same endpoint within seconds, for example, when running an automation script, ensure to leave a minimum of 10 second gap between deleting and adding an endpoint.

   If the endpoint is deleted and added immediately without any delay, the Notify Sync feature might cause the endpoint to not display in System Manager.

Related links

New Endpoint / Template field descriptions on page 743

Saving an endpoint as a template

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more 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 navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more 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 776

Bulk adding endpoints

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more 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 776

Deleting endpoints in bulk

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more 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 navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more 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

New Endpoint / Template field descriptions on page 743

Using Advanced Search

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more 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

New Endpoint / Template field descriptions on page 743

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 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 one or more 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

New Endpoint / Template field descriptions on page 743

Releasing endpoints

About this task

Important:

This maintenance operation is service affecting.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the Endpoint List section, select one or more endpoint, and click **Maintenance** > **Release Endpoint**.

   System Manager displays the Release Endpoint Confirmation page.
6. Click **Now** to release the endpoints immediately or do one of the following:
   - Click **Schedule** to perform the release at a specified time.
   - Click **Cancel** to cancel the release.

   System Manager displays the result of the release operation on the Release Endpoint Report page.

Related links

New Endpoint / Template field descriptions on page 743
Error codes on page 777

Busy out endpoints

About this task

Important:

This maintenance operation is service affecting.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the Endpoint List section, select one or more endpoint, and click **Maintenance** > **Busyout Endpoint**.

   System Manager displays the Busyout Endpoint Confirmation page.
6. Click **Now** to busy out the endpoints immediately or do one of the following:
   - Click **Schedule** to perform the busy out at a specified time.
   - Click **Cancel** to cancel the busy out.

   System Manager displays the result of the busy out operation on the Busyout Endpoint Report page.

Related links

New Endpoint / Template field descriptions on page 743
Error codes on page 777

Testing endpoints

About this task

Important:

This maintenance operation is service affecting.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the Endpoint List section, select one or more endpoint, and click **Maintenance** > **Test Endpoint**.

   System Manager displays the Test Endpoint Confirmation page.

6. Click **Now** to test the endpoints immediately or do one of the following:
   - Click **Schedule** to test the endpoints at a specified time.
   - Click **Cancel** to cancel the test operation.

   System Manager displays the test result and error code of the endpoint on the **Test Endpoint Report** page. You can click the **Error Code Description** link to view the error details.

Related links

New Endpoint / Template field descriptions on page 743
Error codes on page 777

Using Clear AMW All

About this task

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 navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the Endpoint List section, select one or more endpoint, and click **Maintenance** > **Clear AMW All**.

   System Manager displays the Clear AMW All Confirmation page.
6. 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.

   System Manager displays a confirmation that the command is completed and returns you to the Manage Endpoints page.

   To view the job status and to view log for any errors associated with the job, go to the **Services** > **Scheduler** page.

Performing list trace station

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.

2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the Endpoint List section, select an endpoint, and click **Maintenance** > **List Trace Station**.

   When you select the endpoint that is on the standalone Communication Manager, System Manager displays the list trace station command for the selected endpoint on the Element Cut Through screen.

Viewing endpoint status

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the Endpoint List section, select an endpoint, and click **Maintenance** > **Status**.

   When you select the endpoint that is on the standalone Communication Manager, System Manager displays the status for the selected endpoint.

Related links

New Endpoint / Template field descriptions on page 743
Error codes on page 777

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 navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more 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 777
New Endpoint / Template field descriptions on page 743

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.
Tenant Number	The tenant number 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.

Exporting selected endpoints

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.

3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In **Endpoint List**, select the endpoint that you want to export.
6. Click **More Actions** > **Export Selected Endpoints**.

   The system displays the **Export Endpoints** page.
7. In the **Schedule Job** field, click one of the following:
   - **Run immediately**
   - **Schedule later**
8. Click **Export**.

Exporting all endpoints

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Export All Endpoints**.

   The system displays the **Export All Endpoints** page.
6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

Importing endpoints

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Import Endpoints**.

   The system displays the **Import CM Objects** page.
6. In the **Select a file** field, select the required excel file and click **Browse**.
7. Select one of the following in the **Select Error Configuration** field.

Default value is **Continue processing other records**.

- **Abort on first error**
- **Continue processing other records**

8. Select one of the following in the **If a matching record already exists** field.

   Default value is **Skip**.

   - **Skip**
   - **Merge**
   - **Delete**

9. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
10. Click **Import**.

Downloading Excel Template

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Download Excel Template**.
6. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and then click **OK**.

Migration of J1xx endpoints configured as 96x1 SIP set type

If a J-Series endpoint is configured as 96x1 SIP set type on Communication Manager, then from System Manager Release 8.1.3, you can migrate that to J1xx set type. To migrate the set type:

- System Manager and Session Manager must be on Release 8.1.3 and later.
- Communication Manager must be on Release 8.x and later.
- J1xx phone must be on Release 4.0.6.0 and later. It must be registered at least once to Session Manager Release 8.1.3 and later.

Criteria for migrating 96x1 SIP set type to J1xx set type

If **Current Set Type** configured on Communication Manager is one of the non-Contact Center set types 9608SIP, 9611SIP, 9621SIP, 9641SIP or Contact Center set types 9608SIPCC, 9611SIPCC, 9621SIPCC, 9641SIPCC, or ALIAS of any of these set types, and if a user has one of the following, System Manager marks an endpoint eligible.

- One device connected of type J129, J139, J159, J169, J179, or J189.
- More than one devices connected and has at least one device of type J129, J139, J159, J169, J179, or J189.

When an endpoint is eligible for migration, you can migrate the endpoint to specific Set type(s).

1. If **Current Set Type** configured on Communication Manager is one of the non-Contact Center set types 9608SIP, 9611SIP, 9621SIP, or 9641SIP, then you can migrate to the endpoint as described in the following table.

Set type	Migrate to
J129	J129
J139	J179
J159	J179
J169	J169
J179	J179
J189	J179

   For multiple connected devices, System Manager always displays J179 as the preferred set type in the list of allowed set type for migration.

2. If **Current Set Type** configured on Communication Manager is one of the Contact Center set types 9608SIPCC, 9611SIPCC, 9621SIPCC, or 9641SIPCC, then migrate to the endpoint as described in the following table.

Set type	Migrate to
J129	J179CC
J139	J179CC
J159	J179CC
J169	J169CC
J179	J179CC
J189	J179CC

   For multiple connected devices, System Manager always displays J179CC as the preferred set type in the list of allowed set type for migration.

Discover 96x1 SIP set type ready for J1xx migration

You can discover the endpoints that are ready for J1xx migration by enabling the **Discover Endpoints Eligible for Migration** job on the **Services** > **Scheduler** > **Pending Jobs** page.

By default, the **Discover Endpoints Eligible for Migration** job is disabled. You cannot edit and perform **Schedule Job On Demand** settings for this job.

When the **Discover Endpoints Eligible for Migration** job is executed, System Manager:

- Processes all endpoints on all Communication Managers that have a user associated on the **Users** > **User Management** > **Manage Users** page.

  For information about the J1xx migration criteria, see “Criteria for migrating 96x1 SIP set type to J1xx set type”.

- Marks the endpoint as **Migration Eligible** on the **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints** page, if it meets the current and connected set type criteria.

Note:

System Manager automatically disables the discovery job details after 31 days. If required, the administrator can enable the discovery job again.

Once the **Discover Endpoints Eligible for Migration** job is executed at least once, you can perform an advanced search to see the list of endpoints that are ready for migration.

If any new user is added in System Manager that meets migration criteria, then System Manager processes the endpoint in the next execution of discover job.

Related links

Searching for 96x1 SIP set type for J1xx endpoint migration by using advanced search on page 734

Enabling the Discover Endpoint eligible for migration job

Procedure

1. On the System Manager web console, click **Services** > **Scheduler** > **Pending Jobs**.
2. In the Job List section, select the **Discover Endpoints Eligible for Migration** job, and click **Enable**.
3. On the Enable Confirmation page, click **Continue**.

   After enabling the **Discover Endpoints Eligible for Migration** job, it executes daily at 1 A.M according to the System Manager server timezone and continues for 31 days. Once the job completes for consecutive 31 days, System Manager disables the job automatically.

Searching for 96x1 SIP set type for J1xx endpoint migration by using advanced search

About this task

On the Manage Endpoint page, System Manager displays the list of endpoints eligible for migration that were discovered in its last run of the **Discover Endpoints Eligible for Migration** job.

Note:

If some endpoints have already been migrated to J-Series phones, System Manager does not display those endpoints.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.

4. Click **Show List**.
5. In the **Endpoint List** section, click **Advanced Search**.
6. In the Criteria section, do the following:
   a. From the first drop-down field, select the search criterion **Endpoint General**.
   b. From the second drop-down field, select the operator **Migration Eligible**.
   c. From the third drop-down field, select the operator **true**.

      The options are:

      - **true**
      - **false**

      By default, the value of **Migration Eligible** is set to **false**.

   If you want to add a search condition, click the plus sign (**+**) and select the new criteria as required.

   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**.

   System Manager displays the endpoints that meet the search criteria in the Endpoint List section.

Related links

Discover 96x1 SIP set type ready for J1xx migration on page 733

Migrating set type of selected J1xx endpoint from 96x1 SIP to J1xx set type

About this task

If a station is configured on Communication Manager with set types 9608SIP, 9611SIP, 9621SIP, 9641SIP, 9608SIPCC, 9611SIPCC, 9621SIPCC, or 9641SIPCC and if there are one or more J-Series phone with type J129, J139, J159, J169, J179, then you must change the set type on Communication Manager or migrate set type to any of the J129, J169, J179, J169CC, J179CC set types.

Note:

- If there are multiple set types, it is recommended to choose a set type that has more feature capabilities. If you select a set type that has lesser feature capabilities, it can result in loss of functionality on that endpoint after the migration.
- For Contact Center set types, select the Contact Center set-type only.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.

4. Click **Show List**.
5. Search for endpoints ready for migration by using **Advanced Search**.

   For information, see “Searching for 96x1 SIP set type for J1xx endpoint migration by using advanced search”.
6. Select one or more endpoint, click **More Actions** > **Migrate Selected Endpoints**.

   System Manager displays the Endpoint Migration page.

   Depending on the number of connected devices, System Manager displays the 96x1 endpoints that are ready for migration either on the **Same Set-type(s)** tab or on the **Different Set-types** tab.
7. To migrate endpoints that are available on the **Same Set-type(s)** tab, in the Migrate Endpoint List section, do the following:
   a. Select one or more endpoints.
   b. Click **Create New Job**.
8. To migrate endpoints that are available on the **Different Set-types** tab, in the Migrate Endpoint List section, do the following:
   a. Do one of the following:
      - Select one or more endpoint, and select the set type you want to migrate to in the **Set Type After Migration** column.

        Based on **Connected Set Type**, System Manager displays the values in the **Set Type After Migration** column.

        For more information, see the “96x1 endpoint to J100-Series migration criteria” section.
      - Select one or more endpoint, select the **Default for Set Type After Migration** check box, and then select the default set type you want to migrate to from the drop-down list.

        Note:

        - If you select the default set type option and also select a value in the **Set Type After Migration** column for one or more endpoints, then System Manager gives precedence to the **Set Type After Migration** column value for migrating the endpoints where the value is provided and migrates all other endpoints to the default set type.
        - If the selected default set type is not applicable for one or more endpoints, then migration of those endpoints fail.
   b. Click **Create New Job**.
9. On the Migrate Endpoints page, in the Schedule section, perform one of the following:
   - Select **Run immediately** to execute the job now.
   - Select **Schedule later** to execute the job at a later time.

10. Click **Migrate Endpoints**.

    System Manager displays the job status on the:

    - **Services** > **Scheduler** > **Completed Jobs** page.
    - **Endpoint Migration Job History** tab.

Related links

Criteria for migrating 96x1 SIP set type to J1xx set type on page 732
Enabling the Discover Endpoint eligible for migration job on page 734
Searching for 96x1 SIP set type for J1xx endpoint migration by using advanced search on page 734
Endpoint Migration field descriptions on page 740

Migrating set type of all J1xx endpoint from 96x1 SIP to J1xx set type

About this task

If a station is configured on Communication Manager with set types 9608SIP, 9611SIP, 9621SIP, 9641SIP, 9608SIPCC, 9611SIPCC, 9621SIPCC, or 9641SIPCC and if there are one or more J-Series phone with type J129, J139, J159, J169, J179, then you must change the set type on Communication Manager or migrate set type to any of the J129, J169, J179, J169CC, J179CC set types.

Note:

- If there are multiple set types, it is recommended to choose a set type that has more feature capabilities. If you select a set type that has lesser feature capabilities, it can result in loss of functionality on that endpoint after the migration.
- For Contact Center set types, select the Contact Center set-type only.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Migrate All Endpoints Ready for Migration**.

   System Manager displays the Endpoint Migration page.

   Depending on the number of connected devices, System Manager displays the 96x1 endpoints that are ready for migration either on the **Same Set-type(s)** tab or on the **Different Set-types** tab.
6. To migrate endpoints that are available on the **Same Set-type(s)** tab, in the Migrate Endpoint List section, do the following:

   a. Select one or more endpoints.

b. Click **Create New Job**.

7. To migrate endpoints that are available on the **Different Set-types** tab, in the Migrate Endpoint List section, do the following:

   a. Do one of the following:

      - Select one or more endpoint, and select the set type you want to migrate to in the **Set Type After Migration** column.

        Based on **Connected Set Type**, System Manager displays the values in the **Set Type After Migration** column.

        For more information, see the “96x1 endpoint to J100-Series migration criteria” section.

      - Select one or more endpoint, select the **Default for Set Type After Migration** check box, and then select the default set type you want to migrate to from the drop-down list.

        Note:

        - If you select the default set type option and also select a value in the **Set Type After Migration** column for one or more endpoints, then System Manager gives precedence to the **Set Type After Migration** column value for migrating the endpoints where the value is provided and migrates all other endpoints to the default set type.
        - If the selected default set type is not applicable for one or more endpoints, then migration of those endpoints fail.

   b. Click **Create New Job**.

8. On the Migrate Endpoints page, in the Schedule section, perform one of the following:

   - Select **Run immediately** to execute the job now.
   - Select **Schedule later** to execute the job at a later time.

9. Click **Migrate Endpoints**.

   System Manager displays the job status on the:

   - **Services** > **Scheduler** > **Completed Jobs** page.
   - **Endpoint Migration Job History** tab.

Related links

Criteria for migrating 96x1 SIP set type to J1xx set type on page 732
Enabling the Discover Endpoint eligible for migration job on page 734
Endpoint Migration field descriptions on page 740

Viewing endpoint migration job history

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.

2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Perform one of the following:
   - Select an eligible endpoint and click **More Actions** > **Migrate Selected Endpoints**.
   - Click **More Actions** > **Migrate All Endpoints Ready for Migration**.

   System Manager displays the Endpoint Migration page.
6. Click **Endpoint Migration Job History**.
7. Select a job and click **View Job Details**.

   System Manager displays the Endpoint Migration Job Details page with the number of successfully migrated endpoints and list of endpoints that have failed during migration. In the Endpoints Failed List section, you can view the failed endpoint and its cause of failure.

Cancelling an endpoint migration job

About this task

You can cancel only one job at a time.

Before you begin

Ensure that the job is in the **RUNNING** state.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Perform one of the following:
   - Select an eligible endpoint and click **More Actions** > **Migrate Selected Endpoints**.
   - Click **More Actions** > **Migrate All Endpoints Ready for Migration**.

   System Manager displays the Endpoint Migration page.
6. Click **Endpoint Migration Job History**.
7. In the Endpoint Migration Job History section, select a job, and click **Cancel Job**.

   System Manager displays the confirmation message.
8. Click **OK**.

   System Manager cancels the selected job.

Deleting endpoint migration job

About this task

If the job is in the **RUNNING** state, you cannot delete that job.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Perform one of the following:
   - Select an eligible endpoint and click **More Actions** > **Migrate Selected Endpoints**.
   - Click **More Actions** > **Migrate All Endpoints Ready for Migration**.

   System Manager displays the Endpoint Migration page.
6. Click **Endpoint Migration Job History**.
7. In the Endpoint Migration Job History section, select a job, and click **Delete Job**.

   System Manager displays the confirmation message.
8. Click **OK**.

   System Manager deletes the selected job.

Endpoint Migration field descriptions

Name	Description
Same Set-type(s)	Displays the list of endpoints that are connected to the same set type. • If a user has one device connected, then System Manager displays it under **Same Set-type(s)**. • If a user has more than one device connected and all are of the same type, then System Manager categorizes the devices as the same set type and displays under **Same Set-type(s)**.
Different Set-types	Displays the list of endpoints that are connected to different set types. If a user has more than one device connected and has different combinations of set types, then System Manager displays the device under **Different Set-types**.
Endpoint Migration Job History	Displays the history of endpoint migration jobs.

Migrate Endpoint List

The Migrate Endpoint List section displays all endpoints that are ready for migration. You can apply filters and sort each of the columns.

Name	Description
Default for Set Type After Migration	The default set type you want to migrate to. The options are: • **J129** • **J139** • **J159** • **J169** • **J179** • **J189** • **J189CC** • **J169CC** • **J179CC** **Note:** If the selected default type is not available in the **Set Type After Migration** column for an endpoint, then the migration fails.
Name	The name of the endpoint.
Extension	The extension of the endpoint.
Current Set Type	The current set type of the endpoint that is configured on Communication Manager.
Connected Set Type	The connected set type of the endpoint.
Set Type After Migration	The set type after migration of the endpoint. Based on **Connected Set Type**, System Manager displays the values in the **Set Type After Migration** column. **Note:** You must select a set type that has more capabilities in the **Set Type After Migration** column. If you select a set type that has lesser capabilities, it can result in loss of functionality on that endpoint after the migration.
User	The user to which the endpoint is associated.
Tenant Number	The tenant number to which the endpoint is associated.
System	The Communication Manager name of the endpoint.

Button	Description
Create New Job	Displays the Migrate Endpoints page to schedule the endpoint migration job immediately or at a later time.
Cancel	Cancels the changes and returns to the Manage Endpoints page.

Endpoint Migration Job History field descriptions

Name	Description
Start Time	The date and time the job is scheduled to start.
End Time	The date and time the job execution completes.
Status	The status of the job can be: • **SUCCESSFUL**: When the endpoint migration job is successfully completed. • **FAILED**: When the endpoint migration job is failed. • **PARTIAL_FAILURE**: When the endpoint migration job partially fails. • **INTERRUPTED**: When the endpoint migration job is canceled. • **RUNNING**: When the endpoint migration job is in progress. • **PENDING_EXECUTION**: When the endpoint migration job is scheduled.
Job Name	The job name as displayed on the Scheduler page.
Scheduled By	The name of user who created the job
Total Scheduled	The total number of records scheduled for migration.
Processed*	The total number of processed records.
Successful	The total number of successful records.
Failed	The total number of failed records.
Not Processed*	The total number of unprocessed records.

Note:

*: These fields are available only on the Endpoint Migration Job Details page.

Button	Description
View Job Details	Displays the Endpoint Migration Job Details page with the number of successfully migrated endpoints and list of endpoints that have failed during migration.
Cancel Job	Cancels one job at a time. The job must be in the **RUNNING** state.
Delete Job	Deletes one or more job. You cannot delete the job that is in the **RUNNING** state.

Endpoint Migration Job Details: Endpoints Failed List

Name	Description
Extension	The extension of the failed endpoint.
CM Name	The Communication Manager name of the endpoint.
Error Message	The cause of failure.

Add Endpoint Template

New 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	Communication Manager to which the endpoint is assigned.
Template	Template 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. With blank, an incoming call to the virtual extension can be redirected to the virtual extension “busy” or “all” coverage path.

The extension length must be within 16 digits.

Port

The Auxiliary and Analog ports assigned to the station are as follows.

Valid Entry	Usage
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 999. • 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

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 sixteen 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.

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.

Primary Session Manager, Secondary Session Manager, Third Session Manager, and Fourth Session Manager

These four fields are populated by System Manager and are read-only on Communication Manager. You cannot modify these fields from the Communication Manager SAT interface.

If the call to this SIP station is routed to a SIP trunk with a clustered signaling group, then the SIP Trunk Optimization feature sends the Invite to the station on the primary Session Manager. If primary Session Manager is not reachable, the Invite is sent to the secondary Session Manager.

The Session Manager selection for routing to a SIP station does not apply to a call between two SIP stations. In this case, Session Manager decides the destination Session Manager for the called SIP station.

Note:

IP addresses are allocated to these fields, when the policy-based assignment is enabled in System Manager.

System ID

This field can be configured for CS 1000 station types only. This field allows you to leave the field blank or enter a string of up to 9 characters. With Release 8.0 and later, more than one station can use the combination of **System ID** and **Terminal Number**.

With Release 8.0.1 and later, each station must have a unique combination of **System ID** and **Terminal Number**.

Terminal Number

This field can be configured for CS 1000 station types only. You can enter numbers in the following range: 0.0.0.0 to 252.1.15.31.

The first digit must be divisible by 4. For example: 0, 4, 8, …, 252.

Attendant

When you select the 9641SIP template type from **Template**, the system enables the **Attendant** check box. If you select this check box, you can administer the endpoint as an attendant.

When you select the **Attendant** check box, the system disables the **Feature Options** and **Group Membership** tabs.

Feature Options

With Features Options, you can 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*.) 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*.
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.
sip-adjunct	Used to audit message waiting lamps.
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."

Table continues…

Valid Entries	Usage
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, 9600-series telephones (Avaya one-X Deskphone Edition SIP R2 or later), and Avaya J100 Series IP Phones 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

Map-to Station

The extension of a physical telephone used for calls to a virtual extension. Cannot be used with an xmobile, xdid or any other virtual extension.

This field is applicable only for the virtual endpoints.

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 Soft Phone 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 LLC 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.

Table continues…

Valid Entry	Usage
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 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.

Bridging Tone for This Extension

Allows you to enable or disable a single burst of tone when a station bridges on to the principal's call.

Valid Entry	Usage
y	Enables a single burst of tone when a station bridges on to the principal's call.
n	Disables a single burst of tone when a station bridges on to the principal's call. This is the default value for a new SIP station, or when a SIP station upgrades to Communication Manager 8.0 or later from a previous release.

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 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.

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.

Table continues…

Valid Entries	Usage
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 for H.323 and SIP station types.

Valid entry	Usage
0 to 999 blank	The Group ID number for the station.

Configuration of IP Phone Group ID on SIP Devices

You can configure the **IP Phone Group ID** field for SIP endpoints on:

- System Manager web console by using one of the following pages:
  - **Elements** > **Communication Manager** > **Endpoints** > **New** > **Manage Endpoints** > **Feature Options**.
  - **User Management** > **Manage Users** > **New** > **Communication Profile** > **CM Endpoint Profile** > **Extension Editor** > **Feature Options**.
  - **Elements** > **Communication Manager** > **Element Cut-Through**.
- Communication Manager SAT, using the `add station` command on page 3 of the Station form.
- Endpoint using the **Group** field.

Note:

If you manually set the **Group** field on the endpoint to a value other than 0, then the group setting on the endpoint precedes the **IP Phone Group ID** setting on the System Manager web console or Communication Manager station form.

If you manually set the **IP Phone Group ID** field on the System Manager web console or Communication Manager station form to value 0, then the **Group** field setting on the endpoint precedes the **IP Phone Group ID** setting.

If the assigned group ID is not defined as the **Terminal Group Number** on the **Elements** > **Session Manager** > **Device and Location Configuration** > **Device Settings Group** page, the system applies the **Default Group** settings that are defined on the **Elements** > **Session Manager** > **Device and Location Configuration** > **Device Settings Group** page.

For administering **Terminal Group Number**, see *Administering Avaya Aura® Session Manager*.

Configuring the IP Phone Group ID for an endpoint

About this task

Use one of the following procedures to configure the **IP Phone Group ID** field on the System Manager web console.

- Click **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**, and perform the following:
  1. Click **New**.

     The system displays the New Endpoint page.
  2. In the **Template** field, select the required template.
  3. In the **Extension** field, type the extension number.
  4. On the **Feature Options** tab, in the **IP Phone Group ID** field, type the group ID for the endpoint.

     When you change the group ID of the endpoint, the system displays the following message:

     ```
     Changes to this field may result in some or all the users of
     Avaya SIP phones to reboot once they are not involved in a SIP
     call or in other important functions.
     ```
  5. Click **Commit** to save the changes.
- Click **User Management** > **Manage Users**, and perform the following:
  1. Click **New**.

     The system displays the User Profile | Add page.
  2. On the **Identity** tab, fill the required details.
  3. On the **Communication Profile** tab, in PROFILES, click **CM Endpoint Profile**.
  4. In the **System** field, select the Communication Manager system.
  5. In the **Profile Type** field, select **Endpoint**.
  6. In the **Extension** field, type the extension number, and then click the **Editor** button next to the given extension number.

System Manager displays the Edit Endpoint window.

7. In the **Template** field, select the required endpoint template.
8. On the **Feature Options** tab, in the **IP Phone Group ID** field, type the group ID for the endpoint.

   When you change the group ID of the endpoint, the system displays the following message:

   ```
   Changes to this field may result in some or all the users of
   Avaya SIP phones to reboot once they are not involved in a SIP
   call or in other important functions.
   ```

9. Click **Commit** to save the changes.

Next steps

Configure the **Terminal Group Number** field on the **Elements** > **Session Manager** > **Device and Location Configuration** > **Device Settings Group** page.

For administering **Terminal Group Number**, see *Administering Avaya Aura® Session Manager*.

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

Audible Message Waiting field 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

Auto Select Any Idle Appearance field 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.

Note:

This field has no impact on a SIP station (OPS) on shuffling. For SIP stations, this field is controlled by the "Direct IP-IP Audio Connections" field in the Signaling group form.

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.

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

This field can be configured when the set type is XMOBILE. 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.

IP Hoteling

When you enable the **(SA8520) - Hoteling Application for IP Terminals** field using the **`change system-parameters special-applications`** command on Communication Manager, the system displays the **IP Hoteling** field for that extension.

Avaya supports this application with DCP digital terminals but not with IP terminals. Using this feature, you can reassign the extension number for a registered IP telephone.

For more information, see *Avaya Aura® Communication Manager Special Application Features*.

Increase Paging Group Members

When you enable or disable the **(SA9096) - Increase Paging Group Members** field on the special application form, you need to perform the Initialization sync (INIT sync). This action ensures that all changes made in Communication Manager are applied in the group-page form in System Manager as well.

If you do not do an INIT sync, there might be inconsistencies between Communication Manager and System Manager in the group-page form.

For more information, see *Avaya Aura® Communication Manager Special Application Features*.

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

Name	Description
M**usic 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.
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

On the Manage Endpoints page, under the **Button Assignment** tab, the system displays the following tabs based on the **Set Type** selection:

- **Main Buttons**
- **Feature Buttons**
- **Buttons Modules**
- **Phone View**

Note:

With System Manager Release 8.1.1, the **Phone View** tab is displayed for SIP Endpoints.

You can assign features to the buttons on a phone. To assign the main buttons for your endpoint, choose an option from the list for each button.

Note:

On the Manage Endpoint page, when you select the CS 1000 station type and specific set from the **Set** field, System Manager enables or disables the options on **Button Assignment** according to the selected set of the CS 1000 station type.

Field descriptions

Endpoint Configurations:

The Favorite Button and Button Label configurations are available on the 9608, 9611, 9621, 9641 SIP, 96x1SIPCC, J-Series, and CS 1000 endpoints.

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:** On the 96x1 SIP endpoints, you can set up to nine buttons as favorites, which includes the configured contacts. On the J-Series endpoints, you can configure as many favorite buttons as you want to set. The **Favorite** button is disabled for the **call-appr** and **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 **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 Number on Phone	The button number that is available on the phone.
Button Number Administered in CM	The button number that is administered on Communication Manager.

Table continues…

Name	Description
Button Feature or **Feature**	The button feature that is available on the phone.
Argument	The argument for the button feature that is available on the phone.

Note:

From release 10.2, System Manager supports Send-NN and Q-call for J-series SIP phones by default.

Phone view layout of SIP Endpoints

With System Manager Release 8.1.1, you can view the read-only phone view layout of SIP Endpoints when the SIP endpoint is registered with Session Manager.

The **Phone View** tab displays the data based on the **Set Type** configuration on the Manage Endpoints page. It is supported only for the following SIP endpoints: J1xx, 96x1 SIP, and 96x0 SIP set types.

The tabular layout of feature buttons is based on the key number ordering of the endpoint.

If the endpoint supports the following two button types, the **Phone View** tab also displays the data about these buttons if they are configured.

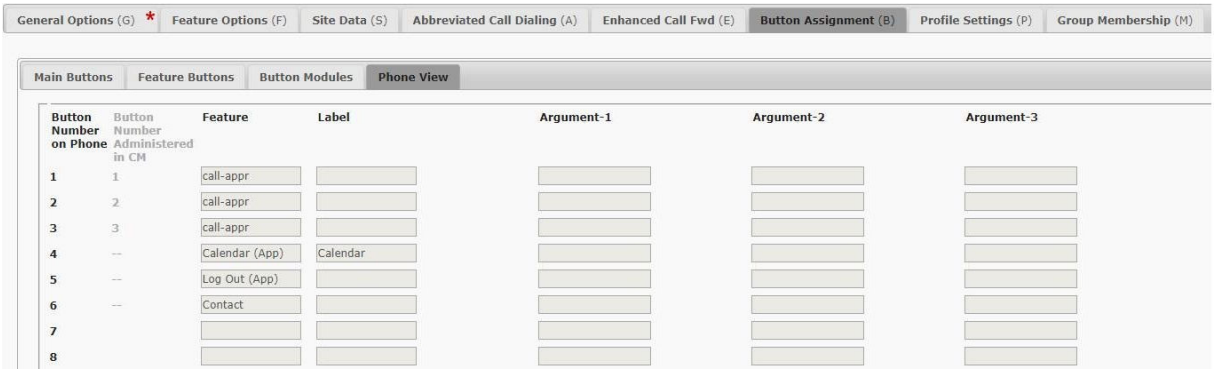
- Contact name on the endpoint then text **Contact** is displayed on phone view instead of the actual contact name available in the customize key on the endpoint.

  Example: If the key layout customization contains Calendar, its App on the endpoint, then on the **Phone View** tab, the value is displayed as **Calendar (App)**.

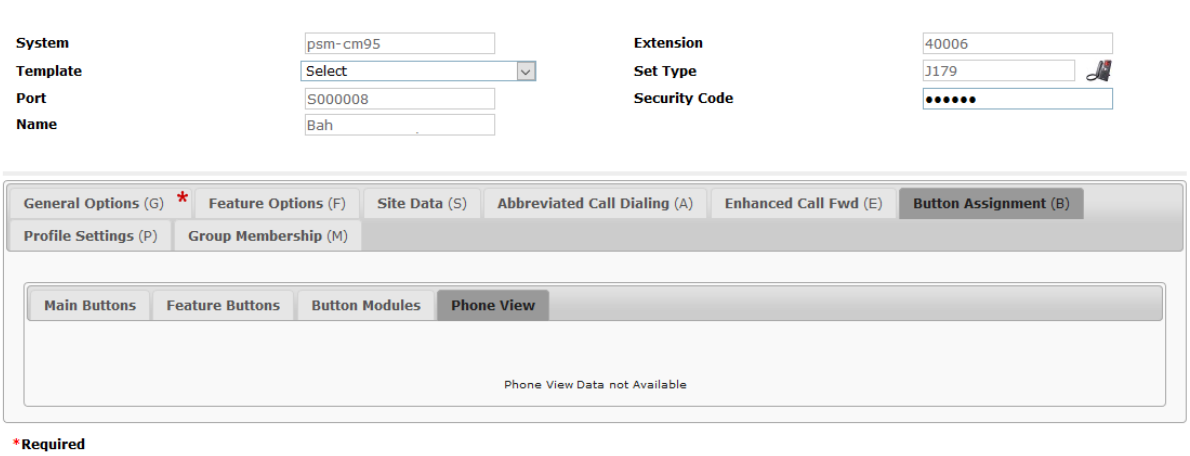
- App (Application) on the endpoint then **App** is appended to key layout customization while displaying on the phone view.

Endpoints that support key layout customization

- If the endpoints support the key layout customization, then the phone key numbering is displayed on **Phone View** as customized by the user on the endpoint.



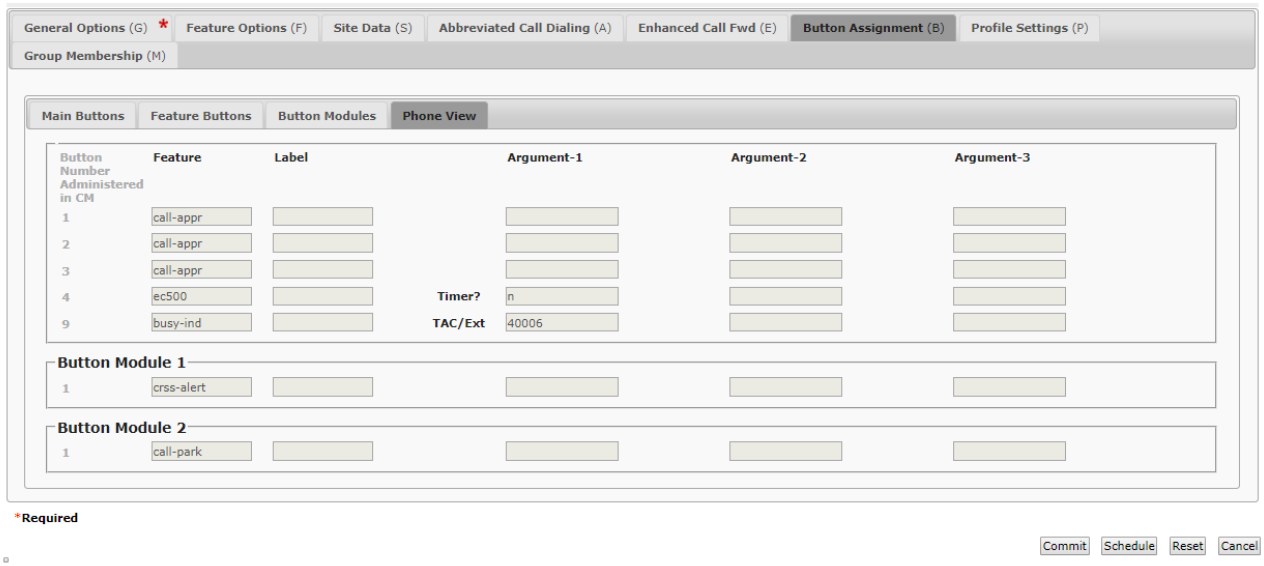
- If the endpoint is not registered with Session Manager or data is not available with Session Manager, then the system displays the message: `Phone View Data not Available`



Endpoints that do not support key layout customization

If the endpoints do not support the key layout customization, then the phone key numbering is displayed as administered on Communication Manager.

Examples of endpoints that do not support the key layout customization are: J129, J139, J159, J189, J189CC, 9641SIP, and 9641SIPCC.



Endpoint display mode

The phone can be set to use either the full screen width (single-column mode) or just a half-width (dual-column mode) for each programmable appearance and feature button.

Full screen width (single-column mode)

Each programmed button feature occupies the full width of the screen. The physical buttons on both sides of the display are used to control the button feature. However, the button status is only shown by the left-hand button. In this mode, appearance button labels also show a call status icon (for example: idle, alerting, connected).

Following is an example of endpoint display mode in full screen width.

The number in the following example corresponds to the **Button Number on Phone** column on the **Phone View** tab of the Add/Edit Endpoint page.

```
1
2
3
4
5
.
.
.
<n>
```

The number in the following table corresponds to the **Button Number on Phone** column on the **Phone View** tab of the Endpoint page.

Half-width (dual-column mode)

Each programmed button occupies one half of the screen line on which it is displayed, either the right-hand or left-hand side. The adjacent physical button on that side of the display is used to indicate the button's status and to control the button feature.

Following is an example of endpoint display mode in half-width screen.

The number in the following example corresponds to the **Button Number on Phone** column on the **Phone View** tab of the Add/Edit Endpoint page.

```
1                                                       2
3                                                       4
5                                                       6
7                                                       8
.                                                       .
.                                                       .
.                                                       <n>
```

Profile settings field descriptions

Note:

Profile Settings is available for the 9608, 9611, 9621, 9641 SIP, 96x1SIPCC, J-Series, and CS 1000 endpoints.

Profile Settings work when the endpoint is associated with 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**

Table continues…

Name	Description
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.
Dialing 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 Signaling	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.
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 in 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.

Table continues…

Name	Description
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 ringtone for an incoming call. The options are: • Classic Tone, with 8 options • Cheerful • Chimes • Telephone Bell • Xylophone • Drum Beat • Shimmer **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. Sometimes, 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** > **Session Manager** link.
Call Pickup Indication	The option to set ringtones 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.

Table continues…

Name	Description
Show Quick Touch Panel	The options to display **Quick Touch Panel** 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. This field is available for 9621 and 9641 SIP and SIPCC set types of endpoints.

Language & Region

Name	Description
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 • Italian • Dutch • Russian • Traditional Chinese • Chinese • Japanese • Korean • Arabic • Polish • Turkish • Thai **Note:** For these specific languages, only the following set types are supported: • Arabic: 9621SIP, 9621SIPCC, 9641SIP, 9641SIPCC, CS1kIP, CS1k39xx, CS1k1col, CS1k2col, CS1kIPCC, CS1kana, J129, J139, J159, J169, J179, J189, J169CC, J179CC, and J189CC. • Polish, Turkish: J129, J139, J159, J169, J169CC, J179, J179CC, J189, and J189CC. • Thai: J139, J159, J169, J169CC, J179, J179CC, J189, and J189CC. From Release 8.1.3.7, System Manager supports the display of the “custom” language string if you configure the custom language on the endpoint. The custom language is pushed from the endpoint to System Manager through Session Manager. You can view the custom language

Table continues…

Name	Description
	with an asterisk (*) in the **User Preferred Language** drop-down field on the **Manage Endpoint** > **Profile Settings** page. User import or export operations will also support the “custom” language string. While editing the endpoint, if you change the custom language to any other language, you cannot revert your changes to the custom language from the System Manager web console. When you add a new endpoint or user through the System Manager web console, System Manager will continue to support the current set of language options only.
Time Format	The option to configure the time format to be displayed on the phone screen. The options are: • **12 Hour** • **24 Hour**

Advance Options Presence integration

Name	Description
Away Timer	The option to enable the automatic away timer for presence indication. The options are: • **On** • **Off**
Away Timer Value	The option to specify a value for the automatic **Away Timer**. For releases earlier than 8.1.3.5, the values are from 5 minutes through to 480 minutes. From Release 8.1.3.5 and later, the values are from 5 minutes through to 999 minutes.

Support of common parameter across endpoint template

With Release 8.1.1, when you create a SIP endpoint, the system retains the common parameter information so that when you log in to SIP endpoints of the same type or of another type, all your SIP endpoints are able to retrieve and update any of the common parameters they utilize.

The following common parameters are available on the **Profile Settings** tab on the **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints** page of System Manager web console.

- **Audio Path**
- **Away Timer**
- **Away Timer Value**
- **Background Logo**

- **Button Clicks**
- **Call Pickup Indication**
- **Dialing Option**
- **Headset Signaling**
- **Personalized Ringing**
- **Phone Screen**
- **Phone Screen on Calling**
- **Redial**
- **Show Quick Touch Panel**
- **Time Format**
- **User Preferred Language**

The following common parameters are available on the **Button Assignment** tab on the **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints** page of System Manager web console.

- **Favorite**
- **Button Label**

Note:

- When you make changes to a common parameter from System Manager, the system gives precedence to that value as System Manager values are from a well-defined common parameter range. But when you make changes to a common parameter from an endpoint, the system gives precedence to that value only if the value is from the well-defined common parameter range. If the value is not from the well-defined common parameter range, then the value is only stored for that device family and the common value for that parameter is not changed.
- Family-specific data is not changed.

If you have more than one SIP endpoint type, the following parameters are synchronized across all your SIP endpoints, which support these parameters according to the following table.

Common parameters	1XC Model: n/a	96x0 Model: 96xx	96x1 Model : 96x1	J1x9 Model: J100	ADA Model: CS1k-xxx	Equinox Model: AvayaClient Services	Vantage Model: K1xx	H Series Model: H1xx, H175
Audio Path	Y	Y	Y	Y				Y
Away Timer			Y	Y				
Away Timer Value			Y	Y				
Background Logo	Y	Y	Y					

Table continues…

Common parameters	1XC Model: n/a	96x0 Model: 96xx	96x1 Model : 96x1	J1x9 Model: J100	ADA Model: CS1k-xxx	Equinox Model: AvayaClient Services	Vantage Model: K1xx	H Series Model: H1xx, H175
Button Clicks		Y	Y	Y			Y	Y
Call Pickup Indication	Y		Y	Y				Y
Dialing Option		Y	Y	Y				Y
Favorite	Y	Y	Y	Y				
Headset Signaling			Y	Y			Y	Y
Button Label	Y	Y	Y	Y	Y	Y		
Personalized Ringing			Y	Y				Y
Phone Screen			Y	Y				
Phone Screen on Calling		Y	Y					
Redial			Y	Y				Y
Show Quick Touch Panel		Y	Y					
Time Format			Y	Y			Y	Y
User Preferred Language		Y	Y	Y			Y	Y

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 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*.

Table continues…

Type	Description
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	Returns 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.

Table continues…

Button	Description
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

The following table lists only the common error codes for Busyout, Release, Test, and Reset commands lists.

In addition to these, many maintenance objects have other unique error codes. For information about the applicable maintenance object, see *Avaya Aura® Communication Manager Alarms, Events, and Logs Reference*.

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 synchronization`** 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.

Table continues…

Error code	Command result	Description/Recommendation
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 Maintenance/Test, Announcement circuit packs MC Call Classifier, Tone Detector, or Speech Synthesis circuit packs. Each of these circuit packs has restrictions on 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	For information about the applicable maintenance object from the **Maintenance Name** field, see *Avaya Aura® Communication Manager Alarms, Events, and Logs Reference*
	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. 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 784
Changing endpoint parameters globally on page 725

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 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. On the **Feature Options** tab:
   a. Enter the required configuration parameters.
   b. In the **Features** list, select the features for the SIP endpoint.

6. On 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 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. On the **Feature Options** tab:
   a. Enter the required configuration parameters.
   b. In the **Features** list, select the features for the SIP endpoint.

6. On 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 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. On the **Feature Options** tab:
   a. Enter the required configuration parameters.
   b. In the **Features** list, select the features for the SIP endpoint.

6. On 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.

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 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 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 navigation pane, click **Endpoints** > **Manage Endpoints**.
3. Select one or more 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.

Hunt Group

Hunt Groups

Use the Hunt Groups feature to set up a group of extensions that can handle multiple calls to a single telephone number. You can choose the call distribution method to route calls. For each call to the number, the system hunts for an available extension in the hunt group, and connects the call to that extension.

A hunt group is especially useful when you expect a high number of calls to a particular telephone number. A hunt group might consist of people who are trained to handle calls on specific topics. For example, the group might be a:

- Benefits department within your company
- Service department for products that you sell
- Travel reservations service
- Pool of attendants

A hunt group might also consist of a group of shared telecommunications facilities. For example, the group might be a:

- Modem pool
- Group of data-line circuit ports
- Group of data modules

Hunt Group List field descriptions

Hunt Group List displays all the Hunt Groups that are associated with the selected Communication Manager. You can view the usage list of the extension of the hunt group. You can also apply filters and sort each of the columns in **Hunt Group List**.

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

Name	Description
Group Number	The group number of the hunt group.
Group Name	The group name of the hunt group.
Group Extension	The group extension of the hunt group.
Group Type	The group type of the hunt group.

Table continues…

Name	Description
Tenant Number	The tenant number of the hunt group.
System	The name of Communication Manager associated with the hunt group.

Adding a hunt group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Groups** > **Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Hunt Group List** section, click **New**.
6. On the New Hunt Group page, in the **General options (O)**, **Message Center Parameters (C)**, and **Group Members (M)** sections, complete the mandatory fields that are marked with a red asterisk (*).
7. To add the hunt group, click **Commit** or do one of the following:
   - To add the hunt group at the specified time, click **Schedule**. On the Job Scheduler page, set the time, and click **Schedule**.
   - To cancel the operation, click **Cancel**.

Editing a hunt group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Groups** > **Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Hunt Group List** section, select the hunt group you want to edit, and do one of the following:
   - Click **Edit**.
   - Click **View** > **Edit**.
6. On the **Edit Hunt Group** page, edit the required fields.
7. Click **Commit** to save the changes.

Viewing a hunt group

About this task

Use the following procedure to view the parameters of a hunt group.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Groups** > **Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Hunt Group List** section, select the hunt group.
6. Click **View**.

   On the View Hunt Group page, you cannot edit the fields. To go to the Edit Hunt Group page, click **Edit**.

Deleting a hunt group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Groups** > **Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Hunt Group List** section, select a hunt group, and click **Delete**.
6. On the Delete Hunt Group Confirmation page, do one of the following:
   - To delete the hunt group immediately, click **Delete**.
   - To delete the hunt group at the specified time, click **Schedule**. On the Job Scheduler page, set the time, and click **Schedule**.
   - To cancel the operation, click **Cancel**.

List Usage Extension in hunt group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Groups** > **Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Hunt Group List** section, select a hunt group.
6. Click **More Actions** > **List Usage Extension**.

   The system displays the **List Usage Extension** page with details.

7. Click **Done**.

Exporting selected hunt group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Groups** > **Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the **Hunt Group List**, select the hunt group you want to export.
6. Click **More Actions** > **Export Selected Hunt Group**.

   The system displays the **Export Hunt Group** page.
7. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
8. Click **Export**.

Exporting all hunt groups

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Groups** > **Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Export All Hunt Groups**.

   The system displays the **Export Hunt Group** page.
6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

Importing hunt groups

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Groups** > **Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Import Hunt Groups**.

   The system displays the **Import CM Objects** page.

6. In the **Select a file** field, select the required excel file and click **Browse**.
7. Select one of the following in the **Select Error Configuration** field.

   Default value is **Continue processing other records**.

   - **Abort on first error**
   - **Continue processing other records**
8. Select one of the following in the **If a matching record already exists** field.

   Default value is **Skip**.

   - **Skip**
   - **Merge**
   - **Delete**
9. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
10. Click **Import**.

Downloading Excel Template

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Groups** > **Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Download Excel Template**.
6. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and click **OK**.

Trunk Group

Trunk Group List field descriptions

Trunk Group List displays all the Trunk Groups that are associated with the selected Communication Manager. You can also apply filters and sort each of the columns in **Trunk Group List**.

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

Name	Description
Group Number	The group number of the trunk group.
Trunk Group Name	The group name of the trunk group.
Group Type	The group type of the trunk group.

Table continues…

Name	Description
Tenant Number	The tenant number of the trunk group.
TAC	The trunk access code (TAC) of the trunk group.
Number of Members	The number of members of the trunk group.
COR	The class of restriction (COR) of the trunk group.
CDR	The call detail record (CDR) of the trunk group.
Outgoing Display	The outgoing display of the trunk group.
Queue Length	The queue length of the trunk group.
System	The system of the trunk group.

Adding a trunk group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Trunk Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Trunk Group List** section, click **New**.
6. On the New Trunk Group page, complete the mandatory fields that are marked with a red asterisk (*) in the following sections:
   - General Options (O)
   - Parameter Options (P)
   - Feature Options (F)
   - Administrable Timer (A)
   - ATM Thresholds (T)
   - Group Members (M)
7. Click one of the following:
   - **Commit**: To add the trunk group.
   - **Schedule**: To add the trunk group at a specific time. On the Job Scheduler page, set the time, and click **Schedule**.
   - **Cancel**: To cancel the operation.

Editing a trunk group

About this task

You can edit one trunk group at a time. If you select more than one trunk group the system disables the **View** and **Edit** options.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Trunk Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Trunk Group List** section, select the trunk group that you want to edit, and click **Edit**.
6. On the **Edit Trunk Group** page, edit the required fields.
7. Click **Commit** to save the changes.

Viewing a trunk group

About this task

Use this procedure to view the parameters of a trunk group. If you select more than one trunk group the system disables the **View** and **Edit** options.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Trunk Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Trunk Group List** section, select the trunk group.
6. Click **View**.

   The system displays the View Trunk Group page.

Deleting a trunk group

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the left navigation pane, click **Network** > **Trunk Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Trunk Group List** section, select one or more trunk groups, and click **Delete**.
6. On the Delete Trunk Group Confirmation page, click one of the following:
   - **Delete**: To delete the Trunk group immediately.

- **Schedule**: To delete the Trunk group at the specified time. On the Job Scheduler page, set the time, and click **Schedule**.
- **Cancel**: To cancel the operation.

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 navigation pane, click **Endpoints** > **Off PBX Telephone** > **Off PBX Configuration Set**.
3. Select one or more 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 navigation pane, click **Endpoints** > **Off PBX Telephone** > **Off PBX Configuration Set**.
3. Select one or more 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.

Table continues…

Name	Description
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 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.

Table continues…

Name	Description
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 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 navigation pane, click **Endpoints** > **Off PBX Telephone** > **Off PBX Endpoint Mapping**.
3. Select one or more 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 navigation pane, click **Endpoints** > **Off PBX Telephone** > **Off PBX Endpoint Mapping**.
3. Select one or more 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 navigation pane, click **Endpoints** > **Off PBX Telephone** > **Off PBX Endpoint Mapping**.
3. Select one or more 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.

Table continues…

Name	Description
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 navigation pane, click **Endpoints** > **Xmobile Configuration**.
3. Select one or more 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 798

Editing Xmobile Configuration

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Xmobile Configuration**.
3. Select one or more 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 798

Xmobile Configuration field descriptions

Name	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.
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.

Table continues…

Name	Description
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-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.

Table continues…

Name	Description
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 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.

Table continues…

Name	Description
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.
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 navigation pane, click **Network** > **Automatic Alternate Routing Digit Conversion**.
3. Select one or more 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 802

Editing Automatic Alternate Routing Digit Conversion data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Network** > **Automatic Alternate Routing Digit Conversion**.
3. Select one or more 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 802

AAR/ARS Digit Conversion field descriptions

Name	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**.

Table continues…

Name	Description
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 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.
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.
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 navigation pane, click **Network** > **Automatic Route Selection Digit Conversion**.
3. Select one or more 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 802

Editing Automatic Route Selection Digit Conversion data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Network** > **Automatic Route Selection Digit Conversion**.
3. Select one or more 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 802

AAR/ARS Digit Conversion field descriptions

Name	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 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**.

Table continues…

Name	Description
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.
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 navigation pane, click **Network** > **Automatic Route Selection Toll**.
3. Select one or more 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 807

Editing Automatic Route Selection Toll data

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Network** > **Automatic Route Selection Toll**.
3. Select one or more 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 807

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.

Table continues…

Button	Description
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.

Cluster Session Manager

Cluster Session Manager

Using the Cluster Session Manager, you can administer a list of unique node names having Session Manager IPs that are configured on Communication Manager. This eliminates the need for provisioning trunks for redundancy. This feature frees up trunks so that the available trunks can be used by SIP agents, SIP stations, or PSTN bound SIP trunk calls. You can also can generate reports for displaying the status of active and idle trunks.

With Cluster Session Manager, you can manage up to 10 clusters, and each cluster can manage up to 28 Session Managers. From the Manage Users page, you can define the Primary Session Manager and the Secondary Session Manager. If the call to the SIP station is routed to a SIP trunk that has a clustered signaling group, then the Invite is sent to the station on primary Session Manager. If the primary Session Manager is not reachable, then the Invite is sent to the station on secondary Session Manager.

Using the Signaling Groups page, you can access the Communication Manager CLI and administer the Clustered and Cluster ID fields. These fields appear for SIP signaling groups only. For more information, see “Cluster Session Manager” chapter in *Avaya Aura® Communication Manager Screen Reference* and “SIP trunk optimization” chapter in *Avaya Aura® Communication Manager Feature Description and Implementation*.

Limitations

Limitations of Cluster Session Manager are as follows:

- You can configure Session Manager node names with IPv6 addresses, only if “procr6” is configured on Communication Manager
- You can configure Session Manager node names with IPv4 addresses, only if “procr” is configured on Communication Manager
- You cannot configure the same node names of type IPv4 and IPv6 in the same cluster

Viewing cluster Session Managers

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Network** > **Cluster Session Manager**

3. Click **Show List**.
4. From the Cluster List, select the cluster you want to view.
5. Click **View**.

Editing cluster Session Managers

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Network** > **Cluster Session Manager**
3. Click **Show List**.
4. From the Cluster List, select the cluster you want to edit.
5. Click **Edit** or click **View** > **Edit**.
6. Edit the required fields on the **Edit Cluster** page.
7. Click **Commit** to save the changes.

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.
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 navigation pane, click **Network** > **Data Modules**.
3. Select one or more 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 811

Viewing a Data Module

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Network** > **Data Modules**.
3. Select one or more 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 811

Editing a Data Module

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Network** > **Data Modules**.
3. Select one or more 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 811

Deleting Data Modules

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Network** > **Data Modules**.
3. Select one or more 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 811

Data Modules field descriptions

Name	Description
List Type	Indicates whether the type of list is group, personal, enhanced, or system type.

Table continues…

Name	Description
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 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 Bearer Capability Classes (BCC) value in an associated routing pattern when attempted calls utilizing the data module fail to complete. The BCC values must be the same. For a detailed description of BCC and their ability to provide specialized routing for various types of voice and data calls, see *Avaya Aura® Communication Manager Feature Description and Implementation*. 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.

Table continues…

Name	Description
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.
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 standby remote loop around tests fails if this field is not administered. Used with Netcon and Processor Interface Data Modules.

Table continues…

Name	Description
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. 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

Table continues…

Name	Description
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`, 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.

Table continues…

Valid Entry	Usage
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 • 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.

Table continues…

Valid Entry	Usage
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.
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. For more information on Point-to-Point data modules, see *Administering Network Connectivity on Avaya Aura® Communication Manager*.
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 navigation pane, click **System** > **Class of Service**.
3. Select one or more 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 820

Viewing Class Of Service data

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. In the navigation pane, click **System** > **Class of Service**.
3. Select one or more 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 820

Filtering the Class Of Service list

Procedure

1. On the System Manager web console, click **Elements** > **Messaging**.
2. In the navigation pane, click **System** > **Class of Service**.

3. Select one or more 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.

Table continues…

Name	Description
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 • 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.
Bridging Exclusion Override	Allows a station to bridge on a call that has exclusion activated.
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.

Table continues…

Name	Description
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 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 navigation pane, click **System** > **Authorization Code**.
3. Select one or more 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 824

Editing Authorization Code

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **System** > **Authorization Code**.
3. Select one or more 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 824

Authorization Code field descriptions

Name	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 navigation pane, click **System** > **Class of Service Group**.
3. Select one or more 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 826

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 navigation pane, click **System** > **Class of Service Group**.
3. Select one or more 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 826

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 independently administered or customized on the Tone Generation screen.

Table continues…

Name	Description
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 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.

Table continues…

Name	Description
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 830

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 830

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 830

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 830

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.
Update on Sync	During Communication Manager Sync, if System Manager finds any new extension within the UDP Group ranges, then System Manager updates the UDP table of all Communication Manager that are in that UDP group.

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.

Table continues…

Name	Description
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**.
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.
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.

Table continues…

Button	Description
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 navigation pane, click **System** > **Uniform Dial Plan**.
3. Select one or more 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 navigation pane, click **System** > **Uniform Dial Plan**.
3. Select one or more 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 navigation pane, click **System** > **Uniform Dial Plan**.
3. Select one or more 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 navigation pane, click **System** > **Uniform Dial Plan**.
3. Select one or more 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 834

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.

Table continues…

Name	Description
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 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

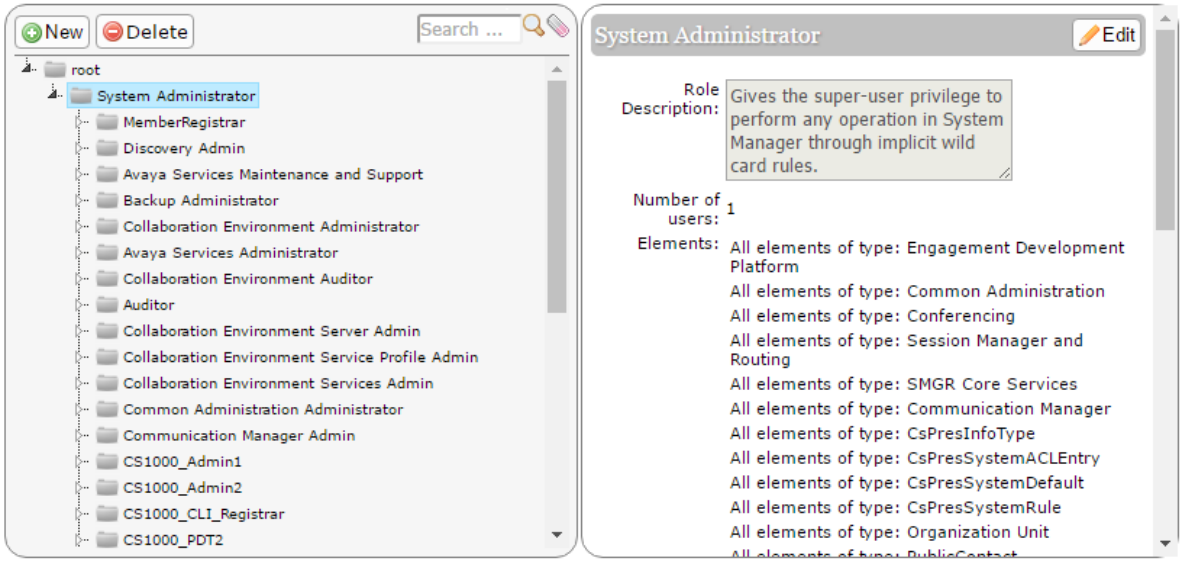
Updating UDP entries on page 834

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 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. 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 the Usage Options page 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.
- Remove a **Send NN** button for the endpoint, if configured.
- Remove a **Busy Indicate** button for the endpoint, if configured.
- Remove a **Auto Message Wait** button for the endpoint, if configured.
- Remove a **Call Forwarding** button for the endpoint, if configured.
- Remove a **Call Forwarding-Busy Do Not Answer** button for the endpoint, if configured.
- Remove a **Enhanced Call Forwarding** button for the endpoint, if configured.
- Remove a **Send All Calls** button for the endpoint, if configured.
- Remove a **No Hold Conference** button for the endpoint, if configured.

Note:

If an endpoint is referenced elsewhere and if you try to delete the endpoint, Communication Manager gives an error. You must remove the reference before you delete the endpoint. Use the Usage Option page to remove the references.

Related links

Re-Calculate route pattern on page 837

Re-Calculate route pattern

You can update the route pattern based on the associated Session Manager.

On the Re-Calculate Route Pattern page, you can apply the changes to the endpoint that might have a Route Pattern value different from the value calculated based on Session Manager to route pattern association. The Select devices from Communication Manager List section provides a list of Communication Manager systems from where you can select Communication Manager.

The Session Manager Route Pattern association section is display only and contains the primary Session Manager and secondary Session Manager to Route Pattern association.

The Users with Administered Route Pattern different from Calculated Route Pattern section contains the users with a Route Selection different from the calculated Route Selection. You can select users and apply the changes by using **Apply Recalculate Route Pattern**. The system triggers a job that can run immediately or schedule for later. When the job is complete, the system applies the changes to Communication Manager and updates the System Manager database.

In the Users with Administered Route Pattern different from Calculated Route Pattern section, you can recalculate, update users, and apply the changes to users:

- After System Manager upgrades to 7.0, and you have configured Communication Manager 7.0 route patterns, you can update users in bulk from the Re-Calculate Route Pattern page. You can also enable the **Calculate Route Pattern** check box on **Manage Users** > **User Management** > **Communication Profile** > **CM Endpoint profile** page.
- After you make changes to the existing route patterns after the initial setup, you can apply the changes to the affected users.

Related links

Endpoint options on page 836

Adding dependencies to an endpoint, agent, or VDN

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Options** > **Usage Options**.
3. Click **Add Options**.
4. Select one or more of the following options for all the Communication Manager servers:
   - **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.

   To customize the default settings selection for a Communication Manager select the required default settings in the table.
5. Do one of the following:
   - To save the changes, click **Commit**.
   - To clear the selected default settings, click **Reset**.

Removing references to an endpoint

Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Options** > **Usage Options**.
3. On the **Remove Options** tab, select the references you want to remove for the endpoint.
4. Click **Commit**.

Related links

Remove options field descriptions on page 839

Remove options field descriptions

Name	Description
System	The name of the Communication Manager system. 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.
Send NN	Select this checkbox to remove the reference between the **Send NN** button and the endpoint you choose.
Busy Indicate	Select this checkbox to remove the reference between the **Busy Indicate** button and the endpoint you choose.
Auto Message Wait	Select this checkbox to remove the reference between the **Auto Message Wait** button and the endpoint you choose.
Call Forwarding	Select this checkbox to remove the reference between the **Call Forwarding** button and the endpoint you choose.
Call Forwarding-Busy Do Not Answer	Select this checkbox to remove the reference between the **Call Forwarding-Busy Do Not Answer** button and the endpoint you choose.
Enhanced Call Forwarding	Select this checkbox to remove the reference between the **Enhanced Call Forwarding** button and the endpoint you choose.
Send All Calls	Select this checkbox to remove the reference between the **Send All Calls** button and the endpoint you choose.
No Hold Conference	Select this checkbox to remove the reference between **No Hold Conference** button and the endpoint you choose.

Button	Description
Commit	Click to apply the remove option settings.
Reset	Click to undo all the changes.

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 840

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.

Decommissioning Communication Manager from System Manager

Performing prerequisite steps on System Manager before decommissioning Communication Manager

About this task

Perform the following steps on System Manager before decommissioning Communication Manager from the host where the Communication Manager is deployed:

Procedure

1. Remove stations and agents associated with Communication Manager users on System Manager.
2. Delete agents associated with users.
3. Remove Communication Manager configuration from tenants.
4. Remove Communication Manager configuration from inventory.
5. Delete Communication Manager from the Manage Endpoints page.
6. Run a full synchronization on System Manager.
7. Decommission Communication Manager from System Manager.

Removing stations and agents associated with Communication Manager users on System Manager

About this task

Use the following procedure to identify a Communication Manager user associated with a station and a station associated with a user. Before decommissioning Communication Manager, you must identify the station extension and the agent login ID associated with a user.

Procedure

1. Log in to the System Manager command-line interface with the administrator credentials.
2. Navigate to **Elements** > **Communication Manager** > **Call Center** > **Agents**.
3. On the Agents page, select the specific Communication Manager.

   The Agents List table displays the user login IDs associated with the station.
4. Navigate to **Elements** > **Communication Manager**.
5. In the navigation pane, click **Endpoints** > **Manage Endpoints**.

6. On the Endpoints page, select the specific Communication Manager and identify the station associated with a user.

   The Endpoint List table displays all stations associated with a user.

Next steps

Delete agents associated with Communication Manager users. See Delete agents associated with Communication Manager users on page 844.

Delete agents associated with Communication Manager users

After identifying stations and agents associated with a user, use one of the following choices to delete agents associated with Communication Manager users:

- Deleting Communication Manager users permanently from System Manager.
- Removing the communication profile for a user.
- Removing communication profiles for users in bulk.
- Clearing the Delete on Unassign from User or on Delete User check box.
- Clearing the Delete on Unassign from User or on Delete User check box for users in bulk.

Related links

Deleting Communication Manager users permanently from System Manager on page 844
Removing the communication profile for a user on page 844
Deleting communication profiles from users in bulk on page 845
Clearing the Delete on Unassign from User or on Delete User check box on page 845
Clearing the Delete on Unassign from User or on Delete User check box for users in bulk on page 845

Deleting Communication Manager users permanently from System Manager

Procedure

1. On the System Manager web console, navigate to **Users** > **User Management** > **Manage Users**.
2. Select the user associated with the Communication Manager and click **Delete**.
3. Click **More Actions** and select **Show Deleted Users**.
4. Select the listed users and click **Delete**.

Removing the communication profile for a user

Procedure

1. On the System Manager web console, navigate to **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, select the user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **PROFILES** section, click the toggle button next to the **CM Endpoint Profile**.

   System Manager disables **CM Endpoint Profile**.

5. Click **Commit**.

Deleting communication profiles from users in bulk

About this task

Do the following steps to remove communication profile from users in bulk:

Procedure

1. Navigate to **Users** > **User Management** > **Manage Users**.
2. Select multiple users and click **More Actions**.
3. Export all users and extract necessary information from users.
4. Modify XML values to remove the communication profile section.
5. Re-import users only in XML format using the Replace option.

   For more information on importing and exporting bulk users, see Bulk import and export on page 368.

Clearing the Delete on Unassign from User or on Delete User check box

About this task

Use the following procedure to retain Communication Manager details on System Manager after decommissioning Communication Manager:

Procedure

1. Navigate to **Users** > **User Management** > **Manage Users**.
2. On the Manage Users page, select the user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **PROFILES** section, click the toggle button next to the **CM Endpoint Profile**.

   System Manager enables **CM Endpoint Profile** and displays the fields of the **CM Endpoint profile**.
5. Clear the **Delete on Unassign from User or on Delete User** check box.

Clearing the Delete on Unassign from User or on Delete User check box for users in bulk

Procedure

1. Navigate to **Users** > **User Management** > **Manage Users**.
2. Select multiple users and click **More Actions**.
3. Export all users and extract necessary information from users.
4. Re-import users only in Excel format using the Replace option.

   For more information on importing and exporting bulk users, see Bulk import and export on page 368.

Deleting Communication Manager configuration from tenants

Procedure

1. On the System Manager web console, click **Services** > **Tenant Management**.
2. On the Tenant Management page, select a tenant associated with the Communication Manager.
3. Click **Delete**.

Next steps

Remove Communication Manager configuration from inventory. See Deleting Communication Manager configuration from inventory on page 846.

Deleting Communication Manager configuration from inventory

Procedure

1. On the System Manager web console, navigate to **Services** > **Inventory** > **Manage Elements**.
2. On the Elements table, select Communication Manager associated with a user.
3. Click **Delete**.

Next steps

Delete Communication Manager from the Manage Endpoints page. See Deleting Communication Manager from the Manage Endpoints page on page 846.

Deleting Communication Manager from the Manage Endpoints page

About this task

Though Communication Manager is deleted from the Manage Elements page, it might be visible on the Manage Endpoints page. Wait ten minutes to see if Communication Manager disappears from the Manage Endpoints page.

Procedure

If Communication Manager is still visible on the Manage Endpoints page and other pages, use one of the following choices to delete Communication Manager from System Manager:

- Wait for the `CSM_Iptcmobject_MAINTENANCE_` job that runs every night.
- Perform the following steps:
  a. Navigate to **Services** > **Scheduler** > **Pending Jobs** and select the pending job.
  b. Click **More Actions** > **Schedule On Demand Job**.

Next steps

Run a full synchronization on System Manager. See Running a full synchronization on System Manager on page 847.

Running a full synchronization on System Manager

Procedure

1. Log in to the Communication Manager SAT as a customer super-user.
2. Remove all stations from Communication Manager.
3. Exit the Communication Manager SAT.
4. Log in to the System Manager command-line interface with administrator credentials.
5. Navigate to **Services** > **Inventory** > **Synchronization** > **Communication Systems**.
6. Select **Incremental Sync data for selected devices** and click **Now**.

Decommissioning Communication Manager from System Manager

About this task

After you delete all Communication Manager admins from System Manager, decommission Communication Manager from System Manager.

Procedure

1. Shut down Communication Manager VM on the host where Communication Manager is deployed.
2. Delete Communication Manager.

   If System Manager displays an error after you delete all Communication Manager admins, contact Avaya services.

Chapter 11: 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:

System Manager 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.

During the backup operation, System Manager validates the backup file that you upload, and displays an error if the file type does not match.

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.

System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

You can only restore the data on System Manager that has the same software version and IP address (both OOBM and public), FQDN, and Hardening level as that of System Manager on which you created the backup.

Note:

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

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 information about creating a custom role, see “Adding a custom role”.

Related links

/emdata/svars/ backup in System Manager on page 849
Backup failure due to lack of disk space in /swlibrary on page 849

/emdata/svars/ backup in System Manager

For the System Manager backup operation, note the following:

- System Manager backup operation supports a maximum of 4GB file size of the `/emdata/svars/` directory. This is approximately 41% of `/emdata` occupancy, as displayed in the Disk Space Utilization widget on the System Manager web console Home screen.
- If you have 250K users and 4GB of `svars` file size, the backup file size is 5GB.

  To process the backup in the `/swlibrary` directory, you must have three times of backup file size space.
- The root partition must have at least 1GB of free space.

Related links

Backup and restore on page 848

Backup failure due to lack of disk space in /swlibrary

Condition

If the backup is not successful due to lack of disk space in `/swlibrary`, check the `/var/log/Avaya/mgmt/pem/pemDebugLog.log` file and search for the following string:

```
Caused by: java.io.IOException: No space left on device
```

Solution

1. Clean up space in `/swlibrary`.

   Note:

   Do not delete the `wildfly_java_tmp` directory.
2. Move the backup archives located at `/swlibrary/backup/` to the remote machine.
3. Delete unused SDM artifacts, such as OVAs and patches that are not required.

   To delete SDM artifacts from the System Manager web console, click **Services** > **Solution Deployment Manager** > **Software Library Management** > **Manage Files** > **Select and Delete files**.
4. Delete any files, such as OVAs for patch binaries copied manually.

Related links

Backup and restore on page 848

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 remove older backup files to create additional disk space.

Note:

Ensure the root partition has at least 1GB of free space.

Related links

Disk space required for backup on page 860

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 848

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 862

Enabling backup encryption

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the navigation pane, click **Settings** > **SMGR** > **SMGR Element Manager**.
3. On the View Profile:SMGR Element Manager page, click **Edit**.
4. On the Edit Profile:SMGR Element Manager page, in **Backup Encrypted**, type `true`.
5. In **Encrypted Backup Global Password**, type a backup encryption password.
6. Click **Commit**.

Creating a data backup on a local server

About this task

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

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 **File name**, type the backup file that you want to create.
5. **(Optional)** To create encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the following fields:

      - **Backup Encryption Password**
      - **Confirm Backup Encryption Password**

   b. In **Backup Encryption Password**, type the encryption password.
   c. In **Confirm Backup Encryption Password**, retype the encryption password.

      You must remember the password to restore the backup.
6. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: `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 850

Backup field descriptions on page 863

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.

System Manager requires password authentication to enable the remote backup servers for successful backup.

Starting with System Manager 10.2.x, Avaya Aura® Messaging (AAM) is no longer supported, so you need to clean the AAM data before you take a backup. See *Upgrading Avaya Aura® System Manager*.

Note:

System Manager does not support authentication mechanisms, such as Keyboard-Interactive and public key-based support.

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 the **File transfer protocol** field, click `SCP` or `SFTP`.
     b. Enter the remote server IP, 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, 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. **(Optional)** To create encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the following fields:

      - **Backup Encryption Password**

- **Confirm Backup Encryption Password**

b. In **Backup Encryption Password**, type the encryption password.

c. In **Confirm Backup Encryption Password**, retype the encryption password.

You must remember the password to restore the backup.

6. Click **Now**.

If the backup is successful, the Backup and Restore page displays the message: `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 850
Backup field descriptions on page 863

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 863
Schedule Backup field descriptions on page 865

Scheduling a data backup on a remote server

Before you begin

Ensure 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.

About this task

Use this functionality to schedule a data backup on a remote server. If there is no successful backup in the last ‘n’ days, where ‘n’ is configurable, then System Manager raises an alarm. The backup can be remote or local. The default number of days is set to 7, but it can be configured to any number from 1 to 30 using the 'Alarm Threshold for number of days since last successful SMGR Backup' parameter.

For more information about configuring a threshold for System Manager backup alarm, see Configure a threshold to raise the System Manager backup alarm on page 1007.

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, 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

Backup field descriptions on page 863
Schedule Backup field descriptions on page 865

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 855
Scheduling a data backup on a local server on page 854
Deleting the scheduled backup job on page 856

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 1122.

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 856

Restoring data backup from a local server

About this task

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

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:

   System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.
5. **(Optional)** To restore encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the **Backup Encryption Password** field.
   b. In **Backup Encryption Password**, type the encryption password.
6. 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.
```

7. 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 850
Restore field descriptions on page 866

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 Release 8.1 with Release 8.1.1 software patch installed, System Manager on which you restore the backup must run Release 8.1 that has Release 8.1.1 software patch installed.

If the System Manager release on which you restore the backup does not match, the restore operation fails.

For more information, see “Backup and restore”.

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. **(Optional)** To restore encrypted backup using encryption password, do the following:
   a. Clear the **Use Global Backup Encryption Password** check box.

      System Manager displays the **Backup Encryption Password** field.

b. In **Backup Encryption Password**, type the encryption password.

5. 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:

     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, 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**.
6. 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.
   ```
7. 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.

Note:

It is recommended to restore the backup either on the same profile or higher profile.

Example

If the backup is done for Profile 3, it is recommended to restore to the Profile 3 or higher. Restoring the backup to lower profile such as Profile 2 is not supported.

Related links

Backup and restore on System Manager that is configured for Geographic Redundancy on page 850
Restore field descriptions on page 866

Disk space required for backup

Table 9: 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
100k	2 min 54 sec	1 hr 4 min 03 sec

Table continues…

Backup and Restore Time Duration		
Number of users	System Manager	
	Backup	Restore
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
  - diffie-hellman-group-exchange-sha256
  - ecdh-sha2-nistp256
  - ecdh-sha2-nistp384
  - ecdh-sha2-nistp521
- Encryption algorithms for Client to Server
  - aes128-ctr
  - 3des-ctr
  - aes192-ctr
  - aes256-ctr
  - 3des-cbc
  - blowfish-cbc
  - aes128-cbc
  - aes192-cbc
  - aes256-cbc
  - arcfour
  - arcfour128
  - arcfour256
- Mac algorithm for Client to Server
  - hmac-sha1

- hmac-md5
- hmac-md5-96
- hmac-sha1-96
- hmac-sha256
- hmac-sha2-256
- hmac-sha256@ssh.com
- hmac-sha2-256-96
- hmac-sha512
- hmac-sha2-512
- hmac-sha512@ssh.com
- hmac-sha2-512-96

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	Displays the Backup page from where you can back up the System Manager data.
Restore	Displays 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.
Use Global Backup Encryption Password	The option to use the global encryption password for backup. To use the **Use Global Backup Encryption Password** option, enable **Backup Encrypted** and provide the encryption password on the **Services** > **Configurations** > **Settings** > **SMGR** > **SMGR Element Manager** page. By default, **Use Global Backup Encryption Password** is enabled. To set a new password for backup, you can deselect the **Use Global Backup Encryption Password** check box. System Manager displays the following fields: • **Backup Encryption Password** • **Confirm Backup Encryption Password**
Backup Encryption Password	The password for the encrypted backup. The backup encryption password must contain minimum 8 and maximum 16 characters. The password must be a combination of lower case (a-z), upper case (A-Z), numerals (0-9), and special characters ($@!%*?&). **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.

Table continues…

Name	Description
Confirm Backup Encryption Password	The password for the encrypted backup. **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.

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, 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 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**.
Use Global Backup Encryption Password	The option to use the global encryption password for backup. To use the **Use Global Backup Encryption Password** option, enable **Backup Encrypted** and provide the encryption password on the **Services** > **Configurations** > **Settings** > **SMGR** > **SMGR Element Manager** page. By default, **Use Global Backup Encryption Password** is enabled. To set a new password for backup, you can deselect the **Use Global Backup Encryption Password** check box. System Manager displays the following fields: • **Backup Encryption Password** • **Confirm Backup Encryption Password**

Table continues…

Name	Description
Backup Encryption Password	The password for the encrypted backup. **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.
Confirm Backup Encryption Password	The password for the encrypted backup. **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.

Button	Description
Now	Creates a backup 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. The system generates an alarm if you do not schedule a System Manager backup every 7 days.
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 returns to the Backup Restore page.

Restore field descriptions

Use this page to restore the application data from a local or a remote location.

Name	Description
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**.

Name	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:** System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.
Use Global Backup Encryption Password	The option to use the global encryption password for backup. To use the **Use Global Backup Encryption Password** option, enable **Backup Encrypted** and provide the encryption password on the **Services** > **Configurations** > **Settings** > **SMGR** > **SMGR Element Manager** page. By default, **Use Global Backup Encryption Password** is enabled. To set a new password for backup, you can deselect the **Use Global Backup Encryption Password** check box. System Manager displays the following fields: • **Backup Encryption Password** • **Confirm Backup Encryption Password**

Table continues…

Name	Description
Backup Encryption Password	The password for the encrypted backup. The backup encryption password must contain minimum 8 and maximum 16 characters. The password must be a combination of lower case (a-z), upper case (A-Z), numerals (0-9), and special characters ($@!%*?&). **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.
Confirm Backup Encryption Password	The password for the encrypted backup. **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.

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**.

Name	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, 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 displays the Backup and Restore page.

Chapter 12: Configuring applications

Managing data retention rules

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 in Database
- Log files:
  - Application
  - System
- Backup files stored locally on System Manager
- Cleared alarms
- Aged alarms
- Aged Scheduler Completed Jobs

Excluded log files

System Manager does not delete the following logs while executing the **`pruneAllLogs.sh`** command.

- /var/log/audit/data/
- /var/log/anaconda/
- /var/log/aide/aide.log
- /var/log/Avaya/cs1000/cs1000_install_
- /var/log/Avaya/RHEL-07-010010.log
- /var/log/Avaya/GRState.log
- /var/log/Avaya/kernelupdateflag.log
- /var/log/Avaya/VEProfile.log
- /var/log/Avaya/setStaticRoute.out

- /var/log/Avaya/setStaticRoute.log
- /var/log/Avaya/PostDeployLogs/post_install_sp.log
- /var/log/Avaya/easg.log
- /var/log/Avaya/patch_verification.log
- /var/log/Avaya/applyPatch.out
- /var/log/Avaya/SMGR_Patch.log
- /var/log/Avaya/patchinstallation
- /var/log/Avaya/enableASG.log
- /var/log/Avaya/RestoreSMGR.log
- /var/log/Avaya/backup_not_taken.txt
- /var/log/Avaya/dump_cleanup_service.log
- /var/log/Avaya/purgeExportFilesLog.log
- /var/log/Avaya/editHost.log
- /var/log/secure
- /var/log/yum.log
- /var/log/wtmp
- /var/log/avaya/common_os/hardening_log
- /var/log/ntpCheck.log
- /var/log/setBootPass.log
- /var/log/btmp
- /var/log/dmesg
- /var/log/boot.log
- /var/log/Avaya/OOBM.log
- /var/log/Avaya/smgrUtilityAudit.log
- /var/log/Avaya/logRetention.log
- /var/log/Avaya/SMGRSSP_Patch.log
- /var/log/Avaya/VTMupdate.log
- /var/log/userShellLog.log

Accessing the Data Retention Rules service

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the navigation pane, click **Data Retention**.

The system displays the Data Retention page with the Rule list.

Modifying data retention rule

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the navigation pane, click **Data Retention**.

   The system displays the Data Retention page with the Rule list.
3. From the Rule List section, select a rule.
4. Click **Edit**.

   Note:

   If you change the **LogPurgeRule** settings, the export delta functionality might get affected as the permanently deleted users login-names in the delta period are identified on the basis of audit logs of permanently deleted users in the system.
5. In the **Retention Interval (Days)** field, modify the value.
6. Click **Update** to save the value.

Related links

Data Retention field descriptions on page 870

Applying data retention rule

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the navigation pane, click **Data Retention**.

   The system displays the Data Retention page with the Rule list.
3. From the Rule List section, select a rule.
4. Click **Execute** to apply the rule.

   When the rule is applied, System Manager display the following message:

   `Rule successfully applied.`

Data Retention field descriptions

Name	Description
Option button	The option to select a data retention rule.

Table continues…

Name	Description
Rule Name	The name of the rule. Rules are: • **LogPurgeRule** • **ClrdAlarmPurgeRule** • **AgedAlarmPurgeRule** • **AgedSchedulerCompletedJobsPurgeRule** • **LogRetentionRule**: This is applicable for log files.
Rule Description	A brief description about the data retention rule. For **LogRetentionRule**, the value range is from 1 through 180 days. Default value for number of days to retain log files is 30 days.
Retention Interval (Days)	The number of days the data is retained.

Button	Description
Edit	Modifies the selected rule.
Update	Saves the rule with changes made to the rule.
Cancel	Cancels the editing operation.
Execute	Applies the selected rule.

logRetention command

The **`logRetention`** utility displays the currently administered log retention time.

Syntax

```
logRetention [-a] [-c] [-d] [-h]
```

-a	Displays all log retention time settings.
-c	Displays current log retention time from database.
-d	Displays log retention time set from properties files.
-h,--help	The option to print help options.

updateLogRetention command

The **`updateLogRetention.sh`** utility manages the log retention time.

Syntax

```
updateLogRetention.sh [-p] [-v] [maxRetentionTime]
```

-p	The log files do not get pruned.

-v	Verbose mode.
maxRetentionTime	The Maximum Retention Time in days (optional). If the value is not provided, the current administered value is used.
-h	The option to print help options.

pruneAllLogs command

The **`pruneAllLogs.sh`** utility manages the deletion of log files.

Syntax

```
pruneAllLogs.sh [-b] [-t] [-v] [-h] [maxRetentionTime]
```

-b	Deletes the base log files.
-t	Displays the list of log files that are eligible for deletion. Test mode. Does not delete the log files.
-v	Verbose mode.
-h	The option to print help options.
maxRetentionTime	The Maximum Retention Time in days (optional). If the value is not provided, the current administered value is used.

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

View and Edit Profile SMGR field descriptions on page 883

View Profile: Agent Management field descriptions

Name	Description
Alarm aging keep time	This field is not used for System Manager.

Table continues…

Name	Description
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 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	Displays 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.

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

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 name to display as prefix in the Communication System Management job names. The default is IPO.

Button	Description
Edit	Displays the Edit: Profile page where you can change the values.
Done	Saves the changes.
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

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.
Enable Help Text Retrieval on Element-cut through page	By default, the value is **true**. If the value is **true**, System Manager displays the help text on the Communication Manager element cut through page. This helps to reduce the amount of time required for configuring Communication Manager from the Element cut-through page. If you set the value to **false**, System Manager does not display the help text on the Communication Manager element cut through page.
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 Manager communication profile.
Endpoint Migration Job History Retention in Days	The number of days to retain the endpoint migration job history data. The number of days for retaining the endpoint migration job history data is from 1 through 60 days. By default, the number of days for the **Endpoint Migration Job History Retention in Days** field are 30 days.
Incremental sync interval (Hours)	The time between every incremental synchronization. By default, the value for the **Incremental sync interval (Hours)** field is 24 hours.
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 CSM. This application prefix appears as the prefix in the Communication System Management job names.

Button	Description
Edit	Displays the Edit Profile:Communication System Management Configuration page to edit the parameters.
Done	Click to close the View Profile: Configuration page.

Edit Profile: Communication System Management Configuration field descriptions

Use this page to edit the parameters in the Communication System Management Configuration profile.

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.
Enable Help Text Retrieval on Element-cut through page	By default, the value is **true**. If the value is **true**, System Manager displays the help text on the Communication Manager element cut through page. This helps to reduce the amount of time required for configuring Communication Manager from the Element cut-through page. If you set the value to **false**, System Manager does not display the help text on the Communication Manager element cut through page.
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 Manager communication profile.
Endpoint Migration Job History Retention in Days	The number of days to retain the endpoint migration job history data. The number of days for retaining the endpoint migration job history data is from 1 through 60 days. By default, the number of days for the **Endpoint Migration Job History Retention in Days** field are 30 days.
Incremental sync interval (Hours)	The time between every incremental synchronization. By default, the value for the **Incremental sync interval (Hours)** field is 24 hours.
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 CSM. This application prefix appears as the prefix in the Communication System Management job names.

Button	Description
Commit	Saves the changes to the database.
Cancel	Cancels the edit profile operation and returns to the View Profile: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 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	Displays 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

Name	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

Name	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

Name	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%.
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	Returns 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 returns to the previous page.

View and Edit Profile Messaging field descriptions

Telephony Properties

Name	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. The default value is **1000**.
Maximum Records on single page of table	The maximum number of records that the system displays in the table. The default value is **200**.

General Properties

Name	Description
Append Mailbox Number to Email Handle when adding the Avaya Aura Messaging subscriber	When adding Avaya Aura® Messaging Subscriber the system appends the mailbox number to the email. The default value is **false**.
Application Prefix	The text that the system prefixes to the Messaging System job names. The default value is **MM**.

Table continues…

Name	Description
Refresh Subscriber data from Messaging during edit/ view	Refreshes the subscriber data from Messaging Server on edit/view. The default value is **false**.
Update Email Handle, Common Name and ASCII version of name when changing the Avaya Aura Messaging subscriber First, Last Name values	Updates Email Handle, Common Name and ASCII version of name fields on first or last name changes. The default value is **false**.

View Profile: Configuration buttons

Button	Description
Edit	Displays the View Profile: Messaging Configuration page to edit the properties.
Done	Returns to the previous page.

Edit Profile: Configuration buttons

Button	Description
Commit	Saves the changes on the Edit Profile: Messaging Configuration page.
Cancel	Cancels the changes and displays the previous 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

Table continues…

Name	Description
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 **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.

Table continues…

Name	Description
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.
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	Displays 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 and Edit Profile SMGR field descriptions

Key Management Properties

Name	Description
Number of days before administrator should be notified	The number of days before the key expiry when the administrator must be notified. The default is `21`.
Notify administrator about asymmetric keys expiration	The status of the asymmetric keys expiration notification to the administrator. The options are: • `true`: To enable the notifications. • `false`: To disable the notifications. The default is `false`.

Database Properties

Name	Description
Connection URL	The connection URL of the database.
Host Name	The host name of the database.
JDBC Drive Class	The JDBC drive class for the database.
Password	The password for logging into the database.
Confirm Password	The database login password that you retype. This option is available only in the Edit mode.
Port Number	The port number of the database.
User Name	The user name for logging into the database.
Vendor Name	The vendor name of the database.

Password Policy for Programmatic Accounts

Name	Description
Disallow repeated and/or sequential characters	The options are: • **true**: Repeated and sequential characters are not allowed. • **false**: Repeated and sequential characters are allowed. By default, this is **true**.
Minimum total length	The minimum number of characters that you must use in the password. The valid values are from 1 through 32. The default value is 32.

Table continues…

Name	Description
Minimum number of lower case character(s)	The minimum number of lowercase characters that you must use in the password. The default value is 0.
Minimum number of numeric character(s)	The minimum number of numeric characters that you must use in the password. The default value is 0.
Minimum number of special character(s)	The minimum number of special characters that you must use in the password. The default value is 0.
Minimum number of upper case character(s)	The minimum number of uppercase characters that you must use in the password. The default value is 0.
Previous password(s) blocked	The number of recent passwords that you cannot use. The valid values are from 0 through 24. The default value is 24. The 0 value means that System Manager does not check for the previous passwords.

Multi Tenancy Properties

Name	Description
Multi Tenancy Status	The status of the Multi Tenancy feature on the system. The options are: • `true`: To enable the feature. • `false`: To disable the feature. The default is `false`.

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`: To enable self provisioning. • `false`: To disable self provisioning.

System Manager Properties

Name	Description
Build Version	The build version of System Manager. This field cannot be edited.

Auto Transliteration Properties

Name	Description
Auto Transliteration Flag	The status of the auto transliteration feature. The options are: • `true`: To enable transliteration. • `false`: To disable transliteration. The default is `true`.

Audit Configuration Properties

Name	Description
Number of failed login attempts to indicate a security threat	The number of failed login attempts after which a security threat is indicated. The default is `5` login attempts.

Email Configuration Properties

Name	Description
Enable email notification	The status of the email notifications feature. The options are: • `true`: To enable email notifications. • `false`: To disable email notifications. The default is `false`.
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.
Confirm From Email Password	The email authentication password that you retype. This option is available only in the Edit mode.
Email Host	The URL for the email server. **Note:** SMTPS Email Server is not supported in the Email Host Server attribute configuration.
Email Host Port	The port for the email server. The default port is `25`.

External Admin Connect Properties

The fields in the **External Admin Connect Properties** are used to configure the primary System Manager with the Avaya Infinity™ server.

For more information on Avaya Infinity™, refer to Avaya.

Note:

This section is applicable only for primary System Manager.

Name	Description
External Admin Connect	The **External Admin Connect** have following options: • **True**: Allows you to edit the fields in the **External Admin Connect Properties**. • **False**: Restricts you from editing the fields in the **External Admin Connect Properties**. This is a default value.
Authorization URL	The URL of the Avaya Infinity™ Cloud services.
Client ID	The Client ID for the Avaya Infinity™ Cloud services.
Client Secret	The password for Avaya Infinity™ Cloud services.
Admin Connect URL	The URL of the Avaya Infinity™ server.

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	Displays 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.
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 returns to the View Profile:Alarming UI page.

View Profile:Common Console field descriptions

Note:

For the changes to be effective, log out 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. You can set a value between 10 and 20. The default is 15.
Number of rows	Number of rows that you want the system to display in a table. The range of rows that you can set is 15 through 100. The default is 15.

Table continues…

Name	Description
Max No of Records Selectable (Table)	The maximum number of records that you can select at a time from a table.

Button	Description
Edit	Displays the Edit Profile: Common Console page where you can edit the common console profile parameters.
Done	Closes the View Profile: Common Console page.

Edit Profile:Common Console field descriptions

Note:

For the changes to be effective, log out from the system and log on again.

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. You can set a value between 10 and 20. The default is 15.
Number of rows	Number of rows that you want the system to display in a table. The range of rows that you can set is 15 through 100. The default is 15.
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:GracefulShutdown 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. The default value for the grace period before shutting down System Manager is 10 minutes.

Button	Description
Edit	Displays the Edit Profile:GracefulShutdown page where you can change the grace period.
Close	Closes the View Profile:GracefulShutdown page.

Edit Profile:GracefulShutdown 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. The default value for the grace period before shutting down System Manager is 10 minutes.

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:GracefulShutdown page, and returns to the View Profile:GracefulShutdown 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	Displays 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 889

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 returns to the View Profile:HealthMonitor page.

Related links

View Profile:HealthMonitor field descriptions on page 889

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	Displays 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.

Table continues…

Button	Description
Cancel	Cancels the edit profile operation and returns 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.
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	Displays 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.

Table continues…

Name	Description
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 returns 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.

Table continues…

Name	Description
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	Displays 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 returns to the View Profile:Logging Service page.

View and Edit 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.
Backup Encrypted	The option to enable or disable backup encryption. The options are: • `true` • `false`
Alarm Threshold for number of days since last successful SMGR Backup (Days 1-30)	The option to configure a threshold for raising an alarm when no successful System Manager backup is taken since the configured number of days. The number range is 1 through 30 days, and the default is 7.
Backup Global Password	The global password for the encrypted backup. **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.
Confirm Backup Global Password	The global password for the encrypted backup that you retype to confirm. This field is only available in the Edit mode. **Note:** Ensure to note this password. Otherwise, you cannot retrieve it.
Database Utilities Path	The name of the directory on the database server that contains the PostgreSQL backup and restore utilities. **Note:** • The database user must have execute permissions on these utilities. • Do not change the value of **Database Utilities Path**.
Database Type	The type of database. For example, Oracle, Postgres.
Database server	The hostname of the database server.
Database Port	The port number for the database server. **Note:** Do not change the value of **Database Port**.

Table continues…

Name	Description
Database SCP Port	The port on the database server on which the SSH server is running. **Note:** Do not change the value of **Database SCP Port**.
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 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 is reached, the system rotates backup archives.
Maximum Data Retention Limit (days)	The maximum data retention limit in days. You can set the limit 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 maximum transaction timeout 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. **Important:** To use the **Use Default** option on the Backup or Restore page, ensure that you specify the following: • Remote server IP • User name • Password • Name and path of the backup file
Confirm Remote Server Password	The SCP server password that you retype to confirm. This field is only available in the Edit mode.
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 to edit the System Manager Element Manager profile parameters.
Done	Closes the View Profile: SMGR Element Manager page.
Commit	Saves and commits any changes made in the System Manager Element Manager profile settings. This field is only available in the Edit mode.
Cancel	Cancels any changes and reverts the System Manager Element Manager profile settings to the last saved settings. This field is only available in the Edit mode.

View Profile:SNMP field descriptions

Avaya IM System Manager subagent attributes

Name	Description
Master Agent IPAddress	IP address of the 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 the machine on which subagent 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	Displays 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	
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 returns 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 1045
View Profile: TrapListener field descriptions on page 898

View Profile: TrapListener 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.
Email Forward	The option to forward the emails to the user. The default is **false**. If set to **true**, the system forwards the emails to the user.
Email to addresses	A list of e-mail addresses, which are comma separated, to which alarms are forwarded.
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.

Configuring Trust Management

Procedure

1. On the System Manager web console, click **Services** > **Configurations** > **Settings** > **SMGR** > **Trust Management**.

2. On the View Profile: Trust Management page, click **Edit**.
3. On the Edit Profile: Trust Management page, edit the required parameters.
4. Click **Commit**.

View Profile: TrustManagement field descriptions

Name	Description
Number of days after which system deletes expired certificates	The number of days after which System Manager deletes the data of expired certificates from the System Manager database. The default value is 365 days. If the certificate is expired and expiry date is more than the number of configured days, System Manager purges the data of expired certificates.
Threshold (in days) for raising an alarm for certificate expiration (2-60)	The number of days (n-1) before the certificate expiry when an alarm is generated. For example, if 60 days are configured, the system raises the alarm when the 59 days are remaining.
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 (2-60)	The number of days (n-1) before the certificate expiry when the auto-renewal of certificates is triggered. For example, if 30 days are configured, the certificate renewal takes place when the 29 days are remaining.

Button	Description
Edit	Displays the Edit Profile: TrustManagement page.
Done	Returns to the previous page.

Edit Profile: TrustManagement field descriptions

Name	Description
Number of days after which system deletes expired certificates	The number of days after which System Manager deletes the data of expired certificates from the System Manager database. The default value is 365 days. If the certificate is expired and expiry date is more than the number of configured days, System Manager purges the data of expired certificates.
Threshold (in days) for raising an alarm for certificate expiration (2-60)	The number of days (n-1) before the certificate expiry when an alarm is generated. For example, if 60 days are configured, the system raises the alarm when the 59 days are remaining.
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.

Table continues…

Name	Description
Threshold (in days) for triggering auto-renewal of certificates (2-60)	The number of days (n-1) before the certificate expiry when the auto-renewal of certificates is triggered. For example, if 30 days are configured, the certificate renewal takes place when the 29 days are remaining.

Button	Description
Commit	Saves your changes in the Edit Profile: TrustManagement page.
Cancel	Cancels your changes and returns 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 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**.

Table continues…

Name	Description
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. 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. 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.

Table continues…

Name	Description
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. 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 13: 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 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 Application 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
- Configure SAI Gateway
- Configure Avaya Services Registration
- View certificate add status

From Release 8.1, System Manager displays a progress bar on the Manage Elements for ongoing Geographic Redundancy event notification status that are sent to the elements that are added on System Manager. When you hover on the status bar, the system displays the event name for which this notification is being sent out from System Manager to elements. You can use the **More Actions** > **View Notification Status** page to view the details of this notification.

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, Communication Manager.

You must add the ESXi host from Application Management on Solution Deployment Manager. The system displays the ESXi host on the Manage Elements page.

Adding a new element

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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.

   The tabs and fields on the New <element-name> page varies based on the application that you select
6. Click **Commit**.

   System Manager creates the element and displays on the Manage Elements page.

Related links

Element details field descriptions on page 944

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.

Importing elements

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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**.

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 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 908
Discovery Profile List field descriptions on page 909
Element Access Profile Management field descriptions on page 918
Subnet Configurations field descriptions on page 917
SNMP Access Profiles field descriptions on page 913
Create or Edit Discovery Profile field descriptions on page 910

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 Application Management
Avaya Breeze® 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

Name	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

Name	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

Name	Description
Discovery Profile Name	The name of the discovery profile.

Subnet Configurations

Name	Description
Name	The name of the subnetwork.
IPaddress	The IP address of the subnetwork.
Mask/Network Prefix	The IP subnetwork mask prefix.
No. of IPs to scan in subnet	The number of IPs to be scanned in the subnetwork.

Element Type Access Profiles

Name	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

Name	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.
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 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 914
SNMP Access Profiles field descriptions on page 913

Editing the SNMP access profile

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the 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 914
SNMP Access Profiles field descriptions on page 913

Deleting an SNMP access profile

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the 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

Name	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.
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:

Name	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**. • **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: • **AES**: For SNMP-based communication. • **AES128**: For SNMP-based communication. • **DES**: For SNMP-based communication. The default is **DES**. • **None**: Does not encrypt traffic for this user. Set **Privacy Type** only for an SNMP V3 user.

Table continues…

Name	Description
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. • **None** The default is None. • **Read/Write**: To perform GET and SET operations. • **Read**: To perform only the GET operation.
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:

Name	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 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 917

Editing the subnetwork

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 917

Deleting a subnetwork

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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

Name	Description
Name	The name of the subnetwork.
IPaddress	The IP address of the subnetwork.
Mask/Network Prefix	The IP subnetwork mask prefix.
No. of IPs to scan in subnet	The number of IPs to be scanned in the subnetwork.

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 navigation pane, click **Element Type Access**.
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 919
Element Access Profile Management field descriptions on page 918

Editing an element access profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Element Type Access**.
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 919
Element Access Profile Management field descriptions on page 918

Deleting an element access profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Element Type Access**.
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

Name	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.

Table continues…

Button	Description
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

Name	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** feature to create login profiles for devices, and use the login profiles to discover the Communication Manager devices.

Note:

Do not use the **Create Profiles and Discover SRS/SCS servers** feature to discover and add the Duplex ESS pair to the System Manager Inventory.

The workaround is to add the Duplex ESS pair manually through the Manage Elements page with type as Communication Manager. The process is similar to adding a duplex

Communication Manager to the System Manager inventory, except that you must not select the **Add to Communication Manager** checkbox when adding a Duplex ESS pair.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Create Profiles and Discover SRS/SCS**.
3. In the **Select Devices to Create Profiles** table, select the devices 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 921

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 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 921

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 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 921

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.

Table continues…

Name	Description
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.
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 923

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 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 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 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 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

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.

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.

Procedure

1. Start an SSH session.
2. Log in to the System Manager server by using the command line interface.
3. 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 *System$987*.

5. **(Optional)** Change the log configuration in the `<MGMT_HOME>\rts\bulkExport\conf\log4j2.properties` file.

Related links

runRTSCli.sh command on page 925

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 System$987
```

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\log4j2.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 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 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 navigation pane, click **Manage Elements**.
3. On the Manage Elements page, do one of the following:
   - 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**.

   System Manager displays the Application System Supported Protocol and Access Profile Details sections.

5. In the Application System Supported Protocol section, in the **Protocol** field, select a protocol.

   The options are:

   - **URI**: For system web services API.
   - **SSH**: For application upgrade functions.
   - **SNMP**: For discovering elements.

   Based on the protocol selection, System Manager displays the fields in 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 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 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 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 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 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, to manage the elements from the current System Manager, you can select an element and click **Manage**. Then, 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 perform the Manage operation.

For information about the element manageability status, see “Elements Geographic Redundancy manageability status matrix”

At any time, you can perform the **Get Current Status**, **Manage**, or **Unmanage** operation.

During the split network, ensure that the primary or the secondary System Manager server manages an element at a time, and not both systems.

Related links

Manage Elements field descriptions on page 941

Unmanage elements

In a Geographic Redundancy system, the administrator can select to unmanage an element. Then, 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.

At any time, you can perform the **Get Current Status**, **Manage**, or **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, the administrator must set the manageability status to Unmanaged on the primary System Manager server.

Related links

Manage Elements field descriptions on page 941

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 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 Utility Services to System Manager

About this task

From Release 8.0, Utility Services is replaced by AVP Utilities.

For Release 7.x, Utility Services is a mandatory component of Appliance Virtualization Platform in the Avaya-appliance deployment offer.

When you first install Appliance Virtualization Platform, you must add Utility Services to Appliance Virtualization Platform before you add System Manager.

Use the procedure to manually add Utility Services to System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On the New Elements page, in **Type**, click **Utility Services**.

   The system displays the New Utility Services page.
5. On the General tab, provide the following information:
   - **Name**: The Utility Services name.
   - **Type**: Utility Services, a read-only field. The application type that the system populates from the **Type** field on the New Elements page.
   - **Description**: A description of Utility Services.
   - **Node**: The IP address of Utility Services.
   - Complete the remaining required fields.

   For more information, see “Element details field descriptions”.
6. Click **Commit**.

   On the Manage Elements page, the system displays the Utility Services instance that you added.

Related links

Element details field descriptions on page 944

Adding or editing a Communication Manager instance to System Manager

About this task

Use the following procedure for adding or editing the Simplex or Duplex Communication Manager instance to System Manager.

Important:

When you deploy the Communication Manager duplex pair through Solution Deployment Manager Application Management, Solution Deployment Manager creates the Active Communication Manager and Standby Communication Manager element entries by using the IP Address or FQDN of the respective Communication Manager on the System Manager **Services** > **Inventory** > **Manage Elements** page.

- To perform the Communication Manager synchronization and other operations, you must select the current Active Communication Manager entry and edit the following fields:
  - **Alternate IP Address**: Provide the current Standby Communication Manager server IP Address or FQDN.
  - **Add to Communication Manager**: Select this to administer Communication Manager on System Manager.
  - **Enable Notifications**: Select this to enable the Communication Manager Notify Sync feature.

    For more information, see “Communication Manager notify synchronization”.
- Do not edit the entry of the Standby Communication Manager element.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, do one of the following:
   - To add Communication Manager, click **New**.

     On the New Elements page, in the **Type** field, click **Communication Manager**.

     System Manager displays the Add Communication Manager page.
   - To edit Communication Manager, click **Edit**.

     System Manager displays the Edit Communication Manager <CMName> page.
4. On the **General Attributes** tab, provide the following information:
   a. In **Name**, type the Communication Manager server name.

      The Communication Manager name can be up to 256 characters.

   b. In **Hostname or IP Address**, type the host name or IP Address of the Communication Manager server.

      The IP address can be in the IPv4 or IPv6 format.

      Note:

      - For the active Communication Manager server provide the host name or IP address in **Hostname or IP Address** and for the standby Communication Manager server provide the host name or IP address in **Alternate IP Address**.

- In a duplex configuration, while adding a Communication Manager instance to System Manager, virtual address of Communication Manager must not be used as it is not supported.

c. In **Login**, type the customer login name that is required to access Communication Manager.

d. In **Authentication Type**, select the required option.

e. Enter and reenter the password, or ASG key required to access Communication Manager.

f. In **Port**, type the port number of the Communication Manager server.

g. To administer Communication Manager on System Manager, select the **Add to Communication Manager** check box.

When you select **Add to Communication Manager** check box, Communication Manager instance appears in the **Synchronize CM Data and Configure Options** page, under **Services** > **Inventory** > **Synchronization** > **Communication instance**.

h. In **CM Type**, click **Standalone** to add a Communication Manager.

5. On the **SNMP Attributes** tab, perform the following:

a. Under **Version**, select **V1**.

b. Enter the required information.

c. From **Device Type**, select the type of Communication Manager.

6. Click **Commit**.

System Manager displays the Communication Manager instance that you added on the Manage Elements page.

Related links

Add Communication Manager field descriptions on page 955

Adding a Session Manager instance to System Manager

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Click **New**.
4. On the New Elements page, in the **Type** field, click **Session Manager**.
5. Select **Core Session Manager** and click **Continue**.
6. 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 before the host installation.

7. Enter or select the appropriate information in the remaining required fields.

   For more information, see “Element details field descriptions”.

8. Click **Commit**.

Related links

Element details field descriptions on page 944

Adding an Application Enablement Services instance to System Manager

About this task

Use the following procedure if you are migrating or deploying AE Services using Solution Deployment Manager, or if you are connecting Presence Services snap-in to the AE Services server using the AE Services connector.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Click **New**.
4. On the New Elements page, in the **Type** field, click **Application Enablement Services**.
5. In the General section, do the following:

   a. In the **Name** field, type the name of the application.

   b. In the **Description** field, add a description for this entity.

   This field is optional.

   c. In the **Node** field, type the IP address of the management interface of the AE Services server.

6. In the remaining required fields, enter the appropriate information.

   For more information, see “Adding an Application Enablement Services instance to System Manager field descriptions ”.

7. Click **Commit**.

Related links

Adding an Application Enablement Services instance to System Manager field descriptions on page 959

Adding G430 or G450 Branch Gateway to System Manager

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On the New Elements page, in **Type**, click **Media Gateways**.
5. On the New Media Gateway page, do the following:
   a. In **Name**, type the name.
   b. In **Node**, type **IP address of Media Gateway**.
   c. In **Device Type**, click either **Avaya G430** or **Avaya G450**.
   d. In **Access Profile**, configure the following parameters:
      - In **Name**, enter the name given for the gateway.
      - In **Access Profile Type**, select either **SSH** or **SNMP**.
   e. For **SSH** in **Access Profile Type**, do the following:
      - In **Login Name**, type the CLI login name of the gateway.
      - In **Port**, ensure that default value of the field is 22.
      - In **Password** and **Confirm password**, enter the password for the CLI login name.
   f. For **SNMP** in **Access Profile Type**, do the following:
      - In **Protocol**, select **SNMP** from the drop-down list.
      - In **Profile Name**, enter the profile name.
      - In **Description**, enter the description.
      - In **Type**, select either **V1** or **V3** from the drop-down list.
      - In **User**, enter the SNMP profile user name.
      - In **Authentication Type**, select one of the following from the drop-down list:
        - **None**
        - **MD5**
        - **SHA**
      - In **Authentication Password**, enter the SNMP profile Authentication password.
      - In **Confirm Authentication Password**, enter the SNMP profile Authentication password again.

- In **Privacy Type**, select one of the following from the drop-down list:
  - **AES**
  - **AES128**
  - **DES**
  - **None**
- In **Privacy Password**, enter the SNMP profile Privacy password.
- In **Confirm Privacy Password**, enter the SNMP profile Privacy password again.
- In **Privileges**, select one of the following from the drop-down:
  - **Read**
  - **Read/Write**
  - **None**
- In **Timeout**, ensure that default value is 5000.
- In **Retries**, ensure that default value is 3.
- Click **Save**.

For more information, see “Element details field descriptions”.

Note:

The following parameters of SNMP configuration must be identical in System Manager and G430 Branch Gateway or G450 Branch Gateway:

- Root access password
- SNMP protocol and encryption

6. Click **Commit**.

   On the Manage Elements page, the system displays the gateway that you added.

Related links

Element details field descriptions on page 944

Adding an Avaya Messaging profile for a user

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On the New Elements page, in **Type**, click **Officelinx**.
5. On the **General** tab, in the **Node** field, type the IP address or FQDN according to the configuration in the actual Avaya Messaging server.

System Manager uses these details to establish communication between System Manager and Avaya Messaging.

6. On the **Attributes** tab, provide the Avaya Messaging login name and password.
7. Click **Commit**.

   The system adds Avaya Messaging in System Manager.
8. On the Manage Elements page, click System Manager, and click **More Actions** > **Manage Trusted Certificates**.
9. On the Manage Trusted Certificates page, click **Add** to add a trusted certificate for the Avaya Messaging server.

   For information about adding trusted certificates, see “Adding trusted certificate”.

   For information about Avaya Messaging, see Avaya Messaging documentation on the Avaya Support website.

Related links

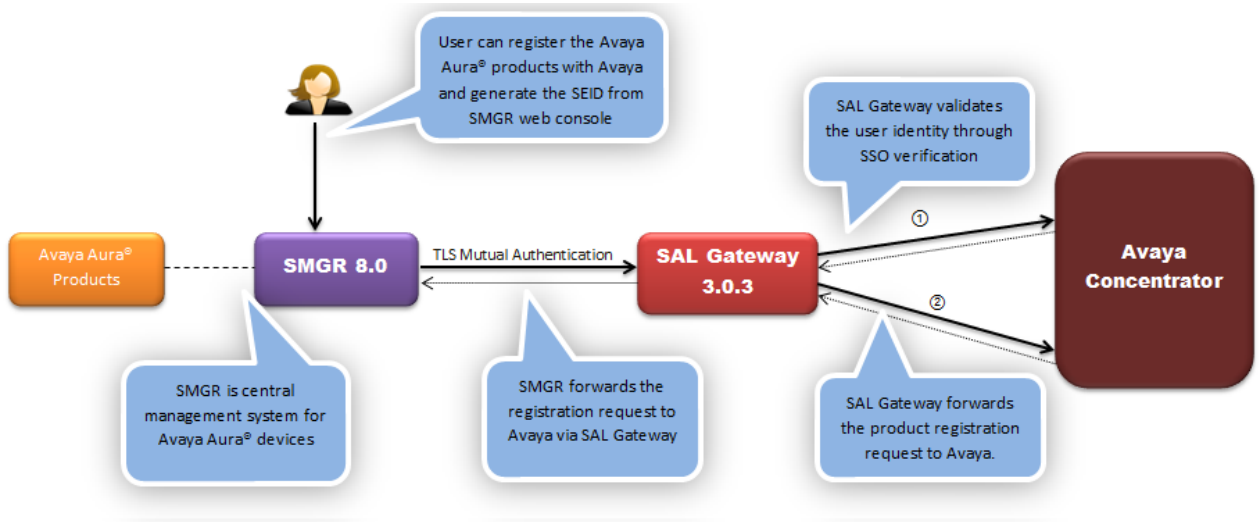
Element details field descriptions on page 944

Product Initiated Registration overview

With System Manager Release 8.0, you can register the Avaya Aura® products from the System Manager web console to make the products serviceability ready.

You can use the Manage Elements page of System Manager to configure the SAL gateway and register the product. After the product is registered, the system generates an SEID and you can view the registration status in the **Reg.Status** column on the Manage Elements page.

The following diagram depicts the product registration with System Manager and SAL Gateway:



For information about the:

- SAL gateway and the Product Initiated Registration feature, see *Administering Avaya Diagnostic Server SAL Gateway* on the Avaya Support website.
- Products that support the Product Initiated Registration feature through the System Manager web console, see *Secure Access Link Supported Products* on the Avaya Support website.

Configuring SAL Gateway

About this task

You can configure only one SAL gateway for a given System Manager application.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, click **More Actions** > **SAL Gateway configuration**.

   The system displays the SAL Gateway configuration page.
3. In **SAL Gateway Name**, type a generic name of the SAL gateway.
4. In **SAL Gateway Address**, type the FQDN or IP Address of the SAL gateway.
5. In **SAL Gateway Port**, type the port number of the SAL gateway.

   The default port is 7443.
6. In **Max Elements per request**, type the number of elements that you want to register to the SAL gateway.

   The maximum number of elements is 10.
7. In **Request timeout in minutes**, type the number of minutes after which the request times out.

   The maximum number of minutes is 90, which is the default value. The minimum number of minutes is 30.
8. To import the SAL gateway certificate, click one of the following:
   - **Import Certificate**.
   - **Services** > **Inventory** > **More Actions** > **Manager Trusted Certificates**
9. To check the SAL gateway connectivity, click **Test Connection**.
10. Click **Commit** to save the changes.

    The system displays the message: `SAL Gateway Configuration successful.`

Configuring Avaya Services registration

About this task

Use this procedure to register Avaya products with SAL Gateway.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select one or more element.

   You can select up to 10 elements or the number of elements configured in the **Max Elements per request** field.
3. On the Manage Elements page, click **More Actions** > **Avaya Services Registration**.

   The system displays the Product Registration page.
4. To validate the user identity and authenticate the user, in **SSO User Name**, type the SSO user name registered with Avaya.

   An SSO user must have permission to register products against the supplied **FL/Sold To** number.
5. To validate the user identity and authenticate the user, in **SSO User Password**, type the password of the SSO user.

   The system does not store the password.
6. In **FL/Sold To**, type the Functional Location number of the element.

   The Functional Location number must be of 10 digits.
7. Click **Commit** to save the changes.

   The system displays the registration status in the **Reg.Status** column on the Manage Elements page.

Viewing notification status

About this task

Use this procedure to view the notification status of the elements.

View Notification Status is available only on the primary or the secondary System Manager server that is in the active state.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, click **More Actions** > **View Notification Status**.

   System Manager displays the View Notification Status page with **Name**, **Event Type**, **Status**, **Last Updated Time**, and **Error**.
3. To resend the notification status, in the Notification Status section, select an event name, and click **Resend Notification**.

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.

If there is ongoing notification being sent in the background, the system displays a progress bar and removes the progress bar once the sending operation is complete or fails.

Viewing certificate add status of elements

About this task

When you add trusted certificates for:

- Multiple elements of same ElementType and Version, the system creates a job and you can view the certificate management job status.
- Single element, the system does not create a job.

Use this procedure to view the certificate management job status of the failed elements.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, click **More Actions** > **View Certificate Add Status**.

   System Manager displays the Certificate Management Jobs page with **Job Name**, **Job State**, **Total Elements**, **Failed Elements**, **Job Start Time**, and **Job End Time**.
3. To view the details, in the Certificate Management Job Status section, select a job name, and click **View**.

   System Manager displays the Failed Elements Detail For Job - <Job_Name> section with **Element IP**, and **Error Message**.
4. Click **Close** to close the Failed Elements Detail For Job - <Job_Name> section.
5. Click **Back** to return to the Manage Elements page.

Field descriptions

Manage Elements field descriptions

Name	Description
Name	The name of the element.

Table continues…

Name	Description
Node	The node on which the element runs. The IP address can be in the IPv4 or IPv6 format.
Type	The type of the element to which the element belongs. **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.
SEID	The number is generated after product registration for further configuration and investigation.
Reg. Status	The registration status of the element with the SAL gateway.

The system also provides the following fields when System Manager is configured with Geographic Redundancy.

Name	Description
Reachable	The state that specifies if the element is reachable from the current server. The values are Yes and No.
Managed by	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, you can click the icon.
Warning	A yellow triangle icon (⚠) if the system generates warnings. For more information, you can click the icon.

Note:

At any time, you can perform the **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.
Details	The Element Details page. Use this page to view the details of the selected element.

Table continues…

Button	Description
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 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 > **Manage Trusted Certificates**	The Trusted Certificates page. Use this page to view, add, export, and delete the trusted certificates for the element.
More Actions > **Manage Identity Certificates**	The Identity Certificates page. Use this page to view, export, renew, and replace the identity certificates for the element.
More Actions > **Manage**	An option to set System Manager to start managing the selected element.
More Actions > **Unmanage**	An option to set System Manager to stop managing the selected element.
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. If a notification is pending, the system displays the progress bar. 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. The valid statuses are **Completed**, **Failed**, and **Inprogress**. 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.
More Actions > **View Certificate Add Status**	The Certificate Management Jobs page. Use this page to view the certificate status of elements.
More Actions > **SAL Gateway configuration**	The SAL Gateway configuration page. Use this page to configure the SAL gateway.
More Actions > **Product Registration**	The Product Registration page. Use this page to register the Avaya products with SAL Gateway.
Advanced Search	The link to perform advance search. When you click on this link, System Manager displays the Criteria section.

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	Selects all elements in the table.
Select: None	Clears the selection for the users that you select.
Refresh	Refreshes the element information in the table.

Criteria

Name	Description
Select Search Criteria	The options are: • **Replica Node Host Name** • **Synchronization State** • **Last Synchronization Time**
Select Search Operator	The options are: • **Equals** • **Not Equals** • **Starts with** • **Ends with** • **Contains**
Enter Search to Text	Specify the search criteria.

Button	Description
-	Removes the additional search criteria fields. This field is enabled when the additional search criteria fields are added.
+	Adds the additional search criteria fields.
Clear	Clears the search criteria.
Search	Performs the search for the specified search criteria
Close	Closes the Criteria section.

Element details field descriptions

Note:

The fields on this page varies with the application that you manage.

General

Name	Description
Type	The application type whose instance you want to create.

The following field is available only for specific applications, such as Session Manager and Presence Services.

Name	Description
Select type of <application name> to add	The application type whose instance you want to create. For example, for Presence Services, you can select a standalone Presence Services or Presence Services on Avaya Breeze® platform.

Name	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. The IP address can be in the IPv4 or IPv6 format. **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

Name	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…

Name	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 the Application System Supported Protocol and Access Profile Details subsections in the Access Profile section 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:

Name	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:

Name	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:

Name	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.
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:

Name	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…

Name	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: • **AES**: For SNMP-based communication. • **AES128**: For SNMP-based communication. • **DES**: For SNMP-based communication. The default is **DES**. • **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. • **None** The default is None. • **Read/Write**: To perform GET and SET operations. • **Read**: To perform only the GET operation.
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.

The page displays the fields when you click **SNMP** in the **Protocol** field and **V1** in the **Type** field:

Name	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 available 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

Name	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.

Table continues…

Button	Description
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.

Name	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.

Name	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. 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. The IP address can be in the IPv4 or IPv6 format.

Table continues…

Name	Description
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. 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.

Table continues…

Name	Description
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.
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	Returns to the Import Elements page.

Add Communication Manager field descriptions

General Attributes

Name	Description
Name	The name of the Communication Manager instance. The Communication Manager name can be up to 256 characters.
Hostname or IP Address	For the Communication Manager instance, you can specify the host name or the IP address. The IP address can be in the IPv4 or IPv6 format. For duplex Communication Manager, this value references the active server host name or the IP address.
Alternate IP Address	The alternate IP address of the element. For duplex Communication Manager, the alternate IP address is the host name or the IP address of the standby server.
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 for the SSH or Telnet login name on the element.
Password	The password that authenticates the SSH or Telnet login name on the element.
Confirm Password	The password that you retype for confirmation. **Note:** **Confirm Password** must match **Password**.
ASG Key	The ASG key that authenticates the SSH or Telnet login name on the element. This field is only available if **ASG Key** is selected in **Authentication Type**.

Table continues…

Name	Description
Confirm ASG Key	The ASG key that you retype for confirmation. This field is only available if **ASG Key** is selected in **Authentication Type**. **Note:** **Confirm ASG key** must match **ASG key**.
SSH Connection	An option to use SSH for connecting to the element. By default, this check box is selected and the system uses SSH to connect to the element. If you clear the check box, the system uses Telnet to connect to the element.
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. You must include the prefix `SHA256:` before the RSA SSH Fingerprint. For example: `SHA256:`<Eb4qM3YEWONzZoLlhgle1s2Ena0A8qhy1z1oWk7Nahs>
RSA SSH Fingerprint (Alternate IP)	The RSA SSH key of the standby Communication Manager server. Use the RSA SSH key only for duplex servers. You must include the prefix `SHA256:` before the RSA SSH Fingerprint. For example: `SHA256:`<Ena0A8qhy1z1oWk7NahsYEWONzEb4qM3ZoLlhgle1s2>
Description	A description of the Communication Manager 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.

Table continues…

Name	Description
Port	The port on which the service provided by the element is running. The default SSH port is 5022. **Note:** From Communication Manager Release 7.1 and later, the telnet port 5023 is disabled. If the telnet port is configured for the Communication Manager element, select the **SSH Connection** checkbox. When you select this checkbox, the system populates the default port value to 5022.
Location	The location of the element.
Add to Communication Manager	An option to administer Communication Manager on System Manager. By default, **Add to Communication Manager** is selected.
CM Type	The type of the Communication Manager server. The options are: • **Standalone**: To add a standalone Communication Manager. • **Node**: Add node Communication Manager to a Communication Manager cluster. **Caution:** Do not select the **Node** option. This is for future use.

SNMPv1 Attributes

In the **Version** field, when you select **V1**, System Manager displays the following fields.

Name	Description
Version	The SNMP protocol type.
Read Community	The read community of the device.
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. The default value is 3.
Timeout (ms)	The duration of time in milliseconds for which an application polls a device without receiving a response before timing out. The default value is 5000 milliseconds.
Device Type	The Communication Manager application type. The options are: • Avaya Aura® **Communication Manager SP** for Communication Manager 6.3.100 on System Platform. • Avaya Aura® **Communication Manager VE** for Virtualized Environment-based Communication Manager 6.3.100 and Release 10.2.x.

SNMPv3 Attributes

In the **Version** field, when you select **V3**, System Manager displays the following fields.

Name	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** This is the default option. • **SHA** • **None**: If you select this option, System Manager does not display the **Authentication Password**, **Confirm Authentication Password**, and **Privacy Protocol** fields.
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 protocol users. The possible values are: • **AES128**: Use the AES encryption for the SNMP-based communication. This is the default protocol. • **DES**: Use the DES encryption for the SNMP-based communication. • **None**: Does not encrypt traffic for this user. If you select this option, System Manager does not display the **Privacy Password**, and **Confirm Privacy Password** fields.
Privacy Password	The pass phrase used to encrypt the SNMP data.
Confirm Privacy Password	Retype the privacy password in this field for confirmation.
Retries	The number of times the application polls a device without receiving a response before timing out. The default value is 3.
Timeout (ms)	The duration of time in milliseconds for which the application waits for the response from the device being polled. The default value is 5000 ms.
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 returns to the previous page.

Adding an Application Enablement Services instance to System Manager field descriptions

General

Name	Description
Name	The name of the Application Enablement Services instance.
Type	The type of the Application Enablement Services instance.
Description	The description of the AE Services server.
Node	The IP address/FQDN of the management interface of the AE Services server.

Port Details

Name	Description
Name	The name of the port to be used for the AE Services server.
Protocol	The protocol type supported by the port and the AE Services server. The options are: • http • https • jnp • rmi • tsapi
Port	The port number to be used for the AE Services server.
Description	The description of the port details.

Attributes

Name	Description
aes.aesMachineName.name	The hostname of the AE Services server.

Assign Elements

Name	Description
Assignment Name	The name to assign the Communication Manager instance to the AE Services server. **Note:** **Assignment Name** must be same as the Switch Connection name in the AE Services management console.
Name	The name of the Communication Manager instance.

Table continues…

Name	Description
Node	The IP address/FQDN of the management interface of the Communication Manager instance.
Type	The type of the Communication Manager instance.
Version	The version number of the Communication Manager instance.

Button	Description
Commit	Adds a AE Services instance in the inventory.
Save	Saves all the entries.
Cancel	Cancels your action and returns to the previous page.

Related links

Adding an Application Enablement Services instance to System Manager on page 935

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 IP address can be in the IPv4 or IPv6 format. 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. The IP address can be in the IPv4 or IPv6 format.
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.

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.

With the Serviceability Agent user interface, System Manager supports Command Line Interface (CLI) scripts for each serviceability task. Avaya offers this CLI support as an alternative to the Serviceability Agent user interface.

For more information, see Command line interface alternative to Serviceability Agents on page 979.

For more information on fault management using SNMP, see *Avaya Aura® System Manager SNMP Whitepaper*.

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 963
Configuration files in the MIBTOOL.jar file on page 963

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 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 965

Editing an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 965

Viewing an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 965

Deleting an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 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.

Table continues…

Name	Description
Authentication Protocol	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The possible values are: • MD5 • SHA The default is SHA.
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 returns 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 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 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 969

Viewing an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 969

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 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 969

Deleting an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 returns 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 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 973
Filter Profiles field descriptions on page 973

Assigning filter profile to a serviceability agent on page 972
Unassigning the filter profile from a serviceability agent on page 972

Viewing the notification filter profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 973
Filter Profiles field descriptions on page 973

Editing notification filter profiles

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 973
Filter Profiles field descriptions on page 973

Deleting the notification filter profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 973
Filter Profiles field descriptions on page 973

Assigning filter profile to a serviceability agent

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 972

Unassigning the filter profile from a serviceability agent

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 972

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 asterisk (.*), 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

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 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 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 976
Managing target profiles for the selected serviceability agents on page 975

Managing target profiles for the selected serviceability agents

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 975
Managing SNMPv3 user profiles for the selected serviceability agents on page 976

Managing SNMPv3 user profiles for the selected serviceability agents

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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 975
Managing target profiles for the selected serviceability agents on page 975

Managing the status of manage profile job for an agent

About this task

From Release 8.1, when you perform manage profile for more than one agent, the system creates a background job.

Use this procedure to view and retry the manage profile job for agents.

Manage Profile for single agent is the same. The system does not create a job for single agent.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. On the Serviceability Agents page, click **Manage Profile Job Status**.

   System Manager displays the Manage Profile Jobs page with **Job Name**, **Status**, **Total Agents**, **Failed Agents**, **Job Start Time**, and **Job End Time**.
4. To view the details, in the Manage Profile Jobs section, select a job name, and click **View Details**.

   System Manager displays the Failed Agents Detail For Job - <Job_Name> section with **Agent IP Address**, and **Error Details**.

   When you hover on **Job Name**, the system displays a brief description about the job, which target is added or removed, and which user is added or removed.
5. To retry the operation for the failed agent, perform the following:
   a. Select one or more agent IP Address.
   b. Click **Retry Operation**.

      System Manager displays the Serviceability Agents page with the list of the failed agents that you selected for retrying any operation.

      You can use the **Reset Table** button on the Serviceability Agents page to display all the agents.
   c. Click **Close** to close the Failed Agents Detail For Job - <Job_Name> section.
6. Click **Back** to return to the Serviceability Agents page.

Serviceability Agents field descriptions

Agent 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.

Table continues…

Name	Description
System OID	The system OID of the server on which the serviceability agent runs.
Status	The enabled or disabled status of the serviceability agent. The system disables SNMPv3 and displays **Inactive** as the default status.

Button	Description
Activate	Activates one or more Serviceability Agent.
Manage Profiles	Manages the target profiles for the selected serviceability agents.
Generate Test Alarm	Generates test alarms from the System Manager web console for agents, hosts, or elements that are installed with Serviceability Agents
Repair Serviceability Agent	Repairs the serviceability agent.
Manage Profile Job Status	Manages the profile job for the serviceability agent.
Reset Table	When you perform the retry operation on the Manage Profile Job Status page, System Manager displays the list of failed agents on the Serviceability Agents page. If you need to clear the list of failed agent list and display all the available agents in the Agent List section, use the **Reset Table** button.
Advanced Search	The link to perform advance search. When you click on this link, System Manager displays the Criteria section.
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 agents based on the filter criteria.
Select: All	Selects all agents in the table.
Select: None	Clears the selection for the agents that you select.
Refresh	Refreshes the agent information in the table.

Criteria

Name	Description
Select Search Criteria	The options are: • **Hostname** • **IP Address** • **System Name** • **Device Type** • **System OID** • **Target Profile** • **User Profile**

Table continues…

Name	Description
Select Search Operator	The options are: • **Equals** • **Not Equals** • **Starts with** • **Ends with** • **Contains**
Enter Search to Text	Specify the search criteria.

Button	Description
-	Removes the additional search criteria fields. This field is enabled when the additional search criteria fields are added.
+	Adds the additional search criteria fields.
Clear	Clears the search criteria.
Search	Performs the search for the specified search criteria
Close	Closes the Criteria section.

Command line interface alternative to Serviceability Agents

Avaya supports a CLI script for several Serviceability Agent user interface capabilities. You must log on using root or sroot. The location of the scripts is the following: `$MGMT_HOME/remoteSnmpConfig/utility`.

Avaya supports the following scripts:

- Create SNMP V3 user profile (createSnmpUserProfile.sh)
- List SNMP V3 user profiles (createSnmpUserProfile.sh)
- Create SNMP V2 or V3 target profile (createSnmpTargetProfiles.sh)
- List SNMP V2 or V3 target profiles (createSnmpTargetProfiles.sh)
- Detach target profile from serviceability agents (attachDetachSnmpTargetDest.sh)
- Attach target profile to serviceability agents (attachDetachSnmpTargetDest.sh)
- List target profile attached to agent (ListTargetsAgents.sh)
- List agents attached to target profile (ListTargetsAgents.sh)
- Create notification filter profile (createSnmpFilterProfile.sh)
- List notification filter profile (createSnmpFilterProfile.sh)

- Attach filter profile to target profile - serviceability agent (attachDetachSnmpTargetDest .sh)
- Detach filter profile to target profile - serviceability agent (attachDetachSnmpTargetDest .sh)
- List attached filter profile to a given target profile and servicablity agent IP Address (listAttachedFilterProfiles.sh)

To support these scripts, two logs provide information about the CLI script execution status. The logs indicate success or failure. They also provide a detailed message containing information about the reason if there is a failure.

The logs are available in the following locations:

- `/var/log/Avaya/mgmt/RemoteSNMPConfig/RemoteSNMPConfigAuditCLI.log`
- `/var/log/Avaya/mgmt/RemoteSNMPConfig/RemoteSNMPConfigTraceCLI.log`

Related links

Creating SNMP user profiles on page 980
Listing SNMP user profiles on page 981
Creating SNMP target profiles on page 981
Listing SNMP target profiles on page 982
Attaching and detaching target profiles from serviceability agents on page 982
Listing target profiles attached to agents on page 983
Listing agents attached to target profiles on page 983
Creating notification filter profiles on page 983
Listing notification filter profiles on page 984
Attaching or detaching filter profiles to or from target profile serviceability agents on page 984
Listing filter profiles attached to given target profiles and agent IP addresses on page 985

Creating SNMP user profiles

Procedure

1. Log in to System Manager as a cust user, then log in as a root user using the command `su -root`.
2. At the prompt, type `sh createSnmpUserProfile.sh -u <SNMP v3 username> -a <Authentication Protocol> -A <Authentication Password> -x <Privacy Protocol> -X <Privacy Password> -p <Privileges>` to run the command and press **Enter**.
   - -u: SNMP V3 username.
   - -a: Authentication protocol that can be MD5 or SHA.
   - -A: Authentication password.
   - -x: Privacy protocol that can be AES, DES, or None.
   - -X: Privacy password.
   - -p: Privileges that can be read (R), read/write (RW), or none.

- -h: Provides help for CLI.
- -l: Lists the available SNMP V3 user profile.

Related links

Command line interface alternative to Serviceability Agents on page 979

Listing SNMP user profiles

About this task

Use the standard CLI command to list the available SNMP V3 user profiles.

Procedure

1. Log in to System Manager as a cust user, then log in as a root user using the command `su -root`.
2. At the prompt, type `sh createSnmpUserProfile.sh -l` to run the command and press **Enter**.

Related links

Command line interface alternative to Serviceability Agents on page 979

Creating SNMP target profiles

Procedure

1. Log in to System Manager as a cust user, then log in as a root user using the command `su -root`.
2. At the prompt, type `sh createSnmpTargetProfiles.sh -n <Target profile name> -i <IP address> -p <Port number> -v <SNMP version> -u <username of existing user> -c <community string> -t <Inform/Trap> [-d <Description>]` to run the command and press **Enter**.
   - -n: Name of the target profile as seen on SMGR UI.
   - -i: Target IP address should be only IPV4.
   - -p: Target port number.
   - -v: SNMP version V2 or V3 (values can be 2 or 3).
   - -u: existing SNMP V3 username that is applicable only when the SNMP version(-v) is 3.
   - -c: SNMPv2 community string that is applicable only when the SNMP version(-v) is 2.
   - -t: Type (values can be Trap or Inform).
   - -d: [Optional] User comment that describes the target profile. This is optional.
   - -h: Provides help for CLI.
   - -l: Lists available V2/V3 target profiles.

Related links

Command line interface alternative to Serviceability Agents on page 979

Listing SNMP target profiles

About this task

Use the standard CLI command to list the available SNMP V2/V3 target profile.

Procedure

1. Log in to System Manager as a cust user, then log in as a root user using the command `su -root`.
2. At the prompt, type `sh createSnmpTargetProfiles.sh -l` to run the command and press **Enter**.

Related links

Command line interface alternative to Serviceability Agents on page 979

Attaching and detaching target profiles from serviceability agents

About this task

You can attach or detach up to five target profiles from the serviceability agents.

Procedure

1. Log in to System Manager as a cust user, then log in as a root user using the command `su -root`.
2. At the prompt, type `sh attachDetachSnmpTargetDest.sh -d <TargetName> -o <attachTargetProfile|detachTargetProfile> -a <AgentList>` to run the command and press **Enter**.
   - -d: An existing target profile name.
   - -o: The operation name. The possible values are attachTargetProfile or detachTargetProfile.
   - -a: The list of agents in the form of a comma-separated list of activated agent IP addresses. The maximum is 5.
   - -h: Provides help for CLI.

   If the agent list size is greater than one and more than one agent is active, then jobName will be non-empty for a successfully attached or detached target profile.

   If you execute the attach or detach operation for multiple active agents in a single command then the job is scheduled. To see the result, use the following script: `listTargetsAgents.sh`

   If there is an inactive agent, the response body contains an error message to indicate that an agent is in an inactive state.

Related links

Command line interface alternative to Serviceability Agents on page 979

Listing target profiles attached to agents

Procedure

1. Log in to System Manager as a cust user, then log in as a root user using the command `su -root`.
2. At the prompt, type `sh listTargetsAgents.sh -o listTargets -i <AgentIPAddress>` to run the command and press **Enter**.
   - -o: The operation name. This operation lists target profiles attached to the agent IP address that you enter in the CLI command.
   - -i: The agent IP address.
   - -h: Provides help for CLI.

Related links

Command line interface alternative to Serviceability Agents on page 979

Listing agents attached to target profiles

Procedure

1. Log in to System Manager as a cust user, then log in as a root user using the command `su -root`.
2. At the prompt, type `sh listTargetsAgents.sh -o listAgents -i <TargetProfileName>` to run the command and press **Enter**.
   - -o: The operation name. This operation lists the agents attached to the target profile that you enter in the CLI command.
   - -i: The target profile name.
   - -h: Provides help for CLI.

Related links

Command line interface alternative to Serviceability Agents on page 979

Creating notification filter profiles

Procedure

1. Log in to System Manager as a cust user, then log in as a root user using the command `su -root`.
2. At the prompt, type `sh createSnmpFilterProfile.sh -n <NotificationFilterProfileName> -d <Description> -p <Product Name> -c <Include|Exclude> -o <Notification OIDs>` to run the command and press **Enter**.
   - -n: Notification filter profile name.
   - -d: Description comment that describes the notification filter profile.

- -p: Product name.
- -c: Criteria that can be Include and Exclude.
- -o: Notification OIDs in a comma-separated list.
- -h: Provides help for CLI.
- -l: Lists the available notification filter profiles.

Related links

Command line interface alternative to Serviceability Agents on page 979

Listing notification filter profiles

Procedure

1. Log in to System Manager as a cust user, then log in as a root user using the command `su -root`.
2. At the prompt, type `sh createSnmpFilterProfile.sh -l` to run the command and press **Enter**.

Related links

Command line interface alternative to Serviceability Agents on page 979

Attaching or detaching filter profiles to or from target profile serviceability agents

About this task

You can only assign one filter profile to any agent-target combination.

Procedure

1. Log in to System Manager as a cust user, then log in as a root user using the command `su -root`.
2. At the prompt, type `sh attachDetachSnmpTargetDest.sh -d <TargetName> -n <Notification Filter Profile name> -o <attachTargetProfile|detachTargetProfile> -a <Comma separated up to 5 Agent IP Addresses>` to run the command and press **Enter**.

   Note:

   You can attach or detach the given filter profile to a target profile and up to five serviceability agents.

   - -d: Name of an existing target profile.
   - -n Name of an existing notification filter profile.
   - o Operation that can be attachTargetProfile and detachTargetProfile.
   - -a AgentList that is a comma-separated list of activated agent IP addresses up to a maximum of five.

- -h: Provides help for CLI.

Related links

Command line interface alternative to Serviceability Agents on page 979

Listing filter profiles attached to given target profiles and agent IP addresses

Procedure

1. Log in to System Manager as a cust user, then log in as a root user using the command `su -root`.
2. At the prompt, type `listAttachedFilterProfiles.sh -t <TargetProfileName> -a <AgentIPAddress>` to run the command and press **Enter**.
   - -t: Target profile name.
   - -a: Agent IP address.
   - -h: Provides help for CLI.

Related links

Command line interface alternative to Serviceability Agents on page 979

Synchronization of Data

Communication Manager, Messaging data, and IP Office synchronization

The elements that System Manager manages include alternative ways of administering data. To ensure uniformity in the database you can use the synchronization menu when a variety of tools are used. You can synchronize Communication Manager, Messaging, and IP Office data through this menu.

Communication System

Using System Manager, you can synchronize the System Manager data with Communication Manager. When you add Communication Manager to the system, System Manager automatically initiates synchronization to update the System Manager database.

Initializing synchronization

With initializing synchronization, you can synchronize the data in the System Manager database with each managed Communication Manager system. When you add Communication Manager to your deployment, System Manager automatically initiates an initialization task to get the required Communication Manager data and stores the data in the System Manager database.

Important:

If there is a update in any of the following Communication Manager objects in Communication Manager, you must start full initialization synchronization of this Communication Manager in System Manager:

- system-param special-applications
- 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

Note:

Bulk initialization synchronization of Communication Manager data can be performed successfully on less than 10 Communication Manager systems simultaneously.

Incremental synchronization

With incremental synchronization with selected devices, you can incrementally synchronize the 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 the synchronization was last run.

After the first initialization synchronization job is completed, System Manager schedules a recurring incremental synchronization job every 24 hours.

Incremental synchronization pulls all the incremental commands from the Communication Manager command history. In this context, incremental commands are commands which were performed on Communication Manager after the last Communication Manager synchronization by a Communication Manager user that is unavailable in the System Manager inventory.

Incremental synchronization does not pull the station if the station is added to Communication Manager by the same Communication Manager user that is available in the System Manager inventory.

Important:

In previous releases, an incremental synchronization was switched to an initializing synchronization for an upgraded System Manager or Communication Manager. In 10.2.1 onwards, this does not happen. If you try to run an incremental synchronization for an upgraded System Manager or Communication Manager, the synchronization stops, and an error message displays.

System Manager will now start an initializing synchronization instead of incremental synchronization in the following scenarios:

- The last initializing synchronization status is failed.
- If the count of command history is more than 1800.

Note:

If the CM notify sync feature is enabled on the system, then incremental synchronization does not synchronize Communication Manager commands processed by the CM notify sync feature.

Force initialize data synchronization

Use this feature to run the initializing synchronization forcefully. If you run the synchronization forcefully, System Manager performs the initial synchronization without checking for any data discrepancy between Communication Manager and System Manager.

If you select Communication Manager that has no data and System Manager that has data for the same Communication Manager available and run **Force initialize data sync for the selected devices**, all data present in System Manager is deleted.

IP Office system

With 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.

Messaging data

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

Note:

Before synchronization, you must add a new Communication Manager or a messaging entity from Manage Elements.

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

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

Related links

Running an initializing synchronization on page 988
Running an incremental synchronization on page 989
Saving the Communication Manager translations on page 992

Synchronizing the Communication Manager data and configuring options

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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.

     Optionally you can select **Force initialize data sync for the selected devices** to force an initializing sychronization.

     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**.

Running an initializing synchronization

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Synchronization** > **Communication System**.
2. On the Synchronize CM Data and Configure Options page, select the Communication Manager entities.

3. Select **Initialize data for selected devices**.
4. Do one of the following:
   - To perform the synchronization immediately, click **Now**.
   - To perform the synchronization at a specified time, click **Schedule**.

Running force initialize data synchronization

About this task

Initialization synchronization replaces or deletes all station data on System Manager. If you try to initialize synchronization using a Communication Manager with no data, an error message displays and the sychronization stops. This ensures that you do not accidentally delete the System Manager station data.

You can however, force the initialize synchronization.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Synchronization** > **Communication System**.
2. On the Synchronize CM Data and Configure Options page, select the Communication Manager system that you want to synchronize.
3. Select **Initialize data for selected devices**.
4. Select **Force initialize data sync for the selected devices**.
5. Do one of the following:
   - To perform the synchronization immediately, click **Now**.
   - To perform the synchronization at a specified time, click **Schedule**.

Running an incremental synchronization

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Synchronization** > **Communication System**.
2. On the Synchronize CM Data and Configure Options page, select the Communication Manager system that you want to synchronize.
3. Select **Incremental Sync data for selected devices**.
4. Do one of the following:
   - To perform the incremental synchronization immediately, click **Now**.
   - To perform the incremental synchronization at a specified time, click **Schedule**.

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 IP Office Application Server system configuration

About this task

Use the procedure to synchronize the configuration of a IP Office 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, perform the following:

- Configure VMPro IP Address in IP Office System Configuration.
- Password of VMPro should be same forIP Office, Application Server and VMPro System Preferences.

  Note:

  - You can change the password for Application Server 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 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 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 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 993
CM audit field descriptions on page 993

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.

Table continues…

Name	Description
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 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.

Note:

- The account synchronization feature updates the UPM CS 1000 communication profile with data from the CS 1000 element, and deletes the communication profiles that are linked to phones or mailboxes that do not exists in the CS 1000 element.
- If the data, such as, DN, mailbox, and TN has been modified on the CS 1000 element, the system provisions the data to System Manager UPM during account synchronization feature, but the CPND name and **Mailbox Number** are provisioned from System Manager UPM to the CS 1000 element.
- The system maps the CPND name of the CS 1000 element to the System Manager UPM user **Localized Display Name**.

Common scenarios are:

- If the System Manager UPM user first and last names are the same as the phone CPND name (For example: first = "John", last = "Smith", CPND = "John Smith" or CPND = "John, Smith" if display format = "first, last") on the CS 1000 element, then the system links the phone with this user and creates communication profile during the account synchronization process.
- If **Localized Display Name** is changed in the System Manager UPM user and this user has communication profile linked to the CS 1000 phones, the system immediately provisions the CPND name to the CS 1000 phone without using the account synchronization process.
- If the CPND name is changed on the CS 1000 element, the changes will be lost during the account synchronization process, and the system overwrites the CPND name by **Localized Display Name** from the System Manager UPM user.

Synchronizing the CS 1000 profile

Before you begin

Register all CS 1000 element on System Manager 6.2 or later.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the 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

Bulk importing of users on page 377
Exporting users in bulk from web console on page 381
Synchronize communication profiles field descriptions on page 997
Average duration of CS 1000 account operations on page 998

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 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 997

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 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 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 communication profile 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 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	The name of the CS 1000 system.
Status	The current status of the synchronization process. The possible values are: • **Queued**: The synchronization task is queued and runs automatically when once other synchronization tasks are complete. • **Running**: The synchronization is running. The system displays the status when you click **Start**. • **Stopping**: The synchronization stops when you click **Stop**. • **Aborted**: The system displays this status when the synchronization stops completely. • **PASS**: Indicates that the synchronization is complete. • **FAIL**: Indicates that the synchronization has failed. You can view the log files to get the details of failure.
Date	The date when the synchronization started.
Summary	The number of accounts: • Processed • Anonymous accounts • Added, updated, and deleted When no accounts are processed, this field displays `0 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 system.

Table continues…

Field	Description
Target	The customer number of the system for the element.
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 998

Average duration of CS 1000 account operations

Operation	Duration in seconds
Account add	9
Account update	1
Account delete	1
Account anonymous	0.1

Connection pooling

Connection pooling

Connection pooling facilitates reuse of port connections. You can use System Manager to create a connection pool to reserve port connections to perform administrative and maintenance tasks on Communication Manager. Through the web interface, you can reserve 0 to 60 port connections across all Communication Manager elements, depending on the System Manager profile. If you exceed the number of port connections that can be pooled, the system displays an error message.

Configuring Communication Manager Connection Pool

About this task

Use this page to create or edit the connection pools in the System Manager.

System Manager uses OSSI and PCTT port connections. Connection pooling in System Manager pools only PCTT port connections. PCTT port connections manage the cut-through and provisioning through Classic View.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Connection Pooling**.
3. Click **Communication System**.

   The system displays the Configure CM Connection Pool page.
4. In the **Connections Requested** field, type the number for each Communication Manager element in the table.

   Depending on the System Manager profile, the number can be between 0 and 60 port connections across all Communication Manager elements.

   Note:

   If you are configuring *n* connections in System Manager connection pooling, the **Maximum Number of Simultaneous logins for a user** field on the Communication Manager System Management interface must be *n*+1, so that Communication Manager allows you to acquire and pool all requested connections.
5. **(Optional)** To stop the connection pool, type 0 in the **Connections Requested** field.
6. Click **Commit**.

   The system:

   - Changes the **Status** field to Pooling Scheduled.
   - Displays the number of connections assigned to the CM element in the **Connections Attained** field.
   - Changes the **Status** field to Pooling Complete.
7. **(Optional)** To set a common pool size to all Communication Manager elements, perform the following:

   a. Select the **Set Common pool size for all the CMs** check box.

   b. In the **Set Common pool size for all the CMs** field, type the number for all Communication Manager elements in the table.

   c. **(Optional)** To stop the connection pool for all Communication Manager elements, type 0 in the **Set Common pool size for all the CMs** field.

   d. Click **Commit**.

      The system:

      - Changes the **Connections Requested** field to the number for all Communication Manager elements in the table.
      - Changes the **Status** field to Pooling Scheduled.
      - Displays the number of connections assigned to the Communication Manager element in the **Connections Attained** field.

- Changes the **Status** field to Pooling Complete.

Connection Pooling field descriptions

Name	Description
Set Common pool size for all the CMs	The field where the administrator sets a common number to reserve port connections for all Communication Manager elements. **Note:** If you are configuring *n* connections in System Manager connection pooling, the **Maximum Number of Simultaneous logins for a user** field on the Communication Manager System Management interface must be *n*+1, so that Communication Manager allows you to acquire and pool all requested connections.
Element Name	The name of the Communication Manager element.
Connections Requested	The number of port connections the administrator wants to reserves for the Communication Manager element. **Note:** If you are configuring *n* connections in System Manager connection pooling, the **Maximum Number of Simultaneous logins for a user** field on the Communication Manager System Management interface must be *n*+1, so that Communication Manager allows you to acquire and pool all requested connections.
Status	The status of the connection pool for the Communication Manager element. The options are: • NOT POOLED • POOLING SCHEDULED • POOLING COMPLETE
Connections Attained	The number of port connections the system is able reserves for the Communication Manager element.
Connections In Use	The number of port connections the system is using from the pool of connections.
Idle Connections	The number of port connections that are idle in the pool of connections.
Connections Used Outside Pool	The number of port connections that are outside the connection pool and are in use.

Button	Description
Commit	The system reserves a pool of connections between System Manager and Communication Manager.

Modifying the maximum number of simultaneous logins for a user

About this task

From Release 7.1, Communication Manager allows default five simultaneous connections for a user. Use the following procedure to change the maximum number of simultaneous logins for the user.

Procedure

1. Log on to the Communication Manager System Management interface.
2. Click **Administration** > **Server (Maintenance)**.
3. In the navigation pane, click **Security** > **Login Account Policy**.
4. In the **Login Limits** section, in the **Maximum Number of Simultaneous logins for a user** field, enter the new value.

   Note:

   If a user is configuring *n* connections in System Manager for Connection Pooling, you must set the value to *n+1*.

5. Click **Submit**.

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 14: 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 alarm status
- 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 generate 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 Network Management System (NMS). You can configure 6.1 elements with 6.1 SAL agent and 6.2 elements with 6.2 serviceability agent to directly send SNMP traps to a customer 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 and 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 961

Cluster level alarming

From Release 7.1.3, System Manager supports cluster level alarms. Using the cluster level alarms feature, the product-specific cluster type alarms generated from one node of the cluster are cleared from another node.

Note:

Cluster level alarming does not work along with alarm throttling.

Remote key server alarms

When you configure the remote key server and if any of the remote key servers are unavailable, System Manager generates the following alarms:

Alarm/Event ID	Severity	Alarm description
REMOTE_KEY_SERVER_ALARM	Major	Disk encryption key server <IP Address of the remote key server> not reachable.
ALL_KEY_SERVERS_DOWN_ALARM	Major	All configured disk encryption key servers not reachable.

Viewing alarms

Procedure

1. On the System Manager web console, click **Services** > **Events** > **Alarms**.
2. On the Alarming page, select the alarms that you want to view.
3. Click **View**.

   The Alarm - View Alarm Detail page displays the details of the selected alarms.

Changing the alarm status

About this task

Use this procedure to change the alarm status. Maintenance support must manually set the alarm to the required state.

The alarm status can be:

- **Raised**: Indicates the alarm is raised to notify about a system event.
- **Acknowledged**: Indicates the alarm is under investigation.
- **Cleared**: Indicates the error condition is resolved. The auto alarm clear event might result in the Cleared status.

Procedure

1. On the System Manager web console, click **Services** > **Events** > **Alarms**.
2. On the Alarming page, select the alarm and click **Change Status**.
3. Click the status that you want to apply to the selected alarms.

Exporting alarms

About this task

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** > **Alarms**.
2. On the Alarming page, do one of the following:
   - 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.
3. 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 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 to 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

About this task

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 criteria on the selected alarms.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the 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 matching records are found to the specified filter criteria.

Result

The system displays the alarms that match the filter criteria.

Searching for alarms

About this task

Use the Advanced Search function to find alarms based on certain specified conditions. The system displays 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 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 do the following:
   a. Select the AND or OR operator from the drop down field.
   b. Repeat steps 4 and 5.

   To delete a search condition, click **-**. You can delete a search condition if you add multiple search conditions.
7. To find alarms for the given search conditions, click **Search**.

Changing the throttle period from default 720 minutes to other period for specific alarm

About this task

You can configure the throttling period in minutes as a threshold for all alarms or alarms specific to events at spiritAgent service from Avaya Aura®. The system eliminates any redundant alarms raised within the configured period at spiritAgent service.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Open the `AlarmThrottle.properties` file from the `$SPIRIT_HOME/config/agent` location.
3. Set `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 `EPBaseRules_orig.xml` files of the specific product, which contain the events, and add the following lines:

   ```
   <tns:ExtraAttribute>
   <tns:ExtraAttributeName>alarmThrottleInterval</tns:ExtraAttributeName>
   <tns:ExtraAttributeValue>2</tns:ExtraAttributeValue>
   </tns:ExtraAttribute>
   ```

   For example, for System Manager, open the `Panther_EPBaseRules_orig.xml` files.

   You can apply the alarmThrottleInterval as the alarm throttle period for a specific event. If you do not use the generic and 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 spiritAgent service.
5. To disable alarm throttling, perform the following steps:
   a. In the `$SPIRIT_HOME/config/agent/AlarmThrottle.properties` file, set AlarmThrottlePeriod=-1.
   b. Restart spiritAgent service.

Configure a threshold to raise the System Manager backup alarm

Use this functionality to control how alarms are raised for backup and restore, and get notified when there is no successful backup since a long time.

Earlier, the system raised an alarm, if you did not schedule a System Manager backup every 7 days. Now you can configure a threshold for raising a Major alarm when no successful System Manager backup is taken since the configured number of days. The default value is still 7.

To view the alarm, navigate to **Services** > **Events** > **Alarms** screen.

The alarm message contains information on the number of days since the last successful System Manager backup.

`No successful backup taken for System Manager in the last $1 days” where $1 would be replaced by the configured number of days.`

Related links

Viewing the System Manager backup alarm threshold parameter on page 1008
Editing the System Manager backup alarm threshold parameter on page 1008

Viewing the System Manager backup alarm threshold parameter

Procedure

1. On the System Manager web console, click **Services** > **Configurations** > **Settings** > **SMGR** > **SMGR Element Manager**.
2. To view the parameter value, on the View Profile:SMGR Element Manager page, find the value in the **Alarm Threshold for number of days since last successful SMGR Backup (Days 1-30)** field.

Editing the System Manager backup alarm threshold parameter

Procedure

1. On the System Manager web console, click **Services** > **Configurations** > **Settings** > **SMGR** > **SMGR Element Manager**.
2. To change the parameter value, on the View Profile:SMGR Element Manager page, click **Edit**.
3. On the Edit Profile:SMGR Element Manager page, type a value in the **Alarm Threshold for number of days since last successful SMGR Backup (Days 1-30)** field.

   The configuration range is 1 through 30 days, and the default is 7.
4. Click **Commit**.

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 ADC test alarm.

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

Table continues…

Test Clear Event property	Value
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 1009
Generating the test alarm from CLI on page 1009

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 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 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 an alarm.
5. To view the alarm, click **Events** > **Alarms**.

   To view the alarm details, wait until the system displays the alarms on the Alarming page.

Generating the test alarm from CLI

Procedure

1. Log in to the computer where System Manager is installed.
2. At the command prompt, perform the following:
   a. To check the status of spiritAgent service, 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 spiritAgent service.

   b. To start spiritAgent service, type `service spiritAgent start` and press `Enter`.

      The `utils` directory contains spiritAgent service command line utilities.

3. To navigate to the `utils` directory, at the prompt, type `cd $SPIRIT_HOME/scripts/utils/`and press `Enter`.
4. Do 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`.
   - To generate alarms on other products, repeat steps 1 to 4. You can use the **Generate Test Alarm** button on the System Manager web console Manage Serviceability Agents page for generating test alarms for all elements, including System Manager, with a click.

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 primary and secondary System Manager entries.
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 secondary System Manager alarms that are in standby mode.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Type `sh $MGMT_HOME/alarmingui/scripts/DisplayAlternateDBAlarms.sh`.
3. At the prompt, type the number based on the action you want to perform.

   The options are:
   - (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)

System Manager displays the alarms according to your selected option.

AutoRefresh Alarm List 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.

Name	Description
Time Stamp	The date and time when the alarm is generated.
Severity	The severity of the alarm. The options are: • **Cleared**: Displayed as a status change for a raised alarm after the issue is rectified. • **Critical**: Displayed in red for critical failures that cause system or services to be non-functional and require immediate resolution and fix. • **Major**: Displayed in orange for failures that cause critical degradation of service and require immediate attention. • **Minor**: Displayed in yellow for failures that: - Cause degradation of service, but continue to support a crucial part of the system. - Require action, but the consequences of the failure are gradual. - Interfere with a feature or impair the services to trunks or stations. • **Warning**: Displayed in purple for failures that do not cause significant degradation of service. This alarm is not reported to the attendant console or Initialization and Administration System (INADS). • **Indeterminate**: Displayed in blue for an alarm that does not have any rules defined in the System Manager. It is displayed as a raw SNMP packet, as there is no information available in the System Manager for its description and severity. Hence, marked as **Indeterminate**.
Status	The current status of the alarm.
Host Name/SysName	The name of the host computer that generated the alarm.
Source IP address	The IP address of the system that generated the alarm.
Description	A detailed description of the problem that generated the alarm.
Identifier	The unique identifier for an alarm.

Table continues…

Name	Description
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 the trap listener service, 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

Name	Description
Time Stamp	The date and time when the alarm is generated.
Severity	The severity of the alarm.
Status	The current status of the alarm.
Host Name/SysName	The name of the host server that generated the alarm. For the trap listener service, this column displays the system name.
Source IP Address	The IP address of the system that generated the alarm.
Description	A 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 the trap listener service, 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	Displays the details of the selected alarms.

Table continues…

Button	Description
Change Status	Changes the status of the selected alarm. The options are: • **Raised** • **Cleared** • **Acknowledged**
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. This is 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 to search for 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. This is a toggle button.
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 alarms based on the filter criteria.
All	Selects all the alarms in the table.
None	Clears the check box selections.
Previous	Displays the logs in the previous page. This button is not available if you are on the first page.
Next	Displays 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 top-right corner of the page.

Name	Description
Criteria	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. Select the following search criteria from the first drop down list: • Time Stamp: Searches all 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. • Severity: Searches all alarms that match the specified severity level. • Status: Searches all alarms that match the specified status. • Host Name: Searches all alarms that are generated from the specified host. • M/E Ref Number: Searches all alarms that match the specified M/E Ref Number. • Event ID: Searches all alarms that match the specified Event ID. • Source IP address: Searches all alarms that are generated from the specified source IP address. • NotificationID: Searches all alarms that match the specified NotificationID. • Identifier: Searches all alarms that match the specified identifier. • Description: Searches all alarms that match the specified description. The operators available are based on the search criterion that you select in the first drop down field. The following operators are available for search criteria: • Time Stamp: =, >, <, >=, <=, >=, != • Severity: Equals, Not Equals • Status: Equals, Not Equals • Host Name: Equals, Not Equals, Starts With, Ends With, and Contains • Identifier: =, >, <, >=, <=, >=, != • Source IP address: Equals, Not Equals, Starts With, Ends With, and Contains • Event ID: Equals, Not Equals, Starts With, Ends With, and Contains • Description: Equals, Not Equals, Starts With, Ends With, and Contains • M/E Ref Number: Equals, Not Equals, Starts With, Ends With, and Contains When you select **Begin Date** and **End Date** from the first drop down list, you are prompted to enter the date in the third field.

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. It 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 a consistent presentation of log messages for System Manager and the adopters.

The log viewer displays a list of logs where you can view each log details, perform a search for logs, and filter specific logs. The log details include event information 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:

- Log Harvester: Through the Log Harvester menu, you can harvest log files for one or more products of the same or different types, running on the same or 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 you may 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 the 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. With a successful

harvest request related to a harvest profile, the logging service 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 or 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

On the System Manager web console, click **Services** > **Events** > **Logs** > **Log Harvester**.

Creating a new log harvesting profile

About this task

To harvest log files for products running on different servers, you must specify multiple filter criteria.

Before you begin

To create a new log harvesting profile, you must specify:

- The hostname of the server on which the product is running.

  If you do not see the hostname 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

Note:

By default, harvesting is enabled for System Manager. All other products should always integrate and install their log harvesting extension packs during System Manager installation.

After integration, they directly get their product type and files in System Manager in the drop down list on the Log Harvesting page.

Procedure

1. On the System Manager web console, click **Services** > **Events** > **Logs** > **Log Harvester**.
2. On the Log Harvester page, click **New**.
3. On the Create New Profile page, do the following:
   a. In **Profile Name**, type the profile name.
   b. In **Profile Description**, type a description of the profile.
4. Select 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 `CTRL` and click the item.
   - To add another log harvesting request for a different product, or another instance of the same product running on the same server or a different server, click plus (**+**).
5. **(Optional)** If you select one or more directories, in the **File Name Filter** field, type a text pattern as the filter criteria.

   During the harvesting operation, the system harvests those files that match the filter criteria.
6. Click **Save Profile** to save the profile and the log harvesting requests in the profile.

Related links

Create New Profile field descriptions on page 1024

Editing a log harvesting profile

Procedure

1. On the System Manager web console, click **Services** > **Events** > **Logs** > **Log Harvester**.
2. On the Log Harvester page, select a profile, and click **Edit**.
3. On the Harvest Criteria Edit page, modify the information in the **Profile Name** and **Profile Description** fields.
4. Modify 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 another instance of the same product running on the same server or a different server, click plus (**+**).

5. **(Optional)** If you select one or more directories, in the **File Name Filter** field, type a text pattern as the filter criteria.

   During the harvesting operation, the system harvests those files that match the filter criteria.

6. Click **Save Profile** to save the changes to the log harvesting profile.

Related links

Harvest Criteria Edit field descriptions on page 1025

Viewing details of a log harvesting profile

Procedure

1. On the System Manager web console, click **Services** > **Events** > **Logs** > **Log Harvester**.
2. On the Log Harvester page, select a profile, and click **View**.

   The Profile Criteria View page displays the details of the selected log harvesting profile.

3. Click **Done**.

Related links

Profile Criteria View field descriptions on page 1026

Viewing the harvested log files in an archive

About this task

Use this procedure to view the harvested log files of a product stored in an archive file.

Procedure

1. On the System Manager web console, click **Services** > **Events** > **Logs** > **Log Harvester**.
2. On the Log Harvester page, select a log harvesting profile, and click **Requests**.
3. On the Harvest Archives page, in the Harvest Request Details section, click a request in the table.
4. Click **Show Files**.
5. On the Search Archives page, navigate through the folders to view the harvested log files.

Deleting log harvest profiles

About this task

You cannot delete profiles that are in use by the Log Harvester service. If you attempt to delete profiles that are in use, System Manager displays an error message.

Procedure

1. On the System Manager web console, click **Services** > **Events** > **Logs** > **Log Harvester**.
2. On the Log Harvester page, select a profile, and click **Delete**.
3. On the Profile Delete Confirmation page, click **Delete**.

System Manager deletes all requests and 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 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** > **Logs** > **Log Harvester**.
2. On the Log Harvester page, select a log harvesting profile, and click **Requests**.
3. On the Harvest Archives page, type the relevant information in the **Archive Name** and **Archive Description** fields.

   The system saves the harvested log files in the specified archive file.
4. Click **Run Profile** to send a request.

   The table in the Harvest Criteria View section provides you the log harvesting request status. If the execution status of the request is successful, 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 1026

Viewing details of a log harvesting request

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the 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, in the Harvest Request Details section, click a request in the table.
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 1028

Searching for text in a log file

Use this feature to search for matching text in the product log file.

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 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, in the Harvest Request Details section, click a request in the table.
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 1028

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 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, in the Harvest Request Details section, click a request in the table.
5. If the system does not display any requests, submit a new request.
6. Click **Show Files**.

   The system lists the harvested log files.

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 1028

Downloading the harvested log files

About this task

You can download the harvested log files of one or more products stored in a zip file on the local server.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the 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, in the Harvest Request Details section, click a request in the table.
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 different servers.
   - If you select a host name of a server under a product, the system creates a zip file containing the harvested log files for the products running on the selected server.
   - 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 1028

Filtering log harvesting profiles

Use this feature to set filter criteria to view those log harvesting profiles that meet the set filter criteria. The titles of the table columns displaying the log harvesting profiles are the filter criteria.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the 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 match the specified filter criteria.

Filtering log harvesting requests

Use this feature to set filter criteria to view those log harvesting requests that meet 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 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 those log harvesting requests that match the specified filter criteria.

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	Displays the Harvest Archives page. You can use this page to view the details of a selected log harvest profile.
New	Displays the Create New Profile page. You can use this page to create a new log harvesting profile.
Edit	Displays the Edit Profile page. You can use this page to edit a log harvesting profile.
Delete	Deletes the selected profile. You cannot delete a profile if the profile is in use by the Log Harvester service.
Requests	Displays 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 to apply the filters without resetting the filter criteria. This is a toggle button.
Filter: Enable	Enables the filter and displays the fields under the columns in the table where you can enter the filter criteria. Only the columns on which you can apply the filter, display where 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.

Host Name	The host name of the servers on which products are installed.
	If you do not see the hostname 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>`
	After typing a minimum of three characters, wait for three seconds to capture the final keyword and fetch the required results.

Product	The products for which you can harvest logs.
Directories	A list of directories that contain 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 system filters the log files present in the selected directory for harvesting. When you select the `/a/b/c` directory and type `com` in this field, the harvest operation for this profile harvests the log files in the directory `/a/b/c`. The log files contain com in the file name. The field does not support wild cards.

Button	Description
+	Displays 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 install the products.
Product	Displays the products for which you can harvest logs.
Directories/Filter Text	Lists the directories containing the log files for the selected product.
Files	Displays the log files that you can harvest for the selected product.

Table continues…

Name	Description
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 returns 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	Displays 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	Displays 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 returns 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 compressed file.

Name	Description
Archive Name	The name of the archive file to create for storing 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 for storing harvested log files.
Request Time Stamp	The date and time when the log harvesting request is submitted.
Request Description	A brief description of log harvesting requests.
Status	The status of log harvesting requests. The options are: • SUCCESS: System Manager successfully harvests the log messages. • FAILURE: System Manager fails to harvest the log messages for the product. • PARTIAL SUCCESS: 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 contains 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 log harvesting requests for selected profiles.
View	Displays the View Harvest detail page to view the details of selected log harvesting requests.
Show Files	Displays the Search Archives page to: • Search for text contained in the harvested log files. • Download log files of one or more products running on the same or different servers. • View the contents of log files.
Filter: Disable	Hides the fields displayed under the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays fields under the column headers of the table that displays the log harvesting requests. You can enter the filter criteria in these fields. Only columns that can be filtered display the fields to enter the filter criteria. This is a toggle button.
Filter: Apply	Filters the log harvest profiles 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 to 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 if the contents of log files span across multiple pages.
Next	Displays the log file contents on the next page. This button is available if the contents of log files span across multiple pages.
Search	Searches for the text occurrences 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.

Table continues…

Name	Description
Status	Displays the status of log harvesting requests. The options are: • SUCCESS: System Manager successfully harvests the log messages. • FAILURE: System Manager fails to harvest the log messages for the product.
Request Description	Displays 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**: System Manager successfully harvests the log messages. • **FAILURE**: 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	Displays a brief description of 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 returns 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 to enter the filter criteria. This is a toggle button.
Filter: Apply	Filters the log harvesting requests based on the filter criteria.
Filter: Disable	Hides the fields displayed under the columns to apply the filters without resetting the filter criteria. This is 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 navigation pane, click **Logs** > **Log Settings**.

Result

The System Manager 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 navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, in the **Logger List**, click a log file.

Related links

Logging Settings field descriptions on page 1030

Logging Settings field descriptions

Use this page to view and edit loggers defined in a log file.

Log Settings

Name	Description
Logger List	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 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. From Release 8.1.3.3, this field is no longer used.
Attached Appenders > host	The name of the syslog host where the log output is stored. From Release 8.1.3.3, this field is no longer used.
Show All	An option to select the maximum number of logger records that you can view at a time.

Button	Description
Edit	Displays the Edit Logger page that you can use to edit loggers.

Related links

Viewing loggers for a log file on page 1030

Editing a logger in a log file

About this task

You can set log levels for loggers defining the level of logging the logger logs.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, in the **Logger List**, click a log file.
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, click **Info** in the **Log Level** of the specified log.

   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 1033

Assigning an appender to a logger

About this task

The appender where a logger logs the messages.

Procedure

1. On the System Manager web console, click **Services** > **Events**.

2. In the navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, in the **Logger List**, click a log file.
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 1034

Modifying an appender

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, in the **Logger List**, click a log file.
4. In the **Logger List** section, select a logger, and click **Edit**.
5. On the Edit logger page, in the **Attached Appenders** section, select an appender.
6. Click **Edit**.
7. On the Edit Appender page, modify the appender information.

   You can modify information in the **Threshold Log Level**, **Rotate File Size**, **File Path**, **Max Retention File Size**, and **Max Retention Time** fields.
8. Click **Commit**.

Related links

Edit Appender field descriptions on page 1033

Removing an appender from a logger

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, in the **Logger List**, click a log file.
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 for which the logger logs the information.

Attached Appenders

Name	Description
Appender	The name of the appender.
Threshold Log Level	The threshold log level set for the appender. Appender logs information of log type set in the threshold log level.
File Path	The path of the file where the appender logs the information.
Rotate File Size	The file size for rotation of the log file. The file size unit can be in KB or MB. The value for the file size must be from 1 through 100MB.
Max Retention File Size	The maximum retention file size for the log file. The file size unit can be in KB or MB. The value for the file size must be from 1 through 100MB.
Max Retention Time	The maximum retention time for the log file. The value for the retention time must be from 1 through 180 days.

Button	Description
Edit	Displays the Edit Appender page. Use this page to modify the appender information.
Attach	Displays 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 returns you 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. **Note:** You can view this information.
Appender	The name of the appender. **Note:** You can view this information.
Threshold Log Level	The threshold log level set for the appender. Appender logs information of log type set in the threshold log level.
Rotate File Size	The file size for rotation of the log file. The file size unit can be in KB or MB. The value for the file size must be from 1 through 100MB.
File Path	The path of the file where the appender logs the information.
Max Retention File Size	The maximum retention file size for the log file. The file size unit can be in KB or MB. The value for the file size must be from 1 through 100MB.
Max Retention Time	The maximum retention time for the log file. The value for the retention time must be from 1 through 180 days.

Button	Description
Commit	Saves the changes to the database.
Cancel	Closes Edit Appender page and returns you 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 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 returns 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 that generated the log, the severity level of the log, and other relevant information. You can search for logs based on search conditions and set filters to view logs that match the filter criteria. Log viewer displays logs that are of type Audit.

Viewing log details

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the 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 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 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 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 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. To add another search condition, click **+** and repeat steps 4 through 6.

   Click **-** to delete a search condition. You can delete a search condition if you have more than one.
7. 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.
8. 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 selected log details, 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 column title to sort the column data 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.

Table continues…

Name	Description
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**: The 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 of 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 generating the message, usually the process name and process ID.
Facility	The operating system, processes, and applications quantify messages into one of several categories. These categories generally consist of the generating facility, along with the severity of the message. The following are the types of supported facilities: • User-Level Messages • Security/authorization • Log Audit

Button	Description
View	Displays 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. This is a toggle button.
More Actions > **Export Selected**	Exports the selected logs to a CSV file. You can view the logs using Wordpad or Excel.

Table continues…

Button	Description
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 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. This is a toggle button.
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 logs based on the filter criteria.
Select: All	Selects all the logs in the table.
Select: None	Clears the selections.
Previous	Displays the logs on the previous page. This button is not available if you are on the first page.
Next	Displays the logs on 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 the 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, and service. • Severity: Severity level of the log. • Message: Brief description of the log. • Event ID: Unique identification number assigned to the event. • Process Name: Process on the device generating 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 consist of the generating facility with the severity of the message. The second drop down list displays operators. Based on the search criteria that you select in the first drop down field, those applicable for the selected criteria 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. Enter the date in MM/DD/YYYY format. You can select the date from the Calendar. 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 that uniquely identifies the component generating the log. For example, product, device, application, and service. 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**: The 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 do not indicate logging severities.
Event ID	The unique identification number assigned to the event generating the log.
Message	Brief description of 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.

Table continues…

Name	Description
Facility	The operating system, processes, and applications quantify messages into one of several categories. These categories consist of the generating facility 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.

Audit Logging

Configuring audit logging

About this task

You can use the functionality to configure actions when the system encounters conditions such as:

- Audit failure
- 75% occupation of the audit partition
- 90% occupation of the audit partition

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the navigation pane, click **Logs** > **Audit Log Configuration**.
3. On the Audit Logging Configuration page, enter the relevant information in the fields.

   For more information, see “Audit Logging Configuration field descriptions”.
4. Click **Commit**.

Audit Logging Configuration field descriptions

Name	Description
Action on Audit Failure	Field to select an action, which is performed after the audit failure.
To Email Address on Audit Failure	Email address to which the notification is sent.
Action on /var/log/audit partition 75% full	Field to select an action, which is performed after 75% occupation of the audit-assigned partition.

Table continues…

Name	Description
To Email Address on /var/log/audit partition 75% full	Email address to which the notification is sent.
Action on /var/log/audit partition 90% full	Field to select an action, which is performed after 90% occupation of the audit-assigned partition.
To Email Address on /var/log/audit partition 90% full	Email address to which the notification is sent.
Email	Option to send an email notification to the configured email address.
Trap	Option to record an entry in the trap log file and send an email notification to the configured address.
JBoss Server Shutdown	Option to shutdown the Application server and send a notification to the configured address.

Button	Description
Commit	Saves and commits any changes made in the audit logging configuration.

configureSyslog command

With System Manager Release 8.1.3.3, you can configure, list, and delete the remote syslog server by using the **`configureSyslog`** command.

Syntax

```
configureSyslog -h [-e] [-s <syslog server destination> ""]
```

-h

Displays help for the command and also displays the required and optional parameters.

-e

Lists the currently configured remote syslog servers.

-s <*syslog server destinations*>

Configures one or more of the remote syslog server destinations.
When you run this command, System Manager replaces the existing remote syslog server configuration and does not add into it.
syslog server destinations is a pipe ('|') separated list of remote syslog destinations.

Where, the format for *syslog server destinations* is:

(transport_specifier)hostname_or_ip:port

- *transport_specifier* can be:
  - @ for UDP
  - @@ for TCP
  - @@@ for one-way TLS (CA certificate only)

- @@@@ for two-way TLS with client certificate authentication (Mutual TLS)

- *hostname_or_ip*: The host name or IP address of the remote syslog server. The IP Address can be either in the IPv4 or IPv6 format. If you are using IPv6 then provide it in square brackets .
- *port*: The port of the remote syslog server.

If you are using TLS, certificates for remote syslog server must be managed through the System Manager web console.

-s "" Removes all the configured remote syslog servers.
When the -s is followed by an empty string with in double quotes (""), System Manager deletes all the configured remote syslog server.

Configuring remote syslog server from CLI

About this task

From System Manager Release 8.1.3.3, you can configure the remote syslog server by using the **`configureSyslog`** command. You can configure one or more remote syslog servers at a time. For entering more than one remote syslog server, each of the remote syslog server entry must be pipe separated.

Before you begin

- If the one-way TLS authentication (Server certificate authentication) is required, then add the CA certificate of the remote syslog into the System Manager trust store (select **SYSLOG** in **Select Store Type to add trusted certificate**).

  For information, see “Adding trusted certificates”.

- If two-way TLS authentication (Mutual TLS authentication) is required then you must also add CA certificate, corresponding to the identity certificate used by System Manager syslog service, to the trusted store of the remote syslog server.

  For information, see “Replacing an identity certificate”.

  Note:

  For the two-way TLS authentication (Mutual TLS authentication):

  - When you fresh deploy System Manager Release 10.1 and later, add the rsyslog sever details in the `/etc/hosts` file before running the **`configureSyslog`** command.
  - When you upgrade System Manager to Release 10.1 and later from 8.1.x, ensure to add the rsyslog sever details in the `/etc/hosts` file of System Manager 8.1.x.

  Use the **`editHosts`** command to modify the `/etc/hosts` file on System Manager. For information, see “editHosts”.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.

2. Based on the authentication type, do one of the following:
   - To configure remote syslog server that is using the UDP protocol, type the following:

     ```
     configureSyslog -s @<hostname_or_ip:port>
     ```

     For example, to configure remote syslog server (IP Address 1.2.3.4 and Port 514) that is using the UDP protocol, type the following:

     ```
     configureSyslog -s @1.2.3.4:514
     ```

     For example, to configure two remote syslog servers that is using the UDP protocol, type the following:

     ```
     configureSyslog -s "@1.2.3.4:514|@5.6.7.8:514"
     ```
   - To configure remote syslog server that is using the TCP port, type the following:

     ```
     configureSyslog -s @@<hostname_or_ip:port>
     ```

     For example, to configure remote syslog server (IPv6 Address [2000:1::4] and Port 514) that is using the TCP protocol, type the following:

     ```
     configureSyslog -s @@[2000:1::4]:514
     ```
   - For one-way TLS authentication (Server certificate authentication), type the following:

     ```
     configureSyslog -s @@@<hostname_or_ip:port>
     ```

     For example, to configure remote syslog server (IP Address 1.2.3.4 and Port 6514) that is using the one-way TLS authentication, type the following:

     ```
     configureSyslog -s @@@1.2.3.4:6514
     ```

     Add the CA certificate to syslog_truststore.
   - For two-way TLS authentication (Mutual TLS authentication), type the following:

     ```
     configureSyslog -s @@@@<hostname_or_ip:port>
     ```

     For example, to configure remote syslog server (IP Address 1.2.3.4 and Port 6514) that is using the two-way TLS authentication, type the following:

     ```
     configureSyslog -s @@@@1.2.3.4:6514
     ```

     Add the CA certificate to syslog_truststore and certificate to syslog keystore.

Related links

editHosts on page 1521
Replacing an identity certificate on page 1214
Adding trusted certificates on page 1205

Viewing remote syslog server configuration from CLI

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.

2. Type the following command:

   ```
   configureSyslog -e
   ```

   System Manager displays the list of configured remote syslog servers.

   For example:

   ```
   get for rsyslog completed successfully.
   SUCCESS:@@1.1.1.1:514|@@@2.2.2.2:6514
   ```

   In this example, one remote syslog server is using the TCP protocol and the other remote syslog server is using one-way TLS authentication.

Deleting the remote syslog server configuration from CLI

About this task

You cannot remove one remote syslog server. When -s is followed by an empty string with in double quotes (“”), System Manager deletes all the configured remote syslog servers.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Type the following command:

   ```
   configureSyslog -s ""
   ```

   System Manager deletes the remote syslog server configuration and displays the following message:

   ```
   SUCCESS:Successfully deleted all profiles from /etc/rsyslog.conf
   set for rsyslog completed successfully.
   ```

TrapListener service

The TrapListener service receives traps and informs from different applications and displays on the System Manager Alarming page.

- TrapListener receives V2c and V3 traps and informs 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. Attach the System Manager SNMPv3 user profile to the System Manager target profile, and 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 897
View Profile: TrapListener field descriptions on page 898
Serviceability Agents on page 961

Chapter 15: 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 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) website 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 the 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 1053

Finding LAC for System Manager in PLDS

About this task

You can find License Activation Code (LAC) using a Group ID or a SAP order number. With LAC, you can activate the available associated entitlements.

Procedure

1. Log in to the PLDS at https://plds.avaya.com.
2. From the Assets menu, select **View Entitlements**.
3. In the **Application** field, select **System Manager**.
4. Do one of the following:
   - To search using group ID, in the **Group ID** field, enter the appropriate group ID.

     Note:

     All group IDs are numeric without any leading zeros.
   - To search using the SAP order number, click **Advanced Search**, and in the **Sales/ Contract #** field, enter the SAP order number.
5. Click **Search Entitlements**

   The system displays the LAC(s) in the search results.

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. Use the Uninstall functionality to remove the license file from the WebLM server.

Licenses installed for WebLM Release 7.1 and later must support a SHA256 digital signature and 14–character host ID.

There is a limit of 50 licenses per WebLM server.

Note:

If you have a mix of Communication Manager Release 6.3.x, 7.x, 8.x, and 10.1.x software with Communication Manager 6.3.x, 7.x, 8.x, and 10.1.x license files, use the Communication Manager 10.1.x license file for all the Communication Manager Release software.

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 web console with administrator privilege credentials.
- For the standard license file, remove the older license file before you install the new file.

  Note:

  WebLM displays an error message if an older license file is still available.

  For a centralized license file, the system automatically overwrites the older license file during installation.

For information about the license file installation errors while installing the license file, see *Administering standalone Avaya WebLM*.

Procedure

1. In the navigation pane, click **Install license**.
2. On the Install license page, 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 the successful installation of the license file. The installation of the license file might fail for reasons such as the following:

- 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.
- An acquired license does not cover a licensed feature or product.
- An over-installation of licenses. In this scenario, free the already acquired licenses and retry installing the new license file. You could also try uninstalling the existing installed license file and installing a new license file.

Related links

Install license field descriptions on page 1053

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 web console with administrator privilege credentials.
- 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 navigation pane, in **Licensed products**, click the required product.
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, centralized licensing ID, license owner, license host, and license file host IDs for the element.

Related links

View License Capacity field descriptions on page 1054

Viewing peak usage for a licensed product

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the license file on the WebLM server for the licensed product.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
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 centralized licensing ID for the element.

Related links

View Peak Usage field descriptions on page 1055

Uninstalling a license file

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. In the navigation pane, click **Uninstall license**.
3. On the Uninstall license page, select the required license file.
4. Click **Uninstall**.
5. On the Uninstall License Confirmation page, click **Uninstall**.

   If you do not have permission to uninstall the selected license file, the system only displays the **Cancel** button.

Related links

Uninstall license field descriptions on page 1061

Viewing the server properties

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

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 1062

WebLM Home field descriptions

If the TLS version is set to TLS 1.0 or TLS 1.1, the WebLM Home page displays the following message:

```
Warning! TLSv1 or TLSv1.1 is enabled.
For increased security, it is recommended that the Minimum TLS Version
be set to TLS 1.2 or higher if these protocol levels can be supported
in your configuration.
```

You can view information about the products and associated license files installed on the WebLM server.

Name	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. The options are: • **solution** (Avaya Subscription License) • **standard** • **enterprise**
Date of Installation	The date and time of installing the license file.
Active License Mode	The type of license file installed for the product.
License State	The status of the installed license file.
Avaya Subscription License Available	The availability status of the Avaya Subscription license.
Standard License Available	The availability status of the standard license.

Button	Description
Export All Licenses	Exports the licenses to the `/tmp/all_licenses.zip` file on the WebLM server.

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

Name	Description
License File Host IDs	The host ID of the license file.

The following fields are applicable for the Solution license:

Name	Description
Active License Mode	The type of license active on WebLM. The default value is **Avaya Subscription**. The WebLM server can have Avaya Subscription and Standard (Perpetual) licenses installed. However, at a time only one license can be active. These licenses are used while switching between two modes.
License State	The status of the Avaya Subscription license. The default value is **Granted**.
Avaya Subscription License Available	The availability status of the Avaya Subscription license on WebLM. The default value is **Yes**.
Standard License Available	The availability status of the standard license on WebLM. The default value is **No**.

Licensed Features

You can view the total number of feature licenses in the license file and the current usage of those licenses.

Name	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.
Licensed capacity	The number of licenses for each licensed feature. WebLM fetches the number of feature licenses information from the license file. For the Solution license, the value is **Metered**.
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.

Name	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.
Acquirer ID	The unique identifier 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

You can view information about the usage of feature licenses of a licensed application at different time intervals.

For the Solution license, the usage fields shows the number of used license file, but not the percentage (%) of usage.

Name	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. For the Solution license, the value is **Metered**.
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 (today): qty	The highest number of feature licenses for each licensed feature used for the day.
Peak Usage (Last 7 days): qty/%	The highest number of feature licenses for each licensed feature used in the last seven days. 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%.

Table continues…

Name	Description
Peak Usage (Last 30 days): qty/%	The highest number of feature licenses for each licensed feature 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.

Button	Description
Back	Cancels the action and returns to the previous page.

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 supports centralized licensing feature so that products can have multiple license files installed for multiple instances of the product. On a single WebLM server, you can install multiple license files of a product 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:

To install the Communication Manager license file version 10, if the customer has Communication Manager license file with version 8.x or older and the license file was generated before June 22, 2023, see PSN020578u Avaya Aura Communication Manager Centralized Licensing Changes.

Enabling centralized licensing

Before you begin

Install a product license file that supports centralized licensing. Centralized licenses contain the FEAT_WLM_CENTRALIZED feature in the product license file.

About this task

By default, centralized licensing is disabled. You must enable centralized licensing to use this feature.

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. In the navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. Click **Enable Centralized Licensing**.

   Warning:

   After enabling the Centralized Licensing feature for a product, you must link the license file to the associated product server instance. If you do not link the license file to a product server instance, the product 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 element instance.
Centralized Licensing ID	The element identifier for an element instance. The Centralized Licensing ID must match the name used by an element instance to acquire licenses from WebLM. See the product documentation to find the name used by the element instance.
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 hostname of the license, as defined in the license file.
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 hostname of the license, as defined in the license file.
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 files.

Button	Description
New	Adds an element instance and the mapping of an element to a license file.
Edit	Edits the properties of the element instance.
Delete	Deletes an element 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 to assign to an element instance.

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. In the navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. Click **New**.
4. On the Add Element Instance page, type the element display name and the centralized licensing ID of the instance. For more information, see “Element instance field descriptions”.

   The element ID must match the name used by an element instance to acquire licenses from WebLM. See the product documentation to find the name used by the element instance.
5. In the **Select License File** table, select the license file to map to the element instance.
6. Click **Save**.

You can add an element instance and choose to map the license file later. In this scenario, you must type the element display name, the centralized licensing ID, and click **Save**.

Note:

If you select the license file already assigned to an element, WebLM displays the following warning message:

```
Assigning Multiple Centralized Licensing IDs/Element IPs to same license.
```

Related links

Element instance field descriptions on page 1060

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 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**.

   Note:

   If you select the license file already assigned to an element, WebLM displays the following warning message:

   ```
   Assigning Multiple Centralized Licensing IDs/Element IPs to same license.
   ```

Related links

Element instance field descriptions on page 1060

Deleting an element instance

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. In the 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.
Centralized Licensing ID	The element identifier for an element instance. The Centralized Licensing ID must match the name used by an element instance to acquire licenses from WebLM. See the product documentation to find the name used by the element instance.

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.
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 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. • **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 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 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.

Name	Description
License Host Name	The WebLM server where the license files are installed.
Host ID	The host ID of the license file.
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

Server Host ID

Name	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 14 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.

Adopter application cannot communicate with WebLM Server

Cause

Due to higher security settings on the WebLM Server Release 7.1 system, the adopter applications that are using WebLM Server earlier to Release 7.1 might not communicate with WebLM Server to fetch the license file from WebLM Server by using the WebLM client.

Solution

To fetch the license file from the WebLM Server Release 7.1 system, locate the `trusted_weblm_certs.jks` file from the adopter application system, take the backup of the file, delete the file, and then restart the adopter application.

Do this if the adopter application cannot communicate with WebLM Server regardless of the WebLM Server version on the adopter system.

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 can be configured as master WebLM but cannot be configured as local WebLM to an external WebLM.

Standalone WebLM OVA-based deployment can be configured as master WebLM or local WebLM.

No other WebLM flavor can be configured as master WebLM.

	Enterprise Master WebLM	Enterprise Local WebLM
System Manager WebLM	Yes	No
Standalone WebLM OVA-based deployment	Yes	Yes
Other WebLM flavors	No	Yes

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. In the 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 1072
Enterprise Usage field descriptions on page 1079

Retrieving the local WebLM certificate from browser

About this task

Use this procedure to retrieve the local WebLM certificate from the Firefox browser.

Procedure

1. On the web browser, type the local WebLM server URL, `https://<Fully Qualified Domain Name>:<PortNumber>/WebLM`.
2. On the address bar, click the Lock icon.
3. Click the Show connection details icon.
4. Click **More Information**.
5. Click **View certificates**.
6. On the Certificate dialog box, do the following:
   a. Click the **Details** tab.
   b. Click **Export**.
   c. Save the certificate to your local computer.

Adding local WebLM certificate as trusted certificate in System Manager

About this task

To add standalone WebLM as local WebLM in System Manager (master WebLM), you must add local WebLM certificate to the truststore of System Manager.

Before you begin

Download the local WebLM certificate using the browser.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select one or more elements, and click **More Actions** > **Manage Trusted Certificates**.

3. On the Manage Elements page, select System Manager, and click **More Actions** > **Manage Trusted Certificates**.
4. On the Manage Trusted Certificates page, click **Add**.
5. On the Add Trusted Certificates page, in **Select Store Type to add trusted certificate**, select the store type as **TM_INBOUND_TLS**.
6. Click **Import from file**.
7. Type the file name or click **Browse** to select a file.

   Note:

   System Manager validates the file type. If you provide an invalid file type, the system displays an error message.
8. Click **Retrieve Certificate**.
9. Click **Commit**.
10. To restart the Application server, type `smgr restart`.

    During a restart the System Manager web console will be unavailable for 10-15 minutes.

Adding a local WebLM server

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- 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 navigation pane, in **Licensed products**, click the required product.
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”.
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 1074

Modifying a local WebLM server configuration

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the enterprise license file.
- Add at least one local WebLM server.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
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 1075

Removing a local WebLM server

Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the enterprise license file.
- Add at least one local WebLM server.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
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 want to delete.
4. Click **Delete**.

   Note:

   The system displays a warning message before removing the local WebLM server from the master WebLM server.

5. Click **OK**.

Related links

Delete local WebLM field descriptions on page 1077

Viewing the license capacity of the licensed features of a product

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View by feature**.

Related links

View by feature field descriptions on page 1071

Viewing the connectivity status of the local WebLM servers

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
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 1071

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 1074

Viewing usage by WebLM

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
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 1078

Viewing enterprise usage of a license feature

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
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 1079

Viewing the periodic status of the master and local WebLM servers

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Periodic status**.

   The system displays the Periodic Status page.

Related links

Periodic Status field descriptions on page 1083

Querying usage of feature licenses for master and local WebLM servers

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
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 1079

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 navigation pane, in **Licensed products**, click the required product.
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 1082

Viewing allocations by features

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Allocations** > **View by feature**.

   The system displays the Allocations: View by Feature page.

Related links

Allocations by Features field descriptions on page 1080

Viewing allocations by the local WebLM server

Before you begin

Log on to the WebLM web console with administrator privilege credentials.

Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
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 1081

Viewing usage summary

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, in **Licensed products**, click the required product.
3. Click **Usages**.

   The system displays the Usage Summary page.

Related links

Usage Summary field descriptions on page 1077

View by feature field descriptions

Name	Description
License File Host IDs	The host ID of the license file.

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.

Table continues…

Name	Description
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.
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

Name	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

Name	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, 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

Name	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.

Table continues…

Name	Description
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.
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 returns 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 1077

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.

Table continues…

Name	Description
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. 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

You can 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.
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 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.

Table continues…

Name	Description
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

You can 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.

Table continues…

Name	Description
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.
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.
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.
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.

Metering Collector configuration overview

With Release 8.1.2, you can manage the Avaya Subscription license on the WebLM server when metering collector is registered with WebLM. The metering collector configuration is applicable only for the Avaya Subscription license. The Solution-Avaya Subscription license contains more than one application.

Using the metering collector configuration, the WebLM server tracks the license usage information from the deployed applications. The WebLM server provides the license information to the metering collector when metering collector requests.

Related links

Metering Collector Configuration field descriptions on page 1084
Deleting the metering collector configuration on page 1084

Metering Collector Configuration field descriptions

If the metering collector is not registered with WebLM, the system displays the following message:

```
No Metering Collector currently configured for this WebLM.
```

```
Metering Collector is required for Avaya Subscriptions and is configured
via the Metering Collector UI.
```

Name	Description
Name	The name of the metering collector. Each collector has its own unique metering collector id, which is displayed as **Name** on the WebLM server.
URL	The URL of the metering collector. It contains the IP Address or FQDN of the metering collector.
Link Status	The status of the collector link. Default value of the status is **Active**. The options are: • **Active** • **Error** WebLM checks the connectivity status in every 12 hours from the time last communication takes place with registered metering collector. If the metering collector does not send a request to WebLM for at least 24 hours, then the link status is displayed as **Error**.
Last Status Date/Time	The last synchronization timestamp of the metering collector with the WebLM server. The value is in the MM/DD/YYYY hh:mm:ss format.

Button	Description
Delete	Deletes the metering collector configuration.

Related links

Metering Collector configuration overview on page 1083

Deleting the metering collector configuration

Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, click **Metering Collector Configuration**.
3. On the Metering Collector Configuration page, click **Delete**.

The system displays the message: `Are you sure you want to delete the collector configuration?`

4. Click **Ok** to delete the metering collector configuration.

Related links

Metering Collector configuration overview on page 1083

Chapter 16: 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 1091

Viewing replica nodes in a replica group

About this task

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 1092

Repairing a replica node

About this task

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.

From Release 8.1, you can repair more than one replica nodes of a replica group.

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 to 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 one or more replica node, and click **Repair**.

   The **Synchronization Status** column displays the data replication status for the selected replica node.

Related links

Replica Nodes field descriptions on page 1092

Repairing all replica nodes in a replica group

About this task

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 1095

Removing a replica node

About this task

From Release 8.1, you can remove more than one replica nodes from a replica group.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, select the replica group from which you need to remove a node, and click **View Replica Nodes**.
3. On the Replica Node page, select one or more replica nodes, and click **Remove**.

Removing a replica node from the queue

About this task

From Release 8.1, you can remove more than one replica nodes from the queue of a replica group.

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, select one or more replica node, and 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 Polling`: 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. 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

Table continues…

Name	Description
	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 Capable	Displays whether the replica node is GR-capable 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	Displays 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 selected nodes from the replica group.
Remove From Queue	Removes the selected replica node from the queue.
Show All Replica Groups	Returns to the Replica Groups page.
Advanced Search	The link to perform advance search. When you click on this link, System Manager displays the Criteria section.
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 replica nodes based on the filter criteria.
Select: All	Selects all replica nodes in the table.
Select: None	Clears the selection for the users that you select.
Refresh	Refreshes the replica node information in the table.

Criteria

Name	Description
Select Search Criteria	The options are: • **Replica node name** • **Synchronization time** • **Synchronization Status**

Table continues…

Name	Description
Select Search Operator	The options are: • **Equals** • **Not Equals** • **Starts with** • **Ends with** • **Contains**
Enter Search to Text	Specify the search criteria.

Button	Description
-	Removes the additional search criteria fields. This field is enabled when the additional search criteria fields are added.
+	Adds the additional search criteria fields.
Clear	Clears the search criteria.
Search	Performs the search for the specified search criteria
Close	Closes the Criteria section.

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.

Table continues…

Name	Description
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 Capable	Displays whether the replica node is GR-capable 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 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.

Table continues…

Name	Description
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 • 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.

Button	Description
Refresh	Refreshes the Replication Node details.
Done	Returns to the Replica Nodes page.

Chapter 17: Managing reports

Reports

Avaya Aura® System Manager supports the Reports feature for communication objects. System Manager has about 350 predefined List and Display Communication Manager configuration reports.

You can use this feature to:

- Generate Communication Manager object reports in various formats, such as CSV, PDF, HTML, and Other (.txt with delimiter).
- Create and manage reports.
- Edit report parameters.
- Rerun reports.
- Customize the report contents.
- Save reports in the System Manager server.
- View and delete reports 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 the specific custom user.

Reports Generation field descriptions

Name	Description
Used Space	The maximum space allocated for storing the generated reports. If the report files exceed the maximum file size of 1 GB, the system generates an alarm. You must manually delete some files before you can generate a new report. On the **Services** > **Configurations** > **Settings** > **Reports** > **Configuration** page, you can configure **Reports Output Directory Properties**. For more information, see View Profile:Configuration field descriptions.

Reports Definition List

Name	Description
Name	The name of the report.
Host Name(s)	The Communication Manager instance from which the report was 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 was generated.
Object	The Communication Manager object used for generating the report.

Button	Description
Edit	Displays the Edit Report Definition page to edit the selected report.
New	Displays the New Report page to create a new report.
Run Now	Runs the selected report immediately.
Delete	Deletes the selected report.
Filter: Enable	Displays fields 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: Clear	Clears the filter criteria.
Filter: Apply	Filters reports based on the criteria.

Related links

View Profile:Configuration field descriptions on page 877

Accessing the tabs main buttons, feature buttons, expansion/module buttons, and softkeys buttons

About this task

From System Manager Release 10.1.3 and later, the following tabs are not available in the detailed report:

- **Main Buttons**.
- **Feature Buttons**.
- **Expansion/Module Buttons**.
- **SoftKeys Buttons**.

Procedure

1. On the System Manager web console, navigate to **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**.

2. On the Endpoints page, click **More Actions** > **Export All Endpoints** option to generate the detailed report with **Main Buttons**, **Feature Buttons**, **Expansion/Module Button**, and **SoftKeys Buttons**.

Generating a detailed report

About this task

You can generate a detailed report from the System Manager database.

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the 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 the **Detailed (Database)** option to generate the report for Communication Manager objects in the database.
8. Select a report type from the **Report Type** list.
9. On the Detailed Report page, in the **Available Fields** section, select the fields to include in your report.
10. Click .

    The **Selected Fields** table displays the selected fields. By default, some fields are already available in the **Selected Fields** column.
11. Click **Next**.
12. On the Report Parameters page, complete the report parameters and click **Generate Report**.

    You can generate a **Detailed (Database)** report if the initializing synchronization for the specific Communication Manager instances is successful. Otherwise, report generation fails.
13. To download and view the report, click **Services** > **Reports** > **History**.

Related links

New Report field descriptions on page 1102

Generating a basic report

About this task

When the report generation job runs, the basic report takes real-time data from the Communication Manager.

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the navigation pane, click **Generation**.
3. On the Reports Definition List page, click **New**.
4. On the New Report page, in the **Application** list, select **Communication Manager**.
5. From the Communication Manager table, select one or more Communication Manager instances.
6. Click **Next**.
7. To generate a report directly from Communication Manager, click **Basic (List and Display)**.
8. On the Basic Report page, in the **Report Type** list, select the report type.

   You can generate a **List**, **Display**, or **Status** report.
9. In the **Communication Manager Object** list, select a Communication Manager object 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 generate a **Basic** report if the initializing synchronization for the specific Communication Manager instances is successful. Otherwise, report generation fails.
13. To download and view the report, go to **Services** > **Reports** > **History**.

Related links

New Report field descriptions on page 1102

New Report field descriptions

New Report

Name	Description
Application	The application type for which you want to generate the report.
Name	The name of the element instance you choose to generate the report.
Host	The Communication Manager system you select to generate the report.
CM Type	The type of Communication Manager system.

Basic (List and Display)

Name	Description
Report Type	The report type. You can generate a **List**, **Display**, or **Status** report for the Communication Manager object.
Communication Manager Object	The Communication Manager object you select to generate the report.
Name	The name of the element instance you choose to generate the report.
Host	The Communication Manager system you select to generate the report.
Qualifier	The qualifier for the Communication Manager object you select to generate the report.

Detailed (Database)

Name	Description
Report Type	The Communication Manager object you choose to generate the report.
Available Fields	The fields you want to generate as part of the report. The fields vary according to the Communication Manager object you choose.
Selected Fields	The fields you select from **Available Fields**. The report you generate displays the fields in **Selected Fields**.

Button	Description
Move selected columns to right	Moves selected fields to the right in the **Selected Fields** column.
Move selected columns to left	Moves selected fields to the left in the **Available Fields** column.
Move all columns to right	Moves all the fields to the right in the **Selected Fields** column.
Move all columns to left	Moves all the fields to the left in the **Available Fields** column.
Reset to default columns	Resets your selection. The Communication Manager system displays the default fields when you click **Reset to default columns**.
Move Up	Moves up the selected field by one position in the **Selected Fields** column.

Table continues…

Button	Description
Move Down	Moves down the selected field by one position in the **Selected Fields** column.

Report Parameters

Name	Description
Report Name	The name of the report. Type a name of your choice in the **Report Name** field.
Select file format	The formats of the report output are the following: • **CSV** • **PDF** • **HTML** • **Other (.txt with delimiter)** Basic reports such as **List**, **Display**, and **Status** type support the following file formats: • List type report supports file formats such as CSV, PDF, HTML, and Other (.txt with delimiter). **Note:** List type reports support the given file formats, except for some in CSV format. • Display and status type report supports file formats PDF and HTML. • Detailed (Database) report supports file formats such as CSV, PDF, HTML, and Other (.txt with delimiter).
Select delimiter	The delimiter to apply while generating the report. The options are the following: • **comma** • **semicolon** • **space** • **tab**
Append to existing report	The data appended to the existing report.
Append date to Report File	The date appended to the report file.

Table continues…

Name	Description
Select destination location	The location to save the generated report. The options are: • **Local** (Path : /swlibrary/reports_data): The option to save the generated report to your local computer. By default, the path is `/swlibrary/reports_data`. • **Remote Server**: The option to save the generated report to a **Remote server**. Do one of the following: - Select the **Remote Server** from the field to store your reports. - Select the field to store the reports: • **Name** • **IP** • **Type** • **Remote Server From** • **Default Server** • **Email**: The option to enter one or more email addresses to send the report. To enter multiple email addresses, separate them by a semicolon.
Customize Report	The option to create a customized report. Click one of the following: • **Customize Report Header**: The option to choose the title of your choice. • **Export Column Titles on First Row**: The 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.

Table continues…

Name	Description
Schedule Job	The scheduler options to schedule the report generation job. Click one of the following: • **Now**: To generate the report immediately. • **Later**: To generate the report at the scheduled time. **Note:** • The **Edit report** always displays the default value for **Schedule Job** as **Now**. The following are the example scenarios of **Schedule Job**: • Schedule the job to run daily at 9 AM for 5 occurrences. After 2 days, edit the report at 11 AM and set the **Schedule Job** value to **Now**. After the job report is edited, the start time changes to 11 AM automatically and the report job is scheduled to run daily at 11 AM for 5 occurrences. • Schedule the report to run daily at 9 AM with an end date October 6, 2025. Edit the report on October 7, 2025 at 11 AM and select the **Schedule Job** value to **Now**. Enable the Report job again to run daily at 11 AM with no end date. If you want to stop generating the report, disable or delete the report manually. • To generate new report, select **Run Now** in **Report Generation** page. A new job is generated and the job is disabled once the report is generated.

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 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 the 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 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 report creation.

Customizing reports

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, do 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 the **Basic Report**.
6. In the **Basic Report** section, select one or more Communication Manager instances and do one of the following actions:
   - Select **Basic (List and Display)**, and do the following actions:
     a. Select the type of report 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. Some columns are available by default in the **Selected Fields** table.

7. Click **Next**.

   The system displays the Report Parameters page.
8. In the **Customize Report** field, select the **Customize Report Header** to add a name of your choice to the report.
9. Select **Export Column Titles on First Row** to export the column titles that the system displays on the report output.
10. 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 **Services** > **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 navigation pane, click **History**.
3. Perform one of the following actions:
   - From the **Reports History** table, select the report you want to download and click **Download Report**.
   - In the **Reports 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 1108

Reports History field descriptions

Name	Description
File Name	The name you type while generating a report.
Format	The format in which the report is generated.
Creation Date	The date of creating the generated report.
Created By	The name of the user who generated the report.
Object/CM Command Used	The Communication Manager command that you use to create this report. • For Basic Reports, the column shows the Communication Manager command used. • For Detailed Reports, the column shows the **Object** command used.
File Size	The size of the report file in KB.
Status	The status of the report. The options are: • **SUCCESS** • **FAILURE**: Displays the reason for the failed report.

Button	Description
Download Report	Downloads the selected report to your local computer.
Email Report	Displays the Email Report page to enter one or more email addresses to send the report history. You can enter multiple email addresses separated by a semicolon.
Delete	Displays the Report History Delete Confirmation page to delete the selected report.

Related links

Downloading reports on page 1107

Configuring email properties

About this task

Use this procedure to set up the email configuration for receiving email notifications from System Manager instances.

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the 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, do the following.
   a. In the **Enable email notification** field, type `true`.
   b. In the respective fields, type the appropriate values.

      For more information, see “View and Edit Profile SMGR field descriptions.”
5. Click **Commit**.

Note:

After you configure an email, the Email Host's response determines the operation to send an email based on this configuration. If the Email Host does not respond, there is a delay in sending the email.

For example, user creating/updating process or generating/sending reports depends on response time of the Email Host, if the sending alarm option is enabled.

Note:

The System Manager does not support SMTPS for sending reports through email.

Configuring the External Admin Connect Properties

About this task

Use this procedure to configure the System Manager with the Avaya Infinity™ server.

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the navigation pane, click **Settings** > **SMGR**.
3. On the View Profile:SMGR page, click **Edit**.
4. On the Edit Profile:SMGR page, in the External Admin Connect Properties section, do the following.
   a. In the **External Admin Connect** field, type `true`.
   b. In the respective fields, type the appropriate values.

      For more information, see “View and Edit Profile SMGR field descriptions.”
5. Click **Commit**.

Sending reports through email

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the 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 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 entered email addresses, click **Clear**.

Deleting reports

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the navigation pane, click **History**.
3. From the **Reports 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 navigation pane, click **Settings** > **Reports** > **Configuration**.
3. Click **Edit**.
4. On the Edit Profile:Configuration page, configure the following:
   - Alarm Properties
   - Cleanup Properties
   - Output Directory Properties

5. Click **Commit**.

Related links

View Profile:Configuration field descriptions on page 877

Remote server configuration

Adding a remote server

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the navigation pane, click **Reports** > **Remote Server Configuration**.
3. On the Remote Server Configuration page, click **New**.
4. On the Add Server page, complete the remote server details.
5. Click **Commit**.

Viewing the details of a remote server

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the navigation pane, click **Reports** > **Remote Server Configuration**.
3. On the Remote Server Configuration page, select the server to view its details.
4. Click **View**.

   You can view the remote server details 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 navigation pane, click **Reports** > **Remote Server Configuration**.
3. On the Remote Server Configuration page, select the server to edit its details.
4. Click **Edit**.
5. On the Edit Server page, edit the remote server details.
6. Click **Commit**.

Deleting a remote server

Procedure

1. On the System Manager web console, click **Services** > **Reports**.
2. In the navigation pane, click **Reports** > **Remote Server Configuration**.
3. On the Remote Server Configuration page, select the server or servers that you want to delete.
4. Click **Delete**.
5. On the Confirmation page, click **Delete**.

Add Server field descriptions

Name	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 to retype.

Button	Description
Commit	Adds or edits the changes to the remote server.
Clear	Clears all changes that you perform.
Cancel	Cancels your current action.
Edit	Edits the remote server configuration details.
Done	Saves the remote server configuration changes.

Remote Server Configuration field descriptions

Name	Description
Name	The name of the remote server.
IP	The IP address of the remote server.

Table continues…

Name	Description
Type	The type of remote server: • SCP • SFTP
Default Server	The default server.
Creation Date	The date of creating the remote server.

Button	Description
New	Displays the Add Server page to add a new remote server.
Edit	Displays the Edit Server page to edit the remote server configuration details.
View	Displays the View Server page to view the remote server configuration details.
Delete	Deletes the selected remote server.

Chapter 18: 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.

By default, the following jobs are in **Enabled** state after System Manager is installed.

- **LogPurgeRule**

- **ClrdAlarmPurgeRule**
- **AgedAlarmPurgeRule**

For a better system performance, ensure that these jobs remain in an **Enabled** state.

Note:

It is recommended not to disable the above jobs manually. If you find the above jobs in a **Disabled** state, change their state to **Enabled**. For more information on “Enabling a job”, see Enabling a job on page 1122.

Note:

The system Scheduled job "sys_ConfRefreshConfig" will be disabled from System Manager 10.1.3.3 and 10.2.0.1 or higher if "Meeting Exchange and Conferencing 6.0" is not configured. Enable the job "sys_ConfRefreshConfig" from **Scheduler** > **Completed Jobs** once the "Meeting Exchange and Conferencing 6.0" element is configured.

Note:

The System Manager creates the following default jobs:

Serial Number	Job Name	Description
1	UserMgmtJob	The UserMgmtJob performs user management tasks in User Profile Manager (UPM). The tasks are executed in sequence and may take a long time to complete. The UserMgmtJob performs the following actions: • Disables the inactive communication profiles. • Sends notification for the communication profile password expirations. • Disables the inactive administrative users.
2	CRLExpirationCheckerJob	The CRLExpirationCheckerJob is a system-scheduled job that runs once per day. The job detects and deletes the expired Certificate Revocation Lists (CRLs).
3	AVPLicenseUpdateJob	The AVPLicenseUpdateJob is a system-scheduled job that runs once per day. The job validates, updates, and applies AVP license information on the AVP device to ensure continuous service availability.

Table continues…

Serial Number	Job Name	Description
4	PurgeJobStatus	The PurgeJobStatus is a system-scheduled job that runs once per day. The job cleans up scheduled job execution status records. The job performs the following actions: • Saves the most recent execution record. • Retains the latest failure record. • Removes older failed status records.
5	AgedAlarmPurgeRule	The AgedAlarmPurgeRule is a system-scheduled job that rotates aged alarm records. The job identifies alarm records older than the configured retention threshold and archives or purges them as configured.
6	ExpiredCertificateRemovalJob	The ExpiredCertificateRemovalJob is a system-scheduled job that runs once per day to delete expired certificates. The job calculates a cutoff date by subtracting the configured retention period (in days), from the current date and deletes all expired certificates older than this cutoff date.
7	AgedSchedulerCompletedJobsPurgeRule	The AgedSchedulerCompletedJobsPurgeRule Job is a system-scheduled job that runs once per day. The job purges completed scheduler jobs that exceed the retention period that the Data Retention settings define.
8	PurgeAgedExportUserJobDataRule	The PurgeAgedExportUserJobData Rule Job is a system-scheduled job that runs once per day. The job purges export user records that are older than 30 days. The job deletes entries when the creation date or the end date-time exceeds 30 days. This cleanup improves system performance. The cleanup also reduces slow loading of the Export Users page under the **User Select** option.

Table continues…

Serial Number	Job Name	Description
9	REPORTS_CleanUp_System_Job	The REPORTS_CleanUp_System_Job is a system-scheduled job in System Manager that automatically removes old reports to manage storage space. The job deletes reports that exceed the configured retention period, helping prevent unnecessary data accumulation and maintaining optimal system performance. This job supports the following functions: • **Storage Management**: Prevents System Manager storage from being filled with outdated reports. • **Performance Optimization**: Improves system efficiency by removing large volumes of old report data. • **Compliance**: Supports regulatory or organizational policies by allowing administrators to configure report retention periods. The job runs according to configured schedule, for example, once per day. Administrators can configure the retention period, such as deleting reports that are older than 30 days.
10	IPOFFICE_MAINTENANCE	The IPOFFICE_MAINTENANCE is a system job used by IP Office to remove stale ABG information from the database. The job removes following outdated data from the table: • `cscommprofile` • `abgcommprofile` • `abg_parkandpage_info_abg_parkandpage` • `abg_parkandpage` • `abg_parkandpage_info`
11	LogPurgeRule	The LogPurgeRule Job is a system-scheduled job that runs once per day. The job rotates audit log records. The job archives or purges the records based on the configured retention policy.
12	ClrdAlarmPurgeRule	The ClrdAlarmPurgeRule is a system-scheduled job that runs once per day. The job rotates alarm records that are marked as cleared. The job archives or purges the records based on the configured retention policy.

Functions of the User Management scheduled job

Using the User Management scheduled job, you can:

- Notify users about the communication profile credentials of newly created UPM user.
- Notify users about the login credentials of newly created user.
- Notify users about the reset communication profile password.
- Notify users about their service or account inactivity and the date when it will be disabled.
- Notify users about their service or account disabled status.
- Notify users about account locked status.
- Notify users about password change or reset.
- Notify users about communication profile password change or reset.
- Warn users about password expiration.
- Notify users about expired password status.

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. With the privileges, users with administrator credentials can create custom roles.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the 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. 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 **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 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 1123

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 1125

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, click **Pending Jobs**, select a pending job, and click **More Actions** > **View Log**.
   - To view logs for a competed job, click **Completed Jobs**, 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, click **Scheduler** > **Pending Jobs**, and click **Filter: Enable**.
   - To filter completed jobs, click **Scheduler** > **Completed Jobs**, and 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, click **Pending Jobs**, select a pending job, and click **Edit** or click **View** > **Edit**.
   - To edit a competed job, click **Completed Jobs**, select a pending 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

Ensure that 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. To remove a pending job, click **Pending Jobs** in the left navigation pane.
   a. 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**.
      - If the job that you want to delete is in the enabled state, disable the job. See Disabling a job on page 1122 on how to disable a job.

   b. Click **Delete**.

   c. On the Delete Confirmation page, click **OK**.

      System Manager deletes the selected job from the database.

3. To remove a competed job, click **Completed Jobs** in the left navigation pane.
   a. On the Completed Jobs page, select a completed job.

      If the job that you want to delete is in the enabled state, disable the job.
   b. Click **Delete**.
   c. On the Delete Confirmation page, click **OK**.

      System Manager deletes the selected job 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. To disable a pending job, click **Pending Jobs** in the left navigation pane.
   a. On the Pending Jobs page, select a pending job and click **More Actions** > **Disable**.
   b. On the Disable Confirmation page, click **Continue**.

   The **State** of the selected job changes to **Disabled**.
3. To disable a completed job, click **Completed Jobs** in the left navigation pane.
   a. On the Completed Jobs page, select a completed job and click **More Actions** > **Disable**.
   b. On the Disable Confirmation page, click **Continue**.

   The **State** of the selected job 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. 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**.

The system displays `Enabled` in the **State** column of the selected job.

3. 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 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.

Table continues…

Name	Description
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.
Element	The element name for which the job is executed. For example, Communication Manager and its IP, if the job is for some specific Communication Manager.

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.
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 1119
Scheduler on page 1114

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.

Table continues…

Name	Description
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.
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 1119
Scheduler on page 1114

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.

Table continues…

Name	Description
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	Displays the Logging page that you can use to view the logs for the selected job.
Edit	Displays 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 1114

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 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.

Table continues…

Name	Description
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 1114

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

Table continues…

Name	Description
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 returns 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.

Table continues…

Name	Description
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 returns to the Pending or completed Jobs page.

Related links

Scheduler on page 1114

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.

Table continues…

Name	Description
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 returns to the Pending Jobs page.

Related links

Scheduler on page 1114

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 returns to the Pending or completed Jobs page.

Related links

Scheduler on page 1114

Chapter 19: 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 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 1147

Editing CM Agent template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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 1147

Viewing CM Agent template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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 1147

Deleting CM Agent template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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 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 1147

Adding CM Endpoint templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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

New Endpoint / Template field descriptions on page 743

Editing CM Endpoint templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **CM Endpoint**.
3. Select one or more 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

New Endpoint / Template field descriptions on page 743

Viewing CM Endpoint templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **CM Endpoint**.
3. Select one or more 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

New Endpoint / Template field descriptions on page 743

Deleting CM Endpoint templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the navigation pane, click **CM Endpoint**.
3. Select one or more 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 navigation pane, click **CM Endpoint**.
3. Select one or more 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

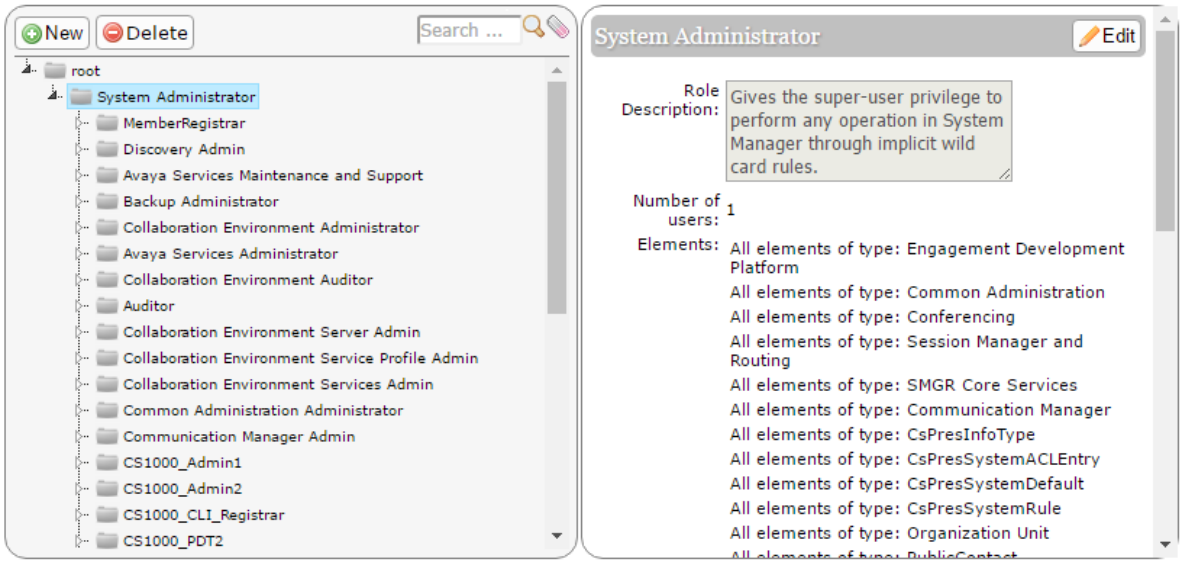
New Endpoint / Template field descriptions on page 743

Assigning permissions for CM templates

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the 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. 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 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 Avaya Aura® Messaging, Modular Messaging, or Communication Manager Messaging 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 1158
Subscriber CMM Templates field descriptions on page 1156
Subscriber Messaging Templates field descriptions on page 1153

Editing subscriber templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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 1158
Subscriber CMM Templates field descriptions on page 1156
Subscriber Messaging Templates field descriptions on page 1153

Viewing subscriber templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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 1158
Subscriber CMM Templates field descriptions on page 1156
Subscriber Messaging Templates field descriptions on page 1153

Deleting subscriber templates

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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 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 1158
Subscriber CMM Templates field descriptions on page 1156
Subscriber Messaging Templates field descriptions on page 1153

Viewing associated subscribers

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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.

Table continues…

Name	Description
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.
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

Name	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.

Name	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 • 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.

Table continues…

Name	Description
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 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.

Table continues…

Name	Description
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 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…

Name	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.
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

Table continues…

Name	Description
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.
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.

Table continues…

Name	Description
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 returns to the subsequent page.
Cancel	Cancels your current action and returns to the previous page.

Subscriber Messaging Templates field descriptions

Name	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

Name	Description
Last Name	The last name of the subscriber.
First Name	The first name of the subscriber.

Table continues…

Name	Description
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

Name	Description
Telephone Number	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.
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

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 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**.

Table continues…

Name	Description
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.
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

Name	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

Name	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.

Table continues…

Name	Description
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 returns to the previous page.
Cancel	Returns to the previous page.
Schedule	Performs the action at the chosen time.

Subscriber CMM Templates field descriptions

Name	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

Name	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

Table continues…

Name	Description
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.
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

Name	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

Name	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

Name	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

Name	Description
Misc 1	Additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the Messaging system.

Table continues…

Name	Description
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 returns to the previous page.
Cancel	Returns to the previous page.

Subscriber MM Templates field descriptions

Name	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

Name	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.

Table continues…

Name	Description
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

Name	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

Name	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**.

Table continues…

Name	Description
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 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

Name	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

Name	Description
Misc 1	Gives additional, useful information about a subscriber template. Entries in this field are for 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 returns to the previous page.
Cancel	Returns 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 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 1164

Viewing an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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 1164

Editing an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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 1164

Duplicating an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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 1164

Deleting an IP Office endpoint template

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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 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 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 the IP 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 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 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 the IP 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 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. 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 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 an 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 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.

Note:

System Manager filters uploaded files based on mime type or bytes in the file. If a file type does not match, System Manager shows up an error message.

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 a .WAV audio file to a .C11 audio file

Procedure

1. On the System Manager web console, click **Services** > **Templates**.
2. In the 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 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.
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.

Table continues…

Button	Description
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 Application Server system configuration templates

Adding an Application Server Configuration template

Procedure

1. In System Manager, click **Services** > **Templates**.
2. In the navigation pane, click **UCM and Application Server Configuration**.
3. In the **Templates List** section, click **New**.
4. Complete the **Name**, **System Type**, and **Version** fields.
5. Click **Details**. The system starts IP Office Manager.
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 IP Office Manager.

Related links

IP Office Application Server Templates field descriptions on page 1173

Viewing an Application Server Configuration template

Procedure

1. In System Manager, click **Services** > **Templates**.
2. In the navigation pane, click **UCM and Application Server Configuration**.
3. On the templates page, in the **Supported System Types** section select **IP Office Application Server**.
4. Click **Show List**.
5. Select the system configuration template you want to view.
6. Click **View**. The system starts IP Office Manager.

7. In IP Office Manager, you can view the system configuration template details. All the fields are read-only.
8. Click **File** > **Exit** to exit IP Office Manager.
9. Select the device to apply the template.

Related links

IP Office Application Server Templates field descriptions on page 1173

Editing an Application Server Configuration template

Procedure

1. In System Manager, click **Services** > **Templates**.
2. In the navigation pane, click **UCM and Application Server Configuration**.
3. On the templates page, in the **Supported System Types** section select **IP Office Application Server**.
4. Click **Show List**.
5. Select the system configuration template you want to edit.
6. Click **Edit**. The system launches the IP Office Manager application.
7. In IP Office Manager, 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.

Related links

IP Office Application Server Templates field descriptions on page 1173

Deleting an Application Server Configuration template

Procedure

1. In System Manager, click **Services** > **Templates**.
2. In the navigation pane, click **UCM and Application Server Configuration**.
3. On the templates page, in the **Supported System Types** section select **IP Office Application Server**.
4. Click **Show List**.
5. Select the template you want to delete.
6. Click **Delete**.
7. Do one of the following:
   - Click **Delete** to confirm the action.
   - Click **Cancel** to cancel the action.

Related links

IP Office Application Server Templates field descriptions on page 1173

Applying an Application Server Configuration template

About this task

Important:

When you apply a template on a device, the data of the template that you apply may override the existing system configuration data on the device.

Procedure

1. In System Manager, click **Services** > **Templates**.
2. In the navigation pane, click **UCM and Application Server Configuration**.
3. On the templates page, in the **Supported System Types** section select **IP Office Application Server**.
4. Click **Show List**.
5. Select the system template you want to apply to a device.
6. Click **Apply**.
7. Select the server to which you want to apply the template.
8. Do one of the following:
   - Click **Now** to perform the action immediately.
   - Click **Schedule** to perform the action at a specified time.
   - Click **Cancel** to cancel the action.

Related links

IP Office Application Server Templates field descriptions on page 1173

IP Office Application Server Templates field descriptions

Name	Description
Name	The name of the system configuration template of IP Office Application Server.
System Type	The type of system associated with the template. The options are: • **Unified Communications Module** • **Application Server**
Version	The version number of the template.
Last Modified Time	The date and time when the IP Office 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 1177

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 a **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 1177

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 1177

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 1177

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 1177

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 1177

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 1180

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 1180

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 1180

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 1180

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 1180

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 1180

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 20: Security

Extended Security Hardening

System Manager supports Standard, Commercial, and Military Grade security hardening. By default, System Manager comes with a Standard Grade hardening configuration. No additional action is required to set up this configuration.

Each security hardening grade applies specific security attributes as summarized in the following table:

Security attribute	Standard grade	Commercial grade	Military grade
VM Configuration Hardening[1]	Y	Y	Y
Password Management	Y	Y	Y (more restrictive)
Login and Session Management	Y	Y	Y
System and Application Files Hardening	Y	Y	Y
Certificate Management	Y	Y	Y
Support TLS 1.3	Y	Y	Y
FIPS 140-2 Compliance	—	Y	Y
Multifactor Authentication (PIV and CAC support)	Y	Y	Y
SELinux Enabled	—	—	Enforced
Audit Management	Y	Y	Y (+ OS level audit)
AIDE (File Tampering Prevention)	—	—	Y
Fapolicy (File access policy	—	—	Y

Note:

[1]: VMware ESXi VMX configuration file hardening applied as part of the Solution Deployment Manager deployment.

Enabling Commercial Grade Hardening

About this task

After you enable Commercial Grade hardening, you cannot disable it. To disable Commercial Grade hardening, you must redeploy System Manager.

Before you begin

- To reach the System Manager command-line interface, use one of the following methods:
  - Open vSphere Client (HTML5) and click the **Console** tab or the icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.
- Create the System Manager virtual machine snapshot.

  Note:

  Delete the snapshot after the System Manager operation is complete.

Procedure

1. Log in to the System Manager command-line interface.
2. Type **`setSecurityProfile --enable-commercial-grade`**, and press `Enter`.
3. At the prompt, type the user password and press `Enter`.
4. At the prompt, type one of the following and press `Enter`:
   - `1` to continue.
   - `2` to exit.

   You cannot access System Manager when the profile is enabled.

   System Manager checks for the System Manager CA certificate, takes a few minutes to complete the settings, and reboots to apply the changes.
5. To verify the enabled security profile, type **`getSecurityprofile`**, and press `Enter`.

   If the security profile is successfully enabled, System Manager displays the status.

   For example:

```
Profile Mode : commercial grade hardened mode enabled

SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

```
FIPS State : FIPS enabled.
```

Enabling Military Grade hardening

About this task

After you enable Military Grade hardening, you cannot disable it. To disable Military Grade hardening, you must redeploy System Manager.

Before you begin

- To reach the System Manager command-line interface, use one of the following methods:
  - Open vSphere Client (HTML5) and click the **Console** tab or the icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.
- Create the System Manager virtual machine snapshot.

  Note:

  Delete the snapshot after the System Manager operation is complete.

Procedure

1. Log in to the System Manager command line interface.
2. Type `setSecurityProfile --enable-military-grade`, and press `Enter`.
3. At the prompt, type the user password and press `Enter`.
4. At the prompt, type one of the following and press `Enter`:
   - `1` to continue.
   - `2` to exit.
5. At the `Enable SELinux?` prompt, type one of the following and press `Enter`:
   - `1` to enable.
   - `2` to disable.
6. At the `Enable Audit?` prompt, type one of the following and press `Enter`:
   - `1` to enable.
   - `2` to disable.
7. At the `Enable AIDE Tool?` prompt, type one of the following and press `Enter`:
   - `1` to enable.
   - `2` to disable.
8. At the `Enable Fapolicy?` prompt, type one of the following and press `Enter`:
   - `1` to enable.

- `2` to disable.

You cannot access System Manager when the profile is enabled.

System Manager takes a few minutes to complete the setting, and reboots for the changes to take effect.

Note:

- After a Security Hardening grade is enabled, you cannot enable a lower-level Security Hardening grade.
- In Release 10.1, if System Manager was not rebooted since installation, then during the Military Grade hardening process, System Manager reboots twice for the changes to take effect.

9. To verify the enabled security profile, type **`getSecurityprofile`**, and press `Enter`.

   If the security profile is successfully enabled, System Manager displays the status.

   For example:

```
Profile Mode : military grade hardened mode enabled

SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28

FIPS State : FIPS enabled.

Audit logging Enabled..

AIDE Tool Enabled..

Fapolicy:
      status:                   enabled
      state:                    active
      mode from config file:    enforcing
```

Optional settings for security hardening

To fulfil the security or environmental requirements, following are the optional settings for security hardening.

No.	Settings	Reference
1.	Enable Out of Band Management	Configuring Out of Band Management on System Manager on page 1500
2.	Modify password settings	Editing password policies on page 51
3.	Configure remote logging	Configuring remote syslog server from CLI on page 1043
4.	Configure LDAP for authentication	Provisioning the LDAP server on page 1273
5.	Configure EASG	Remote access of System Manager on page 1546
6.	Change login banner	Editing the login warning banner on page 64

Security hardening options

System Manager provides the following security hardening options:

- selinux
- audit
- fips
- aide
- TLSv1, TLSv1.1, TLSv1.2, and TLSv1.3
- fapolicy

  By default, fapolicy is disabled.

You can enable or disable one or more security hardening options. While you can enable all the options, you can only disable selinux, audit, aide, and fapolicy.

Note:

If the FIPS option is selected or already enabled, you cannot select the TLSv1 and TLSv1.1 options.

Enabling security hardening options

About this task

Use this procedure to enable one or more security hardening options from the following:

- selinux
- audit
- fips
- aide
- TLSv1, TLSv1.1, TLSv1.2, and TLSv1.3

- fapolicy

  By default, fapolicy is disabled.

Procedure

1. Log in to the System Manager command-line interface.
2. Do one of the following:
   - To enable only one security hardening option, type `securityHardeningOptions <security_hardening_option_name> enable`, and press `Enter`.

     For example, type the following command, and press `Enter`.

     ```
     securityHardeningOptions selinux enable
     ```

   - To enable more than one security hardening options, type `securityHardeningOptions <Comma separated_security_hardening_option_name> enable`, and press `Enter`.

     For example, type the following command, and press `Enter`.

     ```
     securityHardeningOptions selinux,audit,fips,aide,TLSv1.2,fapolicy enable
     ```

   System Manager takes a few minutes to complete the setting and reboots for the changes to take effect.

   Note:

   In Release 10.1, if System Manager was not rebooted since installation, then during the Military Grade hardening process, System Manager reboots twice for the changes to take effect.

   You can check the log file `/var/log/Avaya/mgmt/dodenv/securityHardeningOptions.log` to get the execution status.

Disabling security hardening options

About this task

Use this procedure to disable one or more security hardening options from the following:

- selinux
- audit
- aide
- fapolicy

Procedure

1. Log in to the System Manager command-line interface.

2. Do one of the following:
   - To disable only one security hardening option, type `securityHardeningOptions <security_hardening_option_name> disable`, and press `Enter`.

     For example, type the following command, and press `Enter`.

     ```
     securityHardeningOptions selinux disable
     ```

   - To disable more than one security hardening options, type `securityHardeningOptions <Comma separated_security_hardening_option_name> disable`, and press `Enter`.

     For example, type the following command, and press `Enter`.

     ```
     securityHardeningOptions selinux,audit,aide,fapolicy disable
     ```

   System Manager takes a few minutes to complete the setting and reboots for the changes to take effect.

Viewing the status of the security hardening options

Procedure

1. Log in to the System Manager command-line interface.
2. Type **`securityHardeningOptions --showstate`**.

   Based on the configuration, System Manager displays the status.

   For example:

```
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

FIPS State : enabled.

Audit: disabled

AIDE: disabled

Minimum TLS version = TLSv1.2

Fapolicy:
      status:                   enabled
      state:                    active
      mode from config file:    enforcing


SMGR Hardening mode: military
```

Configuring the TLS cipher suite list

About this task

From System Manager Release 8.0, the TLS cipher suite lists for establishing a secure communication are:

- Strict cipher suite list
- Relax cipher suite list

When you deploy the System Manager Release 8.0 OVA or upgrade System Manager to Release 8.0, by default, the system enables the Relax cipher suite list.

Use the following procedure to configure the required cipher suite list for the system.

Procedure

1. Log in to the System Manager command line interface.
2. Do one of the following:
   - To configure strict cipher suite list, type the following command. This would disable CBC ciphers.

     ```
     changeCipherSuiteList LIST2
     ```

   - To configure relax cipher suite list, type the following command. This would enable CBC ciphers.

     ```
     changeCipherSuiteList LIST1
     ```

   The system restarts the Application server on execution of the cipher suite list command.

Changing the TLS version

Changing the TLS version of System Manager

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Configuration** > **Security Configuration**.
3. On the Security Configuration page, click **Global**.
4. In the **Minimum TLS Version** field, click the appropriate TLS version.

   The options are:

   - **TLSv1.0**
   - **TLSv1.1**
   - **TLSv1.2**

- **TLSv1.3**

If you select the minimum TLS version **TLSv1.0** or **TLSv1.1**, System Manager displays a TLS Warning Message pop-up with the following message:

```
You are setting Minimum TLS version to TLS 1.0 or 1.1. For
increased security, it is recommended that the Minimum TLS Version
be set to TLS 1.2 or higher if these protocol levels can be
supported in your configuration.
```

```
Are you sure you want to proceed with selected TLS value?
```

For more information, see “Security Configuration field descriptions”.

- Click **OK** to proceed.
- Click **Cancel** and select the appropriate TLS version.

5. Click **Commit** to save the changes.

Changing the TLS version of primary and secondary System Manager

About this task

Use the following procedure to change the TLS version of System Manager in the Geographic Redundancy setup.

Before you begin

Ensure that the system is in the maintenance window.

Procedure

1. Disable the Geographic Redundancy replication.

   For more information, see “Disabling the Geographic Redundancy replication”.

2. Activate the secondary System Manager server.

   For more information, see “Activating the secondary System Manager server”.

3. On the primary System Manager server, change **Minimum TLS Version**.

   For more information, see “Changing the TLS version of System Manager”.

   Wait until the Application server starts. Application server automatically restarts after 10 minutes.

4. On the secondary System Manager server, change **Minimum TLS Version**.

   For more information, see “Changing the TLS version of System Manager”.

   Wait until the Application server starts. Application server automatically restarts after 10 minutes.

5. Deactivate the secondary System Manager server.

   For more information, see “Deactivating the secondary System Manager server”.

6. Restore data on the primary System Manager server and note the following:

   For more information, see “Restoring the primary System Manager server”.

   a. Perform the **Restore Data** operation from the secondary System Manager server.
   b. Ensure to select **Primary System Manager**.

7. Enable the Geographic Redundancy replication.

   For more information, see “Enabling the Geographic Redundancy replication”.

Related links

Disabling the Geographic Redundancy replication on page 106
Activating the secondary System Manager server on page 108
Changing the TLS version of System Manager on page 1189
Deactivating the secondary System Manager server on page 109
Restoring the primary System Manager server on page 109
Enabling the Geographic Redundancy replication on page 105

outboundConnectionLogging command

The **`outboundConnectionLogging`** command captures the logs in the `/var/log/Avaya/connections` file for every new outgoing connections initiated from System Manager.

By default, the outbound connection logging is disabled.

If you need to monitor logs, you can enable the outbound connection logging. Note that this can generate large amount of logs in the log file and might slightly impact the performance of System Manager. Therefore, it is recommended to disable the outbound connection logging, once your job is complete.

Syntax

```
outboundConnectionLogging [enable] [disable]
```

enable	Enables the outbound connection logging.
disable	Disables the outbound connection logging.

Related links

Enabling outbound connection logging on page 1191
Disabling outbound connection logging on page 1192

Enabling outbound connection logging

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.

2. Type `outboundConnectionLogging enable`, and press `Enter`.
3. When the system prompts for privileged command execution verification [sudo], type the password.

   System Manager enables the outbound connection logging.

Related links

outboundConnectionLogging command on page 1191

Disabling outbound connection logging

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type `outboundConnectionLogging disable`, and press `Enter`.
3. When the system prompts for privileged command execution verification [sudo], type the password.

   System Manager disables the outbound connection logging.

Related links

outboundConnectionLogging command on page 1191

configureOutboundFirewall command

With Release 8.1.3, you can configure System Manager outbound firewall by using the **`configureOutboundFirewall`** command.

When you configure the outbound firewall rule, System Manager can connect only to those destination system that are added in the allowed whitelist. Therefore, when you add the very first outbound firewall rule, ensure that you add all the required destination IP Addresses in the allowed whitelist to which System Manager will connect to.

By using the **`configureOutboundFirewall`** command, you can add, list, view status, disable, remove, and overwrite the IP addresses and FQDN in the whitelist for establishing the outbound connection from System Manager. You can also enable, disable, and view the status of logs for any connection that are dropped. This command supports the IPv4, IPv6, FQDN, and Network with Classless Inter-Domain Routing (CIDR) notation addresses.

Note the following:

- In the Geographic Redundancy setup, if you need to configure the outbound firewall rules, then you need to add the peer IP addresses on the primary and secondary System Manager servers.
- By using, the **`configureOutboundFirewall`** command, you cannot configure the outbound firewall in the Software-only environment.

Syntax

```
configureOutboundFirewall [add {-s} {-f}] [list] [status] [remove {-e} {-f}] [disable]
[overwrite {-s} {-f}] [enable-logging] [disable-logging] [logging-status]
```

-h	Displays the help for the command.
add *-s*	Adds the destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in the whitelist. While processing the FQDN, System Manager resolves the FQDN to its IP Address, and adds that IP address in the whitelist. You can add multiple entries with comma-separated values.
add *-f*	Adds the destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in the whitelist through a file.
list	Displays the list of outbound firewall rules.
status	Displays the status of outbound firewall configuration.
remove *-e*	Removes the entry of the outbound firewall rules from the whitelist.
remove *-f*	Removes the file of the destination outbound firewall rules.
disable	Disables the outbound firewall rules.
overwrite *-s*	Overwrites the existing list of outbound firewall rules in the whitelist.
overwrite *-f INPUT_FILE*	Overwrites the existing file of outbound firewall rules.
enable-logging	Captures the logs for any dropped connections. By default, the outbound firewall rule logging is disabled. System Manager stores the logs in the `/var/log/outbound_firewall.log` file.
disable-logging	Disables the outbound firewall rule logging.
logging-status	Displays the outbound firewall rule logging status.

Related links

Configuring the outbound firewall rules on page 1194
Viewing the list of outbound firewall rules on page 1195
Viewing the outbound firewall rule status on page 1195
Removing outbound firewall rules on page 1196
Disabling the outbound firewall rule on page 1196
Overwriting the existing outbound firewall rules on page 1197
Managing the outbound firewall rule logging on page 1198

Configuring the outbound firewall rules

About this task

When you configure the outbound firewall rule, System Manager can connect only to those destination system that are added in the allowed whitelist. Therefore, when you add the very first outbound firewall rule, ensure that you add all the required destination IP Addresses in the allowed whitelist to which System Manager will connect to.

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Do one of the following:
   - To add the list of destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in the whitelist, type **`configureOutboundFirewall`** `add -s` *`<destination IPv4/IPv6/FQDN/CIDR IPs>`*, and press `Enter`.

     You can add multiple entries with comma-separated values.

     For example, to add the specific entries, type the following:

     `configureOutboundFirewall` `add -s` *`10.10.10.10,10.10.10.11,test.avaya.com,10.10.10.12/24,2a07:2a42:adc0:19::9:25`*
   - To add the list of destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in the whitelist through a file, type **`configureOutboundFirewall`** `add -f` *`<absolute path of the.txt file>`*, and press `Enter`.

     You can add each entry in a separate line in the `<nameofthefile>.txt` file.

     For example, the format of the file is:

     ```
     cat /home/location/filename.txt
      10.10.10.10
      10.10.10.11
      2a07:2a42:adc0:19::9:25
      test.avaya.com
      10.10.10.12/24
     ```

     For example, to add the entries through the file, type the following:

     `configureOutboundFirewall` `add -f` *`/home/location/filename.txt`*

   While processing the FQDN, System Manager resolves the FQDN to its IP Address, and then adds, removes, or overwrites that IP address in the whitelist.
3. If the system prompts, type `y` to continue.

   In the Geographic Redundancy setup, System Manager displays the following message:

   `Geographic Redundancy configuration detected. Separate configuration of Outbound Firewall is required on the Primary and Secondary servers.`

In the Geographic Redundancy setup, if you need to configure the outbound firewall rules, then you need to add the peer IP addresses on the primary and secondary System Manager servers.

System Manager adds the specified IP Addresses and FQDN in the whitelist.

Related links

configureOutboundFirewall command on page 1192

Viewing the list of outbound firewall rules

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type **`configureOutboundFirewall`** `list`, and press `Enter`.

   System Manager displays the outbound firewall rule status and the list of the outbound firewall rules that are configured.

   For example:

```
OutBound connection firewall rules enabled

Following IP Addresses / Networks allowed for OutBound connection
----------------------------------------
10.10.10.11
10.10.10.12/24

2a07:2a42:adc0:19::9:25
```

Related links

configureOutboundFirewall command on page 1192

Viewing the outbound firewall rule status

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type **`configureOutboundFirewall`** `status`, and press `Enter`.

   The outbound firewall rule status can be `enabled` or `disable`.

   System Manager displays the status of the outbound firewall rule.

   For example:

```
enabled
```

Related links

configureOutboundFirewall command on page 1192

Removing outbound firewall rules

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Do one of the following:
   - To remove the list of destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in whitelist, type **`configureOutboundFirewall`** `remove -e <destination IPv4/IPv6/FQDN/CIDR IPs>`, and press `Enter`.

     For example, to remove the specific entries, type the following:

     `configureOutboundFirewall` `remove -e 10.10.10.10`
   - To remove the list of destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in whitelist through a file, type **`configureOutboundFirewall`** `remove -f <absolute path of the.txt file>`, and press `Enter`.

     For example, to remove the entries through the file, type the following:

     `configureOutboundFirewall` `remove -f /home/location/filename.txt`

   While processing the FQDN, System Manager resolves the FQDN to its IP Address, and then adds, removes, or overwrites that IP address in the whitelist.

   System Manager removes the specified IP Addresses, FQDN, and CIDR notation IP addresses from the whitelist.

Related links

configureOutboundFirewall command on page 1192

Disabling the outbound firewall rule

About this task

If you disable the outbound firewall rule, System Manager removes all the rules from the whitelist. Later, if you need to enable the outbound firewall rule, then you need to again add all the details in the whitelist.

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type **`configureOutboundFirewall`** `disable`, and press `Enter`.
3. At the prompt, type `y` to continue.

   System Manager disables the outbound firewall rule.

Related links

configureOutboundFirewall command on page 1192

Overwriting the existing outbound firewall rules

About this task

If you overwrite the outbound firewall rule, System Manager removes all the existing rules from the whitelist and adds the new entries in the whitelist.

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Do one of the following:
   - To overwrite the list of destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in whitelist, type **`configureOutboundFirewall`** `overwrite -s` *`<destination IPv4/IPv6/FQDN/CIDR IPs>`*, and press `Enter`.

     For example, to overwrite the specific entries, type the following:

     `configureOutboundFirewall` `overwrite -s` *`10.10.10.14,10.10.10.15,example.avaya.com,10.10.10.16/24,2a07:2a42:adc0:19::9:25`*
   - To overwrite the list of destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in the whitelist through a file, type **`configureOutboundFirewall`** `overwrite -f` *`<absolute path of the.txt file>`*, and press `Enter`.

     You can enter each entry in a separate line in the `<nameofthefile>.txt` file.

     For example, the format of the file is:

     ```
     cat /home/location/filename.txt
      10.10.10.14
      10.10.10.15
      2a07:2a42:adc0:19::9:25
      example.avaya.com
      10.10.10.16/24
     ```

     For example, to overwrite the entries through the file, type the following:

     `configureOutboundFirewall` `overwrite -f` *`/home/location/filename.txt`*

   While processing the FQDN, System Manager resolves the FQDN to its IP Address, and then adds, removes, or overwrites that IP address in the whitelist.

   System Manager overwrites the existing IP Addresses and FQDN with the new details in the whitelist.

Related links

configureOutboundFirewall command on page 1192

Managing the outbound firewall rule logging

About this task

Use this procedure to enable, disable, or view the status of the outbound firewall rule logging for the dropped connections.

If you need to monitor logs, you can enable the outbound firewall rule logging. Note that this can generate large amount of logs in the log file and might slightly impact the performance of System Manager. Therefore, it is recommended to disable the outbound firewall rule logging, once your job is complete.

Before you begin

Log in to the System Manager command line interface with CLI user credentials that you created at the time of application deployment.

- To enable the outbound firewall rule logging, type **`configureOutboundFirewall`** `enable-logging`, and press `Enter`.

  System Manager enables the outbound firewall rule logging and captures the logs for the dropped connections in the `/var/log/outbound_firewall.log` file.

- To disable the outbound firewall rule logging, type **`configureOutboundFirewall`** `disable-logging`, and press `Enter`.

  By default the outbound firewall rule logging is disabled.

  System Manager disables the outbound firewall rule logging and does not captures the logs for the dropped connections.

- To view the outbound firewall rule logging status, type **`configureOutboundFirewall`** `logging-status`, and press `Enter`.

  System Manager displays the outbound firewall rule logging status.

Related links

configureOutboundFirewall command on page 1192

Managing certificates

Trust Management

System Manager uses Trust Management to provision and manage certificates of various applications, servers, and devices for 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 validates any file you upload during certificate management and accepts only certain file types, such as text and XML. System Manager filters uploaded files based on the file extension and mime types or bytes in the file.

System Manager uses a third-party open-source application, Enterprise Java Beans Certificate Authority (EJBCA), as a Certificate Authority for certificate management.

Related links

Certificate Authorities on page 1232

Certificate generation and certificate management capabilities in System Manager

System Manager can only manage certificates for System Manager (during Geographic Redundancy for secondary System Manager as well), AVP Utilities, Session Manager, Branch Session Managers, and Avaya Breeze® platform elements.

Note:

- You cannot manage certificates of all added or managed elements from System Manager.
- For the Avaya Aura® Device Services and Avaya Aura® Web Gateway elements, even if the **More Actions** > **Manage Trusted Certificates** and **More Actions** > **Manage Identity Certificates** options are enabled on the **Services** > **Inventory** > **Manage Elements** page, after selecting them, do not perform these certificate operations as this is not supported. For information about certificate management of these elements, see the product-specific documents.

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 a certificate authority that the client trusts issued the server identity certificate. If the validation succeeds, a secure connection is established.

The following table provides the major certificate generation and certificate management capabilities that System Manager offers:

#	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	Use the SCEP client to generate a New certificate.	• Request from a product integrated with System Manager for certificates during installation. For example, Session Manager. • Request for certificates during the installation or registration of devices or endpoints that host an SCEP client. For example, B5800.	✔	✔	Not applicable
2	System Manager uses the following to generate a new certificate: • Standard Certificate Signing Request (CSR) • Keystore	Generating certificates manually to install the certificates on remote instances of: • Various products or endpoints • Products generate the keys on product and require System Manager CA to sign the certificates.	✔	✔	Not applicable

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
3	Installing a new identity certificate a third-party CA issues.	Configuring the System Manager web console to use a certificate a well-known CA issues. For example, VeriSign, instead of a certificate issued by its own CA. This applies to products that use System Manager for administration. For example, Session Manager and CS 1000.	✔	✔	✔
4	Replacing an identity certificate the System Manager CA issues with a new certificate the System Manager CA issues.	Installing a new certificate with changed values. For example, new FQDN and new IP address.	✔	✔	Not applicable
5	Replacing an existing identity certificate a third-party CA issues with a new certificate the System Manager CA issues.	Reverting System Manager, Session Manager, and CS 1000 that use third-party identity certificates to use certificates issued by the System Manager CA.	✔	✔	✔
6	Renewal of an existing identity certificate.	Manual or automatic renewal of a certificate that is about to expire. This capability is also available for products such as Session Manager.	✔	✔	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
7	Exporting an identity certificate to a PEM certificate file.	Exporting any identity certificate to a standard PEM format file so the certificate can be manually imported to the trust stores of various products.	✔	✔	✔
8	Adding new certificates to the truststore of the product.	Installing a new certificate to the truststores of the product, such as Session Manager.	✔	✔	✔
9	Removing existing certificates from the truststore of the product.	Deleting a certificate, for example, the SIPCA root certificate, from the truststores of the product, such as Session Manager.	✔	✔	✔

The certificate 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 the trusted certificate or CA certificate.

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.

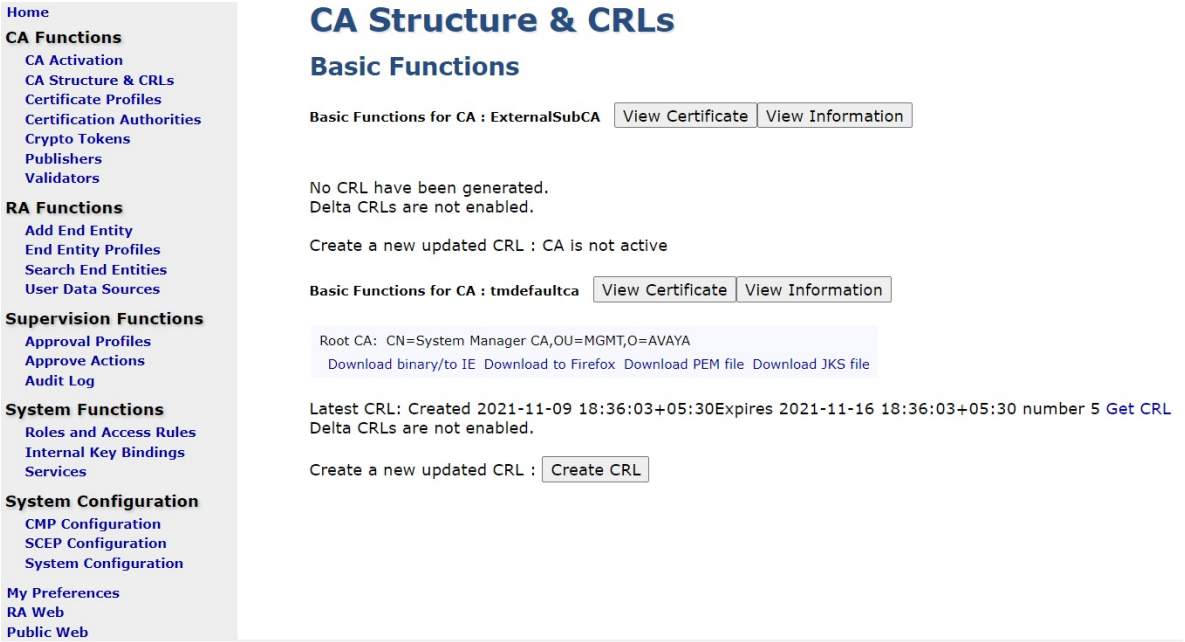
Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the 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.
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.

   You can use the **Services** > **Security** > **Certificates** > **Authority** link for launching EJBCA administration. A customer can configure the settings here, based on its PKI plan.



Related links

Enrollment Password field descriptions on page 1203

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.

Managing trusted certificates

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: Provides details, such as 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.

  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.

Manage 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.

Name	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	Displays the View Trust Certificate page. Use this page to view the certificate details.
Add	Displays the Add Trusted Certificate page. Use this page to import certificates from the selected resource.

Table continues…

Button	Description
Export	Exports the selected certificate from the list of trusted certificates to a PEM formatted file.
Remove	Removes the selected certificate from the list of trusted certificates.

Adding trusted certificates

About this task

Use the following procedure to import the certificates that you want to add as trusted certificate in the trust store of the element.

Note:

From Release 8.1, you can add trusted certificates for multiple elements. All the elements must be of same **Type** and **Version**. When you add trusted certificates for multiple elements, the system creates a scheduled job. To view the certificate management job status, select the element, and click **View Certificate Add Status** on the Manage Elements page.

If you select multiple elements, click **More Actions** > **Manage Trusted Certificates**, and the version of the elements is not up to date or empty then System Manager displays the following error message:

```
ElementType and Version of Selected Elements do not match.
```

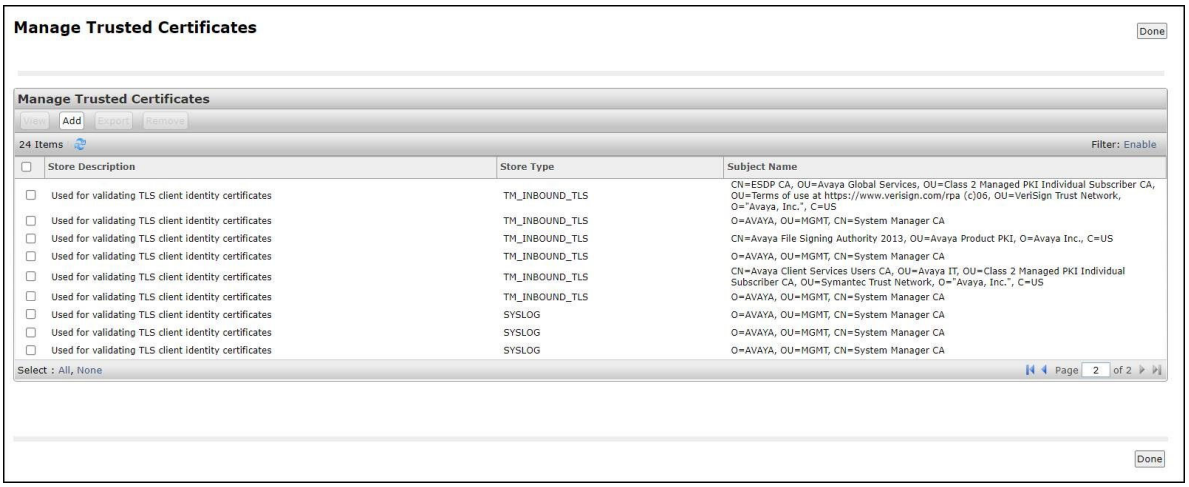
Before you begin

Perform the **Refresh Element(s)** operation under **Pre-upgrade Actions** on the **Services** > **Solution Deployment Manager** > **Upgrade Management** page and ensure that the version in the **Current Version** column is up to date for all the elements on which you plan to add trusted certificates at once.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select one or more elements, and click **More Actions** > **Manage Trusted Certificates**.

3. On the Manage Trusted Certificates page, click **Add**.



4. On the Add Trusted Certificates page, in **Select Store Type to add trusted certificate**, select a store type or select **All** if you are unsure of the store type.
5. To import certificates from a file, do the following:
   a. Click **Import from file**.
   b. Type the file name or click **Browse** to select a file.

      Note:

      System Manager validates the file type. If you provide an invalid file type, the system displays an error message.

   c. Click **Retrieve Certificate**.
6. To import certificates in the PEM format, do the following:
   a. Locate the PEM certificate.
   b. Open the certificate in the Notepad application.
   c. Select and copy the contents in the file.
   d. On the Add Trusted Certificates page, click **Import as PEM certificate**.
   e. Paste the contents from the PEM file in the text box provided on the Add Trusted Certificates page.
7. To import certificates from existing certificates, do the following:
   a. Click **Import from existing certificates**.
   b. In the Global Trusted Certificate section, select a certificate.
8. To import certificates by using TLS, do the following:
   a. Click **Import using TLS**.
   b. In **IP Address**, type the IP address of the computer.

c. In **Port**, type the port of the computer.

d. Click **Retrieve Certificate**.

9. Click **Commit**.

10. Restart the System Manager Application server.

Related links

Add Trusted Certificate field descriptions on page 1207

Add Trusted Certificate field descriptions

Name	Description
Select Store Type to add trusted certificate	The store type that is based on inbound and outbound connection.
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. When you select **Import as PEM certificate**, the system displays the text box to paste the PEM certificate content.
Import from existing certificates	The option to import a certificate from the existing imported certificates.
Import using TLS	The option to import a certificate if the element requires to contact the certificate provider to obtain the certificate.

When you select **Import from file**, the page displays the following fields.

Name	Description
Please select a file	The file that contains the certificates.

Button	Description
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.

Table continues…

Name	Description
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.

Global Trusted Certificate:

When you select **Import from existing certificates**, the page displays the following fields.

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

Name	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.

Button	Description
Retrieve Certificate	Retrieves the certificate and displays the details of the certificate in the Certificate Details section.

Related links

Adding trusted certificates on page 1205

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 navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **More Actions** > **Manage Trusted Certificates**.
4. On the Manage 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 1209

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.
Serial Number	The serial number of the certificate.
Basic Constraints	The extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.
Key Usage Extension	The extension defines the purpose of the key contained in the certificate such as Digital Signature, Key Cert Sign, CRL Sign.
Extended Key Usage	This extension indicates one or more purposes for which the certified public key may be used. in addition to or in place of the basic purposes indicated in the key usage extension.

Button	Description
Done	Closes the page and returns to the Trusted Certificates page.

Removing trusted certificates

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an application and click **More Actions** > **Manage Trusted Certificates**.

4. On the Manage 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.

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 returns to the Add Trusted Certificate page.

Managing identity certificates

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: Provides details, such as subject, issuer, key size, fingerprint, expiry date, and subject alternative name of the certificate that a service uses.
- Add: Adds an additional certificate for following services of Session Manager:
  - securitymodule_http (HTTP)
  - securitymodule_sip (SIP)
- 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: Exports 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.

Note:

The System Manager CA-issued identity certificates are valid for 730 days or from the time of certificate renewal/replacement until the System Manager CA expiry date, whichever is sooner. For an external CA-signed certificate, the validity depends on the configuration of the certificate authority signing the certificate.

Identity Certificates field descriptions

Name	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	Displays 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.

Adding additional certificate for a service

About this task

Use this procedure to add an additional certificate for following services of Session Manager:

- securitymodule_http (HTTP)
- securitymodule_sip (SIP)

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select an element, and click **More Actions** > **Manage Identity Certificates**.
3. On the Manage Identity Certificates page, select the service name to which you want to add another certificate.

4. Click **Add**.

   On the Add Identity Certificate page, select one of the following:

   - **Add new Internal CA Signed certificate**
   - **Add new external CA signed certificate**
   - **Generate Certificate Signing Request (CSR) for adding external CA signed certificate**

5. Click **Add new Internal CA Signed certificate**, and do the following:

   a. Select the **Common Name (CN)** check box and type the common name that is defined in the existing certificate.

   b. In **Key Algorithm**, select the key algorithm.

      System Manager uses the SHA2 algorithm for generating certificates.

   c. In **Key Size**, select the required key size.

   d. In **Subject Alternative Name**, select the relevant options, and enter the details.

   e. **(Optional)** In **OtherName**, type the other name for the certificate signing request.

   f. To add the internal CA signed certificate, click **Commit**.

6. Click **Add new external CA signed certificate**, and do the following:

   a. In **Please select a file (PKCS#12 format)**, choose the file from your local computer.

   b. In **Password**, type the password.

   c. Click **Retrieve Certificate**.

      The Certificate Details section displays the details of the certificate.

   d. Review the details of the uploaded certificate.

   e. To add a new, external CA-signed certificate, click **Commit**.

7. Click **Generate Certificate Signing Request (CSR) for adding external CA signed certificate**, and do the following:

   a. Select the **Common Name (CN)** check box and type the common name that is defined in the existing certificate.

   b. In **Key Algorithm**, select the key algorithm.

      System Manager uses the SHA2 algorithm for generating certificates.

   c. In **Key Size**, select the required key size.

   d. **(Optional)** In **Subject Alternative Name**, select the relevant options and enter the details.

   e. In **OtherName**, type the other name for the certificate signing request.

   f. Click **Generate CSR**.

   g. Ensure that the downloaded CSR is third-party signed.

   h. Import the signed certificate by using the **Import third party certificate** option.

8. For the newly generated certificates to take effect, restart the System Manager Application server.

Making a certificate as a default certificate for a service

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select an element, and click **More Actions** > **Manage Identity Certificates**.
3. On the Manage Identity Certificates page, select the service name.
4. Click the **Expand List** icon and select an additional certificate.
5. Click **Make default**.

   The system displays the following message: `Do you want to make this certificate as default certificate for Service Name: <ServiceName>?`
6. Click **OK**.

Removing an additional identity certificate

About this task

Use this procedure to remove the additional certificate for a service. You cannot remove the default certificate of a service.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select an element, and click **More Actions** > **Manage Identity Certificates**.
3. On the Manage Identity Certificates page, select the service name.
4. Click the **Expand List** icon and select the additional certificate.
5. Click **Remove**.

   The system displays the following message: `Do you want to delete this certificate of Service Name: <ServiceName>?`
6. Click **OK**.

Viewing identity certificates

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element, and click **More Actions** > **Manage Identity 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 1211

Replacing an identity certificate

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **More Actions** > **Manage Identity Certificates**.
4. On the Manage Identity Certificates page, select the certificate that you want to replace.
5. Click **Replace**.

   On the Replace Identity Certificate page, select one of the following:

   - **Replace this Certificate with Internal CA Signed Certificate**
   - **Import third party certificate**
   - **Generate Certificate Signing Request (CSR) for third party certificate**
6. Click **Replace this Certificate with Internal CA Signed Certificate**, and do the following:
   a. Select the **Common Name (CN)** check box and type the common name that is defined in the existing certificate.
   b. Select the key algorithm and key size from the respective fields.

      System Manager uses the SHA2 algorithm for generating certificates.
   c. **(Optional)** In **Subject Alternative Name**, select the relevant options and enter the details.
   d. **(Optional)** In **OtherName**, type the other name for the certificate signing request.
   e. To replace the identity certificate with the internal CA signed certificate, click **Commit**.
7. Click **Import third party certificate**, and do the following:
   a. In the **Please select a file** field, choose the file from your local computer.
   b. In the **Password** field, type the password.
   c. Click **Retrieve Certificate**.

      The Certificate Details section displays the details of the certificate.
   d. Review the details of the uploaded certificate.
   e. To replace the certificate with the third-party certificate that you imported, click **Commit**.

8. Click **Generate Certificate Signing Request (CSR) for third party certificate**, and do the following:
   a. Select the common name (CN) check box and type the common name that is defined in the existing certificate.
   b. Select the key algorithm and key size from the respective fields.

      System Manager uses the SHA2 algorithm for generating certificates.
   c. **(Optional)** In **Subject Alternative Name**, select the relevant options and enter the details.
   d. In **OtherName**, type the other name for the certificate signing request.
   e. Click **Generate CSR**.
   f. Ensure that the downloaded CSR is third-party signed.
   g. Import the signed certificate using the **Import third party certificate** option.
9. For the newly generated certificates to take effect, restart the System Manager Application server.

Related links

Adding trusted certificates on page 1205
Replace Identity Certificate field descriptions on page 1216

Renewing identity certificates

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **More Actions** > **Manage 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 the System Manager Application server.

   You must also restart the System Manager Application server, if certificates are auto renewed.

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 alternative name of the certificate holder.
Serial Number	The serial number of the certificate.
Basic Constraints	The extension that identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.
Key Usage Extension	The extension that defines the purpose of the key contained in the certificate. For example, Digital Signature, Content Commitment, Key Encipherment, Data Encipherment, and Key Agreement.
Extended Key Usage	The extension that indicates one or more purposes for which the certified public key can be used. These are in addition to or in place of the basic purposes indicated in the key usage extension.

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.
Generate Certificate Signing Request (CSR) for third party certificate	The option to generate a certificate signing request for a third-party certificate.

When you select **Replace this Certificate with Internal CA Signed Certificate** or **Generate Certificate Signing Request (CSR) for third party certificate**, the system displays the following fields.

Name	Description
Common Name (CN)	The common name of the certificate holder.
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.

Table continues…

Name	Description
Key Size	The key size in bits for encryption. The options are: • **1028** • **2048** • **4096** Use 2048 as the key size.
Subject Alternative Name	An alternative name of the certificate holder. The options are: • **DNS Name**: The DNS IP address. • **IP Address**: The IP address. • **URI**: The URI address. **Note:** In **DNS Name**, **IP Address**, and **URI** fields, you can enter more than one value separated by a comma. Do not add spaces between comma-separated IP addresses and DNS names.

Button	Description
Commit	Replaces the current identity certificate with the selected certificate.
Generate CSR	Generates a third-party certificate signing request. When you select the **Generate Certificate Signing Request (CSR) for third party certificate** option, the system enables the **Generate CSR** button.
Cancel	Cancels the certificate replacement operation.

When you select **Import third party certificate**, the system displays the following fields.

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 them 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 1214

Certificate renewal command overview

From System Manager Release 10.1.0.1 onwards, you can use the newly added command to renew the System Manager Identity (Server) certificates. The System Manager Certificate Authority (CA), the System Manager subordinate CA (SubCA), or a third-party CA (EJBCA) can sign the System Manager Identity certificates.

Run the certificate renewal command to issue new System Manager CA issued Identity certificates for all System Manager services. The new System Manager CA issued Identity certificates are valid for 730 days or from the time the command runs till the System Manager CA expiry date, whichever is lesser.

You must run the command with the -FORCE argument in any of the following scenarios:

- If the System Manager services are secured using the third-party CA issued Identity certificates.
- If there is a problem with the System Manager certificates causing the System Manager web console to be down.

If you run the certificate renewal command with -FORCE argument, the -FORCE argument replaces the third-party CA issued and System Manager issued certificates with the System Manager CA issued certificates.

Use the certificate renewal command only if certificate management is not possible through **Services** > **Inventory** > **Manage Elements** on the primary System Manager. The best practice is to perform all the certificate management operations from the System Manager web console.

In System Manager configured with Geographic Redundancy, if the primary and secondary System Manager certificates expire, you must first renew the certificates on the primary System Manager. Before you renew the certificates on the secondary System Manager, ensure that the primary System Manager web console is up and running and you can log in. If there are expired certificates on the secondary System Manager, you cannot issue the secondary System Manager certificates from the primary System Manager web console.

You can find the certificate renewal command logs at the following location: `/var/log/Avaya/folder`

Important:

If your System Manager Certificate Authority expires, the command does not work. If the System Manager Certificate Authority expires or is nearing expiry, see the procedure in PSN005555u on the Avaya Support site.

You can run the certificate renewal command with the -FORCE argument or without any arguments.

Using the certificate renewal command

Before you begin

- On Geographic Redundancy-enabled System Manager, disable the Geographic Redundancy replication. Always disable the Geographic Redundancy replication before you take a snapshot.
- Take a snapshot of the System Manager virtual machine on which to run the command.

- For secondary System Manager, set the enrollment password on primary System Manager.

About this task

Use the following procedure to run the certificate renewal command to renew the System Manager CA issued certificates for standalone, primary System Manager, or secondary System Manager.

Procedure

1. On the System Manager CLI, log in as the customer user created at OVA deployment.

   Note:

   For Avaya Services, log in with services root login, `sroot` to run the command.

2. Type `renewCertificates` to run the command and press Enter.

   The System Manager virtual machine displays the validity information for the System Manager Identity certificates. For example, container_tls and data_store.

   a. If there are any valid, unexpired third-party CA issued System Manager certificates, the command displays the certificate information. The command stops and prompts you to re-run the command with the -FORCE argument.

   b. If there are any expired third-party CA issued certificates or any expired or nearing expiry System Manager CA issued certificates, the command prompts you to continue with the certificate renewal process.

      - If you type `n`, the command stops without making any changes to the System Manager.
      - If you type `y`, the command prompts you to do the following:
        - If you have taken a snapshot, type `y`.

          The command continues to renew the certificates.
        - If you have not taken a snapshot, type `n`.

          Note:

          If you have not taken a snapshot, the best practice is to type `n` to stop the command, take a snapshot, and repeat from Step 2.

   c. If it is a secondary System Manager, type the Enrollment password when prompted.

      The command continues the certificate renewal process.

      The best practice is to not interfere with the command when it is in progress. The completion time for the certificate renewal process varies for each system.

Certificate Revocation

Viewing the certificates

About this task

Use this procedure to view the certificates for managed elements. The managed elements require the certificates to establish connection from System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Manage Certificate Revocation**.
3. On the Manage Certificate Revocation page, select the certificate that you want to view.
4. Click **View Certificate**.

   The system displays the View Certificate Detail page with details of the selected certificate.
5. Click **Done** to close the page.

View Certificate Detail field descriptions

Name	Description
Username	The name of the certificate holder.
Serial Number	The serial number that identifies the certificate.
Issuer DN	The distinguishing name of the certificate issuer.
Subject DN	The distinguishing name of the certificate holder.
Subject Alt Name	The alternate name of the certificate holder.
Revoked	The option to indicate whether a certificate is revoked.
Revocation Date	The date when the certificate was revoked. The field remains blank if the certificate is not in revoked state.
Revocation Reason	The reason for certificate revocation. The field remains blank if the certificate is not in revoked state.
Valid From	The date and time from when the certificate is valid.
Valid To	The date and time till the certificate is valid.

Button	Description
Done	Closes the View Certificate Detail page and displays the Manage Certificate Revocation page.

Manage Certificate Revocation field descriptions

Name	Description
Select radio button	The option to select a certificate.
Serial Number	The serial number that identifies the certificate.
Issuer DN	The distinguishing name of the certificate issuer.
Valid From	The date and time from when the certificate is valid.
Valid To	The date and time till the certificate is valid.
Subject DN	The distinguishing name of the certificate holder.
Revoked	The option to indicate whether a certificate is revoked.
Last Updated By	The name of the user who last updated or edited the certificate or both.
Revocation Date	The date when the certificate was revoked. The field remains blank if the certificate is not in revoked state.
Revocation Reason	The reason for certificate revocation. The field remains blank if the certificate is not in revoked state.

Button	Description
View Certificate	Displays all details of the selected certificate.
Revoke Certificate	Displays the option to revoke the selected certificate.
Unrevoke Certificate	Displays the option to unrevoke the selected certificate.
Refresh	Refreshes the certificate information in the table.
Filter: Enable	Displays the 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: Clear	Clears the filter criteria.
Filter: Apply	Filters certificates based on the filter criteria.
Select: None	Clears the selections.
Previous	Displays the certificates in the previous page. This button is unavailable when you are on the first page.
Next	Displays the certificates in the next page. This button is unavailable when you are on the last page.

Revoking and unrevoking certificates

About this task

Use this procedure to revoke a certificate for applications that System Manager manages. The applications require the certificates to establish connection from System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Security**.

2. In the navigation pane, click **Certificates** > **Manage Certificate Revocation**.
3. On the Manage Certificate Revocation page, select a certificate.
4. To revoke the certificate, do the following:
   a. Ensure that the certificate is in an unrevoked state and click **Revoke**.
   b. On the Revoke Certificate page, select the reason for certificate revocation.
   c. Click **Revoke**.
5. To unrevoke the certificate, do the following:
   a. Ensure that the certificate is in a revoked state with the reason **Certificate hold**.
   b. Click **Unrevoke**, and on the Revoke Certificate dialog box, click **Ok**.

Revoke Certificate field descriptions

Name	Description
Serial Number	The serial number that identifies the certificate.
Subject DN	The distinguishing name of the certificate holder.
Valid From	The date and time from when the certificate is valid.
Valid To	The date and time till the certificate is valid.
Revocation Reason	The reason to revoke the certificate.

Button	Description
Revoke	Saves the certificate revocation reason and revokes the certificate.
Cancel	Cancels the certificate revocation and displays the Manage Certificate Revocation page.

Manage Entity Classes

In Certificate Management, entity classes provide a way to manage certificate issue and renewal for a class (group) of entities with common characteristics, for example Endpoints.

From System Manager Release 8.1.3, you can add, edit, and delete the entity classes by using the **Services** > **Security** > **Certificates** > **Manage Entity Classes** page. Endpoints that have certificates issued by System Manager can use these entity classes to send certificate enrollment or renewal request to System Manager. The entity class password set is used to authenticate enrollment requests from endpoints to System Manager.

Adding an entity class

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Manage Entity Classes**.
2. Click **New**.

3. On the Add Entity Class page, do the following:
   a. In **Name**, type the name of the entity class.

      The name is mandatory for each entity class.
   b. In **Description**, type the description of the entity class.
   c. To enable the white list of subject names associated with an entity class, select the **Whitelist Validation of Subject** check box.
   d. In **Password**, type the password for the entity class.
   e. In **Confirm Password**, retype the password for the entity class.

      The password is mandatory for each entity class. Without the password, you cannot generate the certificate from System Manager because you require the password to authenticate the certificate generation request.
   f. In **Password Validity Duration**, select the duration for which the entity class password is valid.
   g. Click **Commit** to save the changes.

      System Manager displays the added entity class on the Manage Entity Classes page.

Editing an entity class

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Manage Entity Classes**.
2. Select an entity class, click **Edit**.
3. On the Update Entity Class page, edit the required parameters.
4. Click **Commit** to save the changes.

Deleting an entity class

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Manage Entity Classes**.
2. Select the entity classes, click **Delete**.

   System Manager displays the message to confirm the delete operation.
3. Click **Yes**.

   System Manager deletes the selected entity class.

Filtering entity classes

About this task

You can apply the filter to search the values of the following columns:

- **Name**
- **Description**

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Manage Entity Classes**.
2. Click the **Filter menu** icon, type the required value, and press `Enter`.

   The page displays the details that match the filter criteria.
3. To clear the filter values, click **Options** > **Clear Filter**.

   System Manager clears the filter criteria.

Manage Entity Classes field descriptions

Name	Description
Name	The name of the entity class.
Description	The description of the entity class.
Password Validity Duration	The password validity duration of the entity class and the duration since when the password is expired. Following is the example, if the password: • Is still valid: `5d 6h 40m`. • Has expired: `Expired 2h 40m ago`.
Whitelist Validation	The white list validation status of the **Subject** field in the certificate. The values are: • **Enabled** • **Disabled**

Button	Description
New	Displays the Add Entity Class page to add a new entity class.
Edit	Displays the Update Entity Class page to edit the entity class.
Delete	Deletes the selected entity class.
Options > **Clear Filter**	Clears the filter criteria.
Options > **Columns**	Customizes the display of columns.
Total Records	Displays the number of available records.

Icon	Description
Filter menu ( )	You can find the Filter menu icon next to the name of the column. You can apply the filter to search the values of the following columns: • **Name** • **Description**
Sorting ( )	You can find this icon next to the name of the column. You can sort the values of the following columns in the alphabetical order: • **Name** • **Description** • **Password Validity Duration**
Clear Filter ( )	Clears the filter criteria.
	Refreshes the entity classes list.

Related links

manageEntityClassWhitelist command on page 1226

Add Entity Class | Update Entity Class field descriptions

Name	Description
Name	The name of the entity class. The name must be 1 to 256 characters long and can include following characters: a-z, A-Z, 0-9, -, and _. The **Name** field does not take the space.
Description	The description of the entity class.
Whitelist Validation of Subject	The option to enable or disable the whitelist of subject names associated with an entity class. You can manage the Subject Names associated with the entity class by using the **`manageEntityClassWhitelist`** command. To enable the whitelist validation, add the Subject names by using the **`manageEntityClassWhitelist`** command, before any enrollment. For information about the **`manageEntityClassWhitelist`** command, see “manageEntityClassWhitelist command”.

Table continues…

Name	Description
Enable Password Details Update	This check box is available only on the Update Entity Class page. In case you also want to update the password and password validity duration of the entity class, you can enable the **Enable Password Details Update** check box. When you enable the check box, System Manager displays the **Password Validity Duration** and **Password** fields. **Note:** For making any changes to password details, you must update both **Password Validity Duration** and **Password** fields.
Password Validity Duration	The password validity duration of the entity class. The format of **Password Validity Duration** is Day:Hours:Minute. The maximum number of days for password validity are 28 days. This field is mandatory.
Password	The password for the entity class. Endpoints use this password in enrollment requests for authentication. You can define the password policy in the Password Policy for Programmatic Accounts section on the View and Edit Profile SMGR page.
Confirm Password	The password for the entity class.

Button	Description
Commit	Saves any changes made in the entity class configuration.
Cancel	Cancels any changes you made for add or update operation and displays the Manage Entity Classes page.

Related links

View and Edit Profile SMGR field descriptions on page 883
Viewing the subject name validation status for an entity class on page 1231
Adding subject names for an entity class on page 1228
manageEntityClassWhitelist command on page 1226

manageEntityClassWhitelist command

With Release 8.1.3, you can add, list, view, and delete the subject names for the provided entity-class by using the **`manageEntityClassWhitelist`** command. You can add and delete the bulk entries of subject names for an entity class. Also, you can check the status of the subject name validation for the entity class.

Syntax

```
manageEntityClassWhitelist [-h] [addAll -e <ENTITY_CLASS_NAME> -f <INPUT_FILE> -u
<USERNAME> -p <PASSWORD>] [add -e <ENTITY_CLASS_NAME> -s <SUBJECT_NAME> -u <USERNAME>
-p <PASSWORD>] [list -e <ENTITY_CLASS_NAME> -f <OUTPUT_FILE> -u <USERNAME> -p
<PASSWORD> -pn <PAGENUMBER> -ps <PAGESIZE>]  [view -e <ENTITY_CLASS_NAME> -s
<SUBJECT_NAME> -f <OUTPUT_FILE> -u <USERNAME> -p <PASSWORD>] [subjectCheck -e
<ENTITY_CLASS_NAME> -u <USERNAME> -p <PASSWORD>] [deleteAll -e <ENTITY_CLASS_NAME>
-u <USERNAME> -p <PASSWORD>] [delete -e <ENTITY_CLASS_NAME> -s <SUBJECT_NAME> -u
<USERNAME> -p <PASSWORD>]
```

-h	Displays help for the command and also displays the required and optional parameters.
addAll *-e* <ENTITY_CLASS_NAME> *-f* <INPUT_FILE> *-u* <USERNAME> *-p* <PASSWORD>	Adds or updates the Subject Names for the provided entity class through a file for bulk operation.
add *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-u* <USERNAME> *-p* <PASSWORD>	Adds the Subject Names for the provided entity class.
list *-e* <ENTITY_CLASS_NAME> *-f* <OUTPUT_FILE> *-u* <USERNAME> *-p* <PASSWORD> *-pn* <PAGENUMBER> *-ps* <PAGESIZE>	Lists the Subject Names for the provided entity class. You can provide a file name where System Manager can save the Subject Names.
view *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-f* <OUTPUT_FILE> *-u* <USERNAME> *-p* <PASSWORD>	Displays the Subject Name for the provided entity class. You can provide a file name where System Manager you can save all the Subject Names.
subjectCheck *-e* <ENTITY_CLASS_NAME> *-u* <USERNAME> *-p* <PASSWORD>	Displays the status of the subject name validation for the entity class. The status can be enabled or disabled.
deleteAll *-e* <ENTITY_CLASS_NAME> *-u* <USERNAME> *-p* <PASSWORD>	Deletes all the Subject Names for the provided entity class.
delete *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-u* <USERNAME>*-p* <PASSWORD>	Deletes the specific entry of the Subject Name for the provided entity class.

Parameter	Description
<ENTITY_CLASS_NAME>	The name of the existing entity class that you create on the System Manager web console.
<SUBJECT_NAME>	The subject name for the entity class.

Table continues…

Parameter	Description

<INPUT_FILE>	The file name with the list of subject names and the file is available on the System Manager server. The file extension is `.csv` file.
	Note:
	The input file can have a maximum of 5000 whitelist entries in it. If you have more than 5000 whitelist entries to be added to the entityClass, add them in batches of 5000.
	Following is an example of the format that is in the subject name file:
	`cat SubjectNameData.csv`
	`subjectName`
	`name1`
	`name2`
	`name3`
	`name4`
	`name5`

<OUTPUT_FILE>	The file name where System Manager copies and saves the details of subject names for the entity class.
<USERNAMRE>	The user name of the System Manager web console for managing the entity classes.

<PASSWORD>	The password of the System Manager web console for managing the entity classes.
	Note:
	If you do not type the `-u <USERNAME>` and `-p <PASSWORD>` parameters with the command, System Manager displays the following options after pressing `Enter`:
	`Enter User Name : -----`
	`Enter Password :-----`
	When the system prompts, provide the user name and password of the System Manager web console where the entity class is configured.

<PAGENUMBER>	Displays the list of subject name for the provided entity class on the specific page number.
<PAGESIZE>	Displays the total number of subject names for the provided entity class.

Related links

Viewing the subject name validation status for an entity class on page 1231
Adding subject names for an entity class on page 1228

Adding subject names for an entity class

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.

2. Do one of the following:
   - To add the subject name for the entity class in whitelist, type **manageEntityClassWhitelist** `add -e <ENTITY_CLASS_NAME> -s <SUBJECT_NAME> -u <USERNAME>`, and press `Enter`.

     Where:

     - <ENTITY_CLASS_NAME>: The name of the existing entity class that you create on the System Manager web console.
     - <SUBJECT_NAME>: The subject name for the entity class.
     - <USERNAMRE>: The user name of the System Manager web console for managing the entity classes.
     - <PASSWORD>: The password of the System Manager web console for managing the entity classes.

       If you do not type the `-u <USERNAME>` and `-p <PASSWORD>` parameters with the command, System Manager displays the following options after pressing `Enter`:

       ```
       Enter User Name : -----
       Enter Password :-----
       ```

       When the system prompts, provide the user name and password of the System Manager web console where the entity class is configured.

     For example, to add the specific entry, type the following:

     manageEntityClassWhitelist `add -e EntityClass1 -s Subject1 -u admin`

   - To add the subject name for the entity class in whitelist by using a file for bulk operation, type **manageEntityClassWhitelist** `addAll -e <ENTITY_CLASS_NAME> -f <INPUT_FILE> -u <USERNAME>`, and press `Enter`.

     For example, to add the entries through a file for bulk operation, type the following:

     manageEntityClassWhitelist `addAll -e EntityClass2 -f Subjectname.csv -u admin`

3. At the **Enter Password** prompt, type the password of the System Manager web console.

   System Manager adds the subject names for the entity class and displays the following message:

   ```
   Subject name(s) added successfully
   ```

Related links

Viewing the subject name validation status for an entity class on page 1231
manageEntityClassWhitelist command on page 1226

Displaying subject names for an entity class

About this task

Use this procedure to list the subject names for an entity class.

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Do one of the following:
   - To list the subject name for the entity class, type **manageEntityClassWhitelist** `list -e <ENTITY_CLASS_NAME> -u <USERNAME>`, and press `Enter`.

     For example, to list the subject names, type the following:

     manageEntityClassWhitelist `list -e EntityClass1 -u admin`
   - To save the subject names in a file, type **manageEntityClassWhitelist** `list -e <ENTITY_CLASS_NAME> -f <output_file> -u <USERNAME>`, and press `Enter`.

     For example, to save the subject names in a file, type the following:

     manageEntityClassWhitelist `list -e EntityClass1 -f SubjectNames.csv -u admin`
3. At the **Enter Password** prompt, type the password of the System Manager web console.

   System Manager displays the subject name for the entity class with the status, subjectName, and resource-uri details. It also displays the status of the subject name validation.

   For example:

```
Subject name check is enabled for Entity Class : EntityClass1
Operation successful, resultSize is <2> and pageSize is <100>. Output is shown
below.
[status, subjectName, resource-uri]
[NEW, Subject1, tm-service-api/entity-classes/EntityClass1/subject-names/Subject1]
[NEW, subjectnametest, tm-service-api/entity-classes/EntityClass1/subject-names/
subjectnametest]
```

   For saving the subject names in a file, System Manager displays the following message. For example:

```
Operation successful, Output copied to <SubjectNames.csv>. ResultSize is <1> and
pageSize is <100>
```

Viewing the subject name for an entity class

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. To view the details of the subject name for the entity class, type **manageEntityClassWhitelist** `view -e <ENTITY_CLASS_NAME> -s <SUBJECT_NAME> -u <USERNAME>`, and press `Enter`.

   For example, to view the specific entry detail, type the following:

   manageEntityClassWhitelist `view -e EntityClass1 -s Subject1 -u admin`

3. At the **Enter Password** prompt, type the password of the System Manager web console.

   System Manager displays the subject name for the entity class with the status, subjectName, and resource-uri details. It also displays the status of the subject name validation.

   For example:

```
Subject name check is enabled for Entity Class : EntityClass1
[status, subjectName, resource-uri]
[NEW, name1, tm-service-api/entity-classes/entity3/subject-names/name1]
```

Viewing the subject name validation status for an entity class

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. To view the status of the subject name validation for the entity class, type **manageEntityClassWhitelist** subjectCheck *-e* <ENTITY_CLASS_NAME> *-u* <USERNAME> *-p* <PASSWORD>, and press Enter.

   For example, type the following:

   manageEntityClassWhitelist subjectCheck *-e* EntityClass1 *-u* admin

3. At the **Enter Password** prompt, type the password of the System Manager web console.

   System Manager displays the subject name validation status. The status can be enabled or disabled.

   For example:

```
Subject name check is enabled for Entity Class : EntityClass1
```

Related links

Adding subject names for an entity class on page 1228
manageEntityClassWhitelist command on page 1226

Deleting the subject names for an entity class

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Do one of the following:
   - To delete the specific subject name entry for the entity class, type **manageEntityClassWhitelist** delete *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-u* <USERNAME>, and press Enter.

     For example, type the following:

     manageEntityClassWhitelist delete *-e* EntityClass1 *-s* Subject1 *-u* admin

- To delete all the subject name entries for the entity class, type **manageEntityClassWhitelist** `deleteAll -e <ENTITY_CLASS_NAME> -u <USERNAME>`, and press `Enter`.

  For example, type the following:

  manageEntityClassWhitelist `deleteAll -e EntityClass2 -u admin`

3. At the **Enter Password** prompt, type the password of the System Manager web console.

   System Manager deletes the subject names for the entity class and displays the following message.

   ```
   Subject name deleted successfully
   ```

Retrieving the System Manager CA certificate

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. To download the pem file for the tmdefaultca, on the **CA Functions** > **CA Structure & CRLs** page, click **Download PEM file**.
4. Click **Save** to save the certificate to a file.

Certificate Authorities

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.

Applying third-party certificates to Appliance Virtualization Platform

About this task

Use this procedure to create, download, upload, and push third-party certificates to Appliance Virtualization Platform hosts.

Before you begin

- Add a location.
- Add an Appliance Virtualization Platform host to the location.

- Ensure that the certificate on the Appliance Virtualization Platform host is valid.

Note:

If you are using a third-party generated CSR, add the private key for the CSR in the file `/etc/vmware/ssl/rui_csr_temp.key` before installing the certificate from Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. **(Optional)** Add the details of the generic CSR.

   If you add the generic CSR details, the system pre-populates the values in the View/Generate CSR dialog box.

   For more information about creating the generic CSR, see “Creating or editing generic CSR”.
5. To generate CSR, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
   b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
   c. Click **View/Generate CSR**.

      System Manager displays the View/Generate CSR dialog box.
   d. If the generic CSR details are not added for the Appliance Virtualization Platform host, add the details of the generic CSR.
   e. Click **Generate CSR**.

      The system generates CSR for the Appliance Virtualization Platform host.
   f. In the **Current Action** column, click **Status Details** to view the status.
6. To download CSR, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
   b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
   c. Click **Download CSR**.

      In case of Firefox browser, the system prompts you to save the `CSR.zip` file.
   d. In the **Current Action** column, click **Status Details** to view the status.

      In the Download CSR Status dialog box, the system displays the path of the downloaded `CSR.zip` file.

7. Extract the downloaded certificates, and ensure that the third-party signs them.
8. To upload and push the signed certificate from a third-party CA, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
   b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
   c. Click **Browse** and select the required certificates from the local computer.
   d. Click **I Agree to accept to add the same certificate in SDM**.
   e. Click **Push Certificate**.
   f. In the **Current Action** column, click **Status Details** to view the status.

Creating or editing generic CSR

About this task

Use this procedure to create or edit a generic CSR for third-party Appliance Virtualization Platform certificates. With a generic CSR, you can apply the same set of data for more than one Appliance Virtualization Platform host.

Procedure

1. In **Application Management Tree**, select a location.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
3. Click **More Actions** > **AVP Cert. Management** > **Generic CSR**.
4. In the Create/Edit CSR dialog box, add or edit the details of the generic CSR, such as organization, organization unit, locality, state, country, and email.
5. Click **Create/Edit CSR** and then click **OK**.

Next steps

Complete the CSR generation, download, third-party signing and push the certificates to the Appliance Virtualization Platform hosts.

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 navigation pane, click **Certificates** > **Authority**.
3. Click **RA Functions** > **Add End Entity**.
4. On the Add End Entity page, in **End Entity Profile**, select **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. Enter the relevant information in the fields.

   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.

The options are **P12 file**, **JKS file**, and **PEM file**.

7. Click **Add**.

   The system displays the message `End Entity <username> added successfully`.

Generating the certificate keystore

Before you begin

Create an end entity.

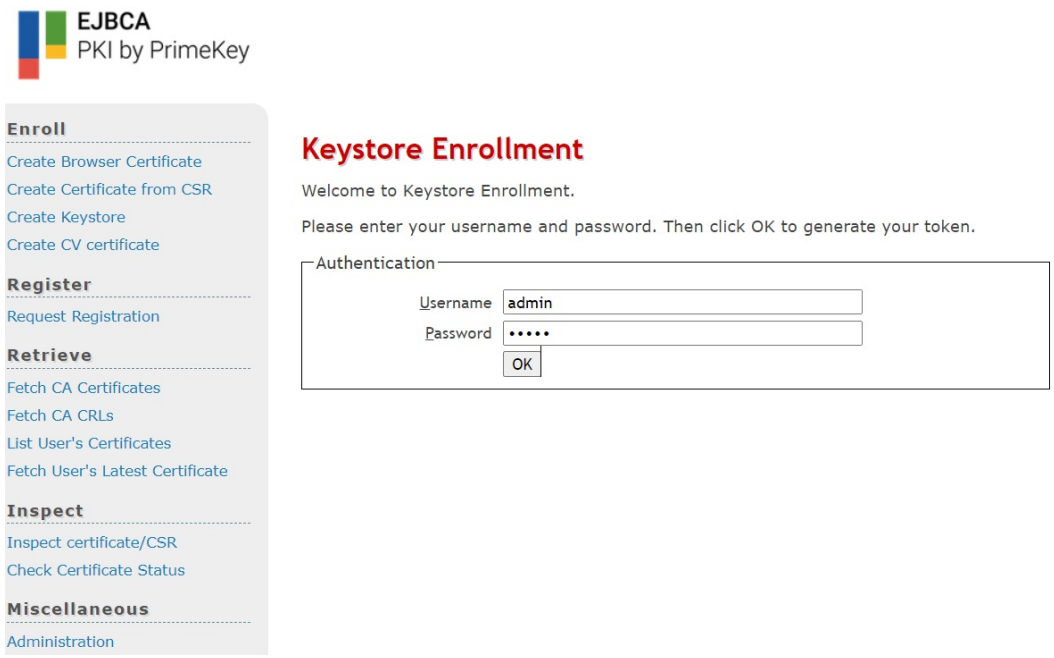
For more information, see Creating an end entity.

Procedure

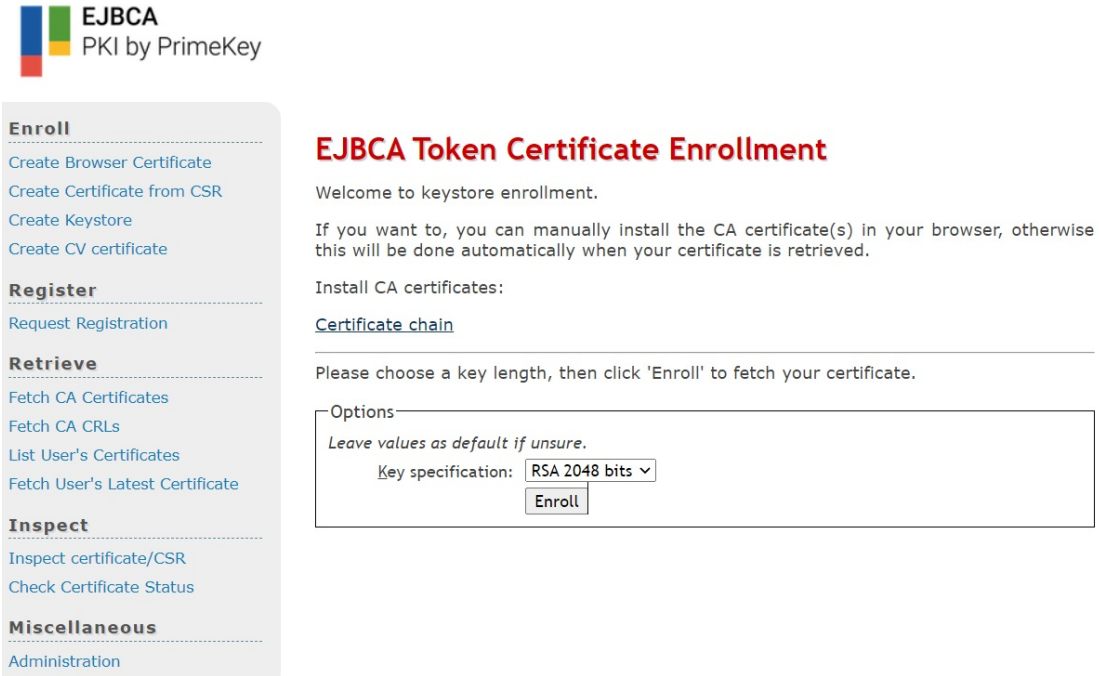
1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. In the navigation pane, click **Public Web**.
4. On the public EJBCA page, do one of the following:
   - If you are generating the certificate by using certificate 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.



- Click **OK**.
- On the next page, in the **Key specification** field, select a value, and click **Enroll**.



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 1235

Creating the certificate using a CSR

Before you begin

Create an end entity as described in Creating an end entity on page 1235.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. In the 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**.

      A certificate in PEM format is generated. The certificate contains the values provided in the end entity.

Related links

Creating an end entity on page 1235

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.

Overview of System Manager root certificate authority created using SHA256withRSA signing algorithm and 2048 key size

System Manager that is upgraded from releases earlier than Release 7.0, contains root Certificate Authority (CA) that has a key size of 1024 bits and uses the SHA1withRSA algorithm for signing own certificates.

You can use the createCA utility to improve the level of security of the System Manager CA by updating the key size to 2048 bits and the algorithm to SHA256withRSA.

Before running the utility, note the following:

- You must not use the createCA utility of one release on another release.
- If you upgrade System Manager after running the createCA utility, you do not need to run this utility again on the upgraded System Manager as the CA is carry forwarded as part of the upgrade process.
- You can use the utility in the following conditions:
  - When the System Manager root CA has been compromised.
  - Or, when you want to upgrade the signing algorithm and key size of the System Manager root CA.

    Tip:

    When you run the utility, the system displays a message along with the signing algorithm information that is used to create the existing root CA. If the signing algorithm is SHA256withRSA, then you do not need to run this utility.
- Starting from System Manager Release 7.0, the createCA utility can be run in a phased manner with the help of different options provided with the utility. The utility has the following options:
  - Option 1: Allows you to create a new root CA using SHA256withRSA signing algorithm and 2048 key size.
  - Option 2: Allows you to make the new root CA the default CA of System Manager.
  - Option 3: Allows you to run a single step process where the system creates a new root CA using SHA256withRSA signing algorithm and 2048 key size and makes that CA the default System Manager CA.

    Note:

    - You should select option 3 in the createCA utility for smaller deployments which have limited number of elements configured with the System Manager.
    - You should not select option 3 to create a new root CA in case you have run the utility by selecting option 1, and option 2.
  - Option 4: Allows you to exit the utility.
- Running the utility in a phased manner allows you to obtain the new root CA certificate after the first phase (option 1), and distribute the certificate to all the TLS connected elements before selecting option 2.

- To minimize service interruptions on a production network, it is recommended to run the utility by using option 1, distribute the certificate to all TLS connected elements, and then run the utility by using option 2.

Creating a new Certificate Authority by using SHA256withRSA signing algorithm and 2048 key size

Before you begin

Ensure that:

- You have read this section properly and have understood the implications of creating a new root Certificate Authority to issue certificates.

  For more information, see Overview of System Manager root certificate authority created using SHA256withRSA signing algorithm and 2048 key size on page 1239.

- System Manager Release 7.0 or later is installed.

  Note:

  - The createCA utility is available in System Manager starting from Release 6.3.8.
  - If you are on a release earlier than Release 7.0, you must upgrade the System Manager to the latest release before running the utility. The utility is not available for System Manager releases earlier than 6.3.8. For details about running the utility in System Manager versions earlier than 7.0, refer the corresponding *Administering Avaya Aura® System Manager* document.

- You have taken backup of the System Manager virtual machine before running the utility. If you are on Release 6.3.x of System Manager running on System Platform, ensure to take a backup from the System Manager UI and System Platform UI before running the utility.
- You have disabled the Geographic Redundancy replication for System Manager. You should re-configure Geographic Redundancy after executing option 1 followed by option 2 in the phased manner or after executing option 3 in the single step approach.

  For more information, see “Geographic Redundancy”.

Procedure

1. On the System Manager CLI, start an SSH session by logging in with customer login credentials.
2. Type `createCA`.
3. If the system prompts you to run the utility, type `y`.
4. Based on your requirement, type the appropriate option:
   - `1` to create a new root CA.
   - `2` to make the new root CA the default System Manager CA.
   - `3` to create a new root CA and then, make that new root CA the default System Manager CA in a single step.
   - `4` to exit from this utility.

Related links

Creating a new CA using option 1 of the createCA utility on page 1241
Making the new CA as default System Manager CA using option 2 of the createCA utility on page 1243
Creating a new CA using option 3 of the createCA utility on page 1244

Creating a new CA using option 1 of the createCA utility

About this task

Use this procedure to create a new CA with SHA256withRSA signing algorithm and keysize of 2048 bits.

Procedure

1. On the System Manager CLI, start an SSH session by logging in with customer login credentials.
2. Type `createCA`.
3. When the system prompts, type `y`.
4. Type `1` to create a new root CA.
5. When the system prompts, type `y`.
6. Type the Common Name (CN) of the new CA.

   Note:

   The default CN of the new CA is `SystemManager` CA.
7. Type `y` to confirm the provided Common Name.

   The system creates a new CA with the name `CreateCA`.

Next steps

Access the new CA by logging in to the System Manager web console.

For more information, see Downloading the new root CA on page 1241.

Downloading the new root CA

Procedure

1. Log in to the System Manager web console with the customer login credential which have administrative privileges.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **CA Structure & CRLS**.
4. For CreateCA, click **Download PEM file** to download the root CA to your desired location.

Next steps

Ensure that you place the new CA in the trusted stores of following elements, which:

- Communicate with System Manager using TLS.

- Get identity certificate issued by the System Manager CA.

Note:

For details about placing the CA in trusted stores of elements, see Prerequisites before making the new root CA as the default CA of System Manager on page 1242.

Prerequisites before making the new root CA as the default CA of System Manager

1. Place the new root CA in the trusted stores of elements which communicate with System Manager using TLS, and which get identity certificate issued by the System Manager CA.

   Elements, such as SIP endpoints, Communication Manager communicate with System Manager using TLS.

   Elements, such as, Session Manager, Session Border Controller get identity certificate issued by the System Manager CA.

   To add the new System Manager root CA certificate to Communication Manager trust store, see Distributing the new root CA with Communication Manager on page 1242.

   To add the new System Manager root CA certificate to the trust store of 96x1 series phones, see Distributing the new root CA with 96x1 series phones on page 1243.

   Note:

   Ensure that all other devices that connect using TLS to System Manager or any other server using the System Manager CA issued certificate also trust the new root CA. For detailed description on how to add a trusted certificate to those devices, refer the corresponding product documentation.

2. Disable the Geographic Redundancy replication for System Manager and convert the primary System Manager server to a standalone server.

   For more information, see Disabling the Geographic Redundancy replication for System Manager and converting the primary server to a standalone server on page 1243.

Distributing the new root CA with Communication Manager

About this task

Use this procedure to add the new System Manager root CA certificate to the trust store of Communication Manager.

Procedure

1. Log in to the Communication Manager SMI with administrative credentials.
2. Click **Miscellaneous** > **Download Files**.
3. Select the *.pem file, and click **Download**.
4. On the SMI, click **Security** > **Trusted Certificates**.
5. Click **Add**.
6. Type the file name that you uploaded and click **Open**.

7. On the next screen, type a file name with *.crt extension and select the Communication Manager repository check box.
8. Click **Add**.
9. Restart the Communication Manager system.

Distributing the new root CA with 96x1 series phones

About this task

Use this procedure to add the new System Manager root CA certificate to the trust store of 96x1 series phones.

Procedure

1. Search for the IP address or Fully Qualified Domain Name (FQDN) of the HTTP server from where the 96x1 series phones download the `settings` file.
2. Upload the new System Manager root CA certificate on the server.
3. Open the `settings` file on a text editor (for example, Notepad), and type the new root CA file name next to the SET TRUSTCERTS parameter.

   Note:

   Ensure that the name of the older root CA is also present next to the SET TRUSTCERTS parameter.
4. Save and close the `settings` file.
5. Restart the phones.

Disabling the Geographic Redundancy replication for System Manager and converting the primary server to a standalone server

Procedure

1. Disable the Geographic Redundancy replication for System Manager.

   For more information, see “Disabling the Geographic Redundancy replication”.
2. Convert the primary System Manager server to a standalone server.

   For more information, see “Converting the primary System Manager server to the standalone server”.

Making the new CA as default System Manager CA using option 2 of the createCA utility

About this task

Use this procedure to make the new CA as the default System Manager CA and issue new certificates for System Manager services by using the new CA.

Note:

After performing this task, the System Manager web console will be unavailable for approximately 15 minutes.

Procedure

1. On System Manager CLI, start an SSH session by logging in with customer login credentials.
2. Type `createCA`.
3. When the system prompts, type `y`.
4. Type `2` to make the new CA the default System Manager CA.
5. When the system prompts, type `y`.

   The CA that was created after typing option `1` is renamed as `tmdefaultca` and this CA becomes the default CA of System Manager.
6. **(Optional)** To download the tmdefaultca, log in to the System Manager web console, and click **Services** > **Security** > **Certificates** > **Authority** > **CA Structure & CRLS**.

Next steps

Manage all the tasks that must be performed after selecting options 1 and 2 in the createCA utility. For more details, see Managing tasks after running the createCA utility on page 1245.

Creating a new CA using option 3 of the createCA utility

About this task

This task sequentially performs all the actions that can be achieved by selecting options 1 and 2 in the createCA utility.

Note:

- You should select option 3 in the createCA utility for smaller deployments which have limited number of elements configured with the System Manager.
- You should not select option 3 to create a new root CA in case you have run the utility by selecting option 1, and option 2.

Procedure

1. On the System Manager CLI, start an SSH session by logging in with customer login credentials.
2. Type `createCA`.
3. When the system prompts, type `y`.
4. Type `3` to create a new root CA and make that CA as the default System Manager CA.
5. When the system prompts, type `y`.

   The new root CA that is created is renamed as `tmdefaultca` and this CA becomes the default CA of System Manager.
6. To download the tmdefaultca, log in to the System Manager web console, and click **Services** > **Security** > **Certificates** > **Authority** > **CA Functions** > **CA Structure & CRLS**.

7. Distribute the new root CA with other elements, for example, Communication Manager, 96x1 series phones, Session Manager, Session Border Controller and so on.
8. Disable the Geographic Redundancy replication for System Manager and convert the primary System Manager server to a standalone server.
9. Manage the tasks that must be performed after running the createCA utility.

Related links

Distributing the new root CA with Communication Manager on page 1242
Distributing the new root CA with 96x1 series phones on page 1243
Disabling the Geographic Redundancy replication for System Manager and converting the primary server to a standalone server on page 1243
Managing tasks after running the createCA utility on page 1245

Managing tasks after running the createCA utility

Before you begin

Ensure that you have run the createCA utility using one of the following procedures:

- Using option 1 followed by using option 2 in the phased approach.
- Using option 3 in the single step approach.

Procedure

1. Set the enrolment password which is reset after running the createCA utility.

   Note:

   For more information, see “Setting the enrollment password”.

2. To configure the System Manager Geographic Redundancy, perform the following:
   a. Convert the primary System Manager server to a standalone server.
   b. Reinstall the secondary System Manager.
   c. Re-configure Geographic Redundancy by logging in to the web console of the secondary System Manager.

   Note:

   For more information, see “Geographic Redundancy”.

3. Regenerate new certificates for elements that use System Manager issued certificates. For example, if your network consists of two core Session Manager systems, then perform the following steps:
   a. Log in to the System Manager web console.
   b. Change the service state for the primary Session Manager to **Deny New Service**. For more details, refer *Administering Avaya Aura® Session Manager*
   c. Log in to the primary Session Manager CLI and System Manager CLI.
   d. Type `initTM -f`.

e. To restart the Application server, type `smgr restart`.

   After you run the above command, the System Manager web console will be inaccessible for approximately 15 minutes.

f. For SIP Endpoints, regenerate the SIP and HTTP certificates using the "enhanced validation" certificates on Session Manager.

   For more information, see the “Installing Enhanced Validation Certificates for Session Manager” section in the *Administering Avaya Aura® Session Manager* document.

g. Change the service state for the primary Session Manager to **Accept New Service**.

   For more information, see *Administering Avaya Aura® Session Manager*

h. Repeat above steps for the secondary Session Manager.

4. To delete the old System Manager CA, perform the following:

   a. Log in to the System Manager web console with customer login credentials which have administrative privileges.

   b. Click **Services** > **Security** > **Certificates** > **Authority** > **Certification Authorities**.

   c. Select the older CA.

      The older CA may appear as `olddefaultcaXXX` after the new root CA is set as the default System Manager CA.

   d. Click **Delete CA**.

      Warning:

      It is an irreversible step. Ensure that you have placed the latest root CA on the trusted stores of all the elements before deleting the older CA.

5. To regenerate new certificates for Presence Services servers starting from Release 6.2.x, perform the following:

   a. Log in to the CLI of the Presence Services server.

   b. Type `prescert reconfigureAll sceppw <smgr_enrollment_passwd>`.

   c. Type `stop.sh`.

   d. Type `start.sh`.

6. Generate a new identity certificate for any other server, for example, Session Border Controller that are configured in the network and that use System Manager issued certificates.

   For more information, refer to the corresponding product documentation.

7. Delete the old CA certificate from System Manager trust stores.

   For more information, refer “Removing trusted certificates”.

8. Delete the old CA certificate from the trust store of endpoints, Communication Manager and any other element that trusted it.

External SSL configurations in System Manager

Using a third-party identity certificate for System Manager

From the System Manager web interface, you can install an identity certificate for System Manager issued by a certificate authority (CA). After the certificate installation, during SSL communications, System Manager presents the identity that is issued by the third-party identity certificate.

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 a third-party certificate.
2. Updating the truststores 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 *Avaya Aura® System Manager Certificate Management* on the Avaya Support site at http://support.avaya.com.

Set the System Manager CA as the subordinate CA

Note:

Before you begin, ensure you take a snapshot of the System Manager application. Once the subordinate CA (SubCA) has been successfully set up and you have verified all the functionalities, ensure you remove the snapshot of the System Manager application.

You can change the default Certificate Authority (CA) that the system generates during the System Manager installation to an externally signed 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.

Note:

System Manager as a certificate authority does not support Delta CRLs and the Avaya Aura® elements also do not validate Delta CRL. Therefore, do not create Delta CRL from System Manager.

The **Extended Key Usage** field should not be set in the SubCA certificate.

Related links

Generating the certificate signing request on page 1247
Guidelines for signing the certificate signing request on page 1248

Generating the certificate signing request

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.

3. Click **CA Functions** > **Certification Authorities**.
4. On the Manage Certification Authorities page, in **Add CA**, type the name `ExternalSubCA`, and click **Create**.
5. On the Create CA page, do the following:
   a. In **CA Type**, select **X.509 CA**.
   b. In **Signing Algorithm**, select **SHA256WithRSA**

      Note:

      Do not use anything else.
   c. In **Crypto Token**, retain the default value.
   d. In **Description**, provide a description.
   e. In **Enforce unique DN**, clear the check box.
   f. In **Subject DN**, type a DN for your SubCA.

      For example, CN=ExternalSubCA,O=AVAYA,C=US.

      Important:

      Entering incorrect values in **Subject DN** can lead to failures.
   g. In **Signed By**, click **External CA**.
6. In the **Externally signed CA creation/renewal** section, click **Choose File**, and open the CA certificate file that is on your computer.

   Note:

   You must have the CA certificate that is used to sign the CA. If the external signing CA is a SubCA, then you need to ensure that you use the full chain in its certificate hierarchy, all the way to the root CA. The certificate chain 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.

Guidelines for signing the certificate signing request

Following are the guidelines for the certificate signing request:

- Use the -preserveDN flag while executing the **`openssl ca`** command to 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.

- You must set basicConstraints=CA:TRUE for the signed certificate while signing the request.
- You must get the certificate request signed by using the SHA256WithRSA Signing Algorithm
- You must ensure the CA-signed certificate contains proper revocation related information in it. Ensure that the revocation checking URLs are correct and reachable from the elements interacting with System Manager CA.

Receiving certificate response

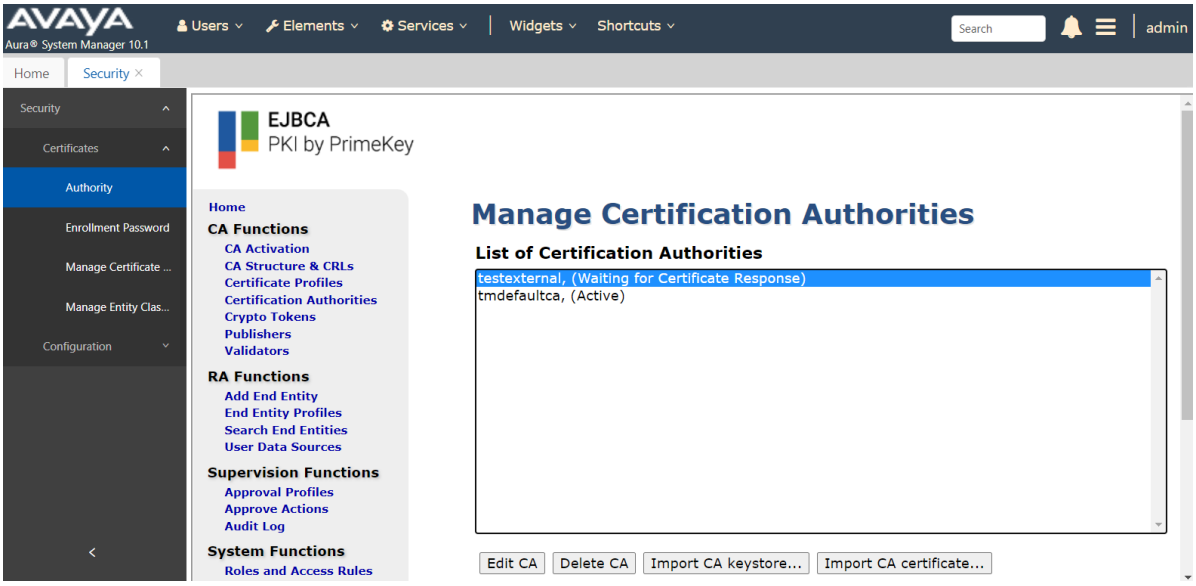
Before you begin

Ensure that the received SubCA certificate is properly signed by the authorised CA. To check, use the openssl command.

```
openssl verify -CAfile ca-cert.pem subca-cert.pem
```

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the 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 the 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.

   ```
   Certificate Response received successfully, CA Activated
   ```

   If you do not see this message, double-check the contents of the certificate file.

Configuring revocation information in the subordinate CA

About this task

It is not mandatory but Avaya recommends configuring revocation information in the SubCA.

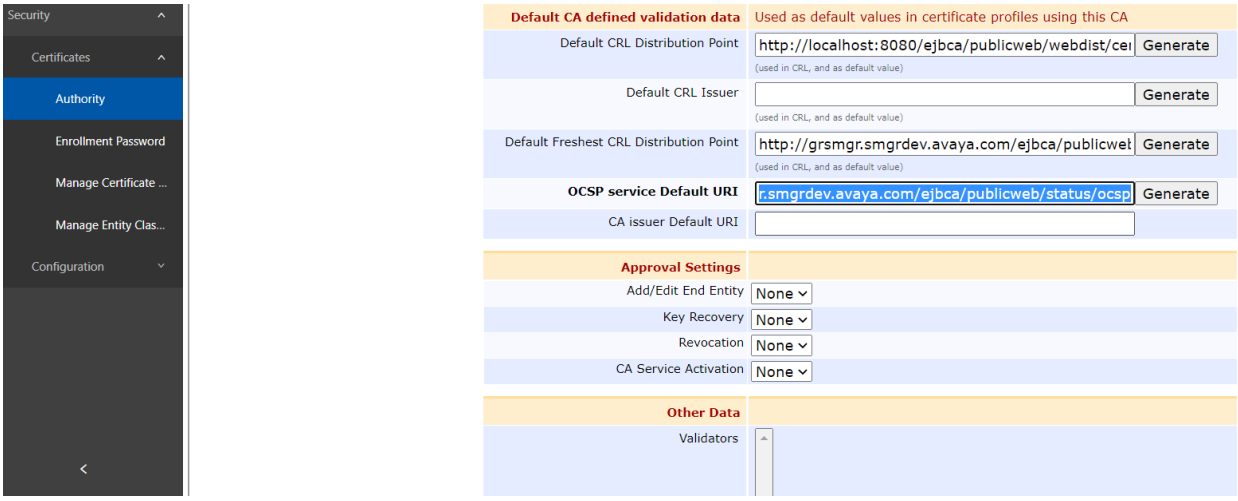
Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **Certification Authorities**.
4. Select ExternalSubCA that you created earlier, and click **Edit CA**.
5. On the Edit CA page, fill values only in these two fields, **OCSP service Default URI** and **Default CRL Distribution Point**.
6. In **OCSP service Default URI**, add the following value:

   `http://<SMGR_VFQDN>/ejbca/publicweb/status/ocsp`

   Note:

   Replace SMGR_VFQDN with the appropriate System Manager VFQDN.



7. To find the System Manager VFQDN, access the URL `https://{system-manager-fqdn}/ws/grservice/getgrstate/test` on the browser.

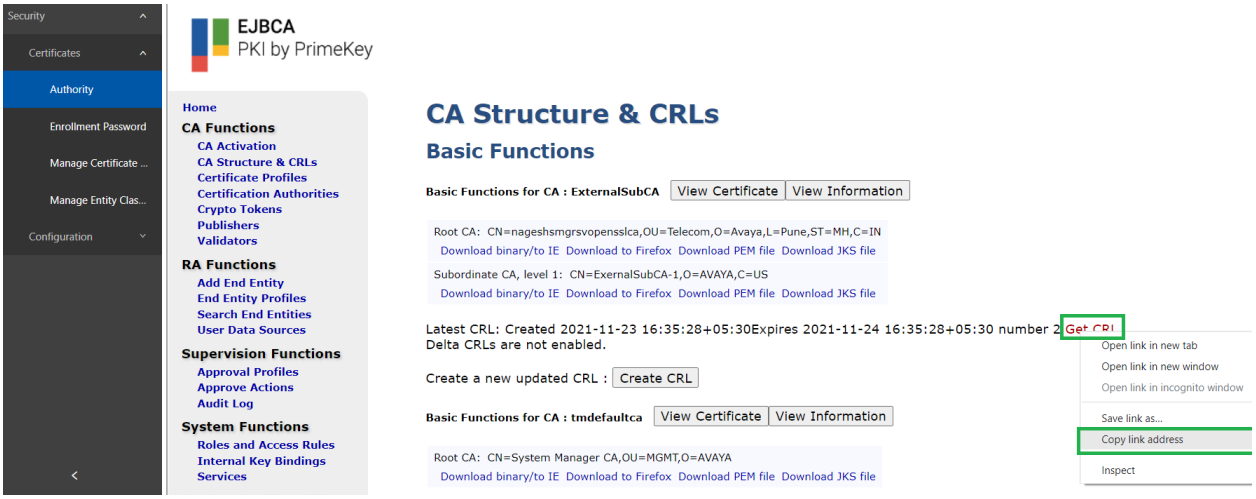
   It returns a value like the following:

   STANDALONE 148.147.163.12 ejbcaJay.smgrdev.avaya.com STANDALONE 127.0.0.1 *grsmgr.smgrdev.avaya.com* 10.1.5.101013907 2021-11-19T07:00:24.798Z

   Here *grsmgr.dsmgrsv.com* is the VFQDN, the value before the release number text.

8. Add a value in the **Default CRL Distribution Point**.

   For deriving the value, replace the last part of the text, http://<SMGR_VFQDN>/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=*url-encoded-issuerD*, do as follows:



a. Click **CA Functions** > **CA Structure & CRLs**.

b. In the **ExternalSubCA** that you created earlier. On **Get CRL**, right-click and select **Copy link address**.

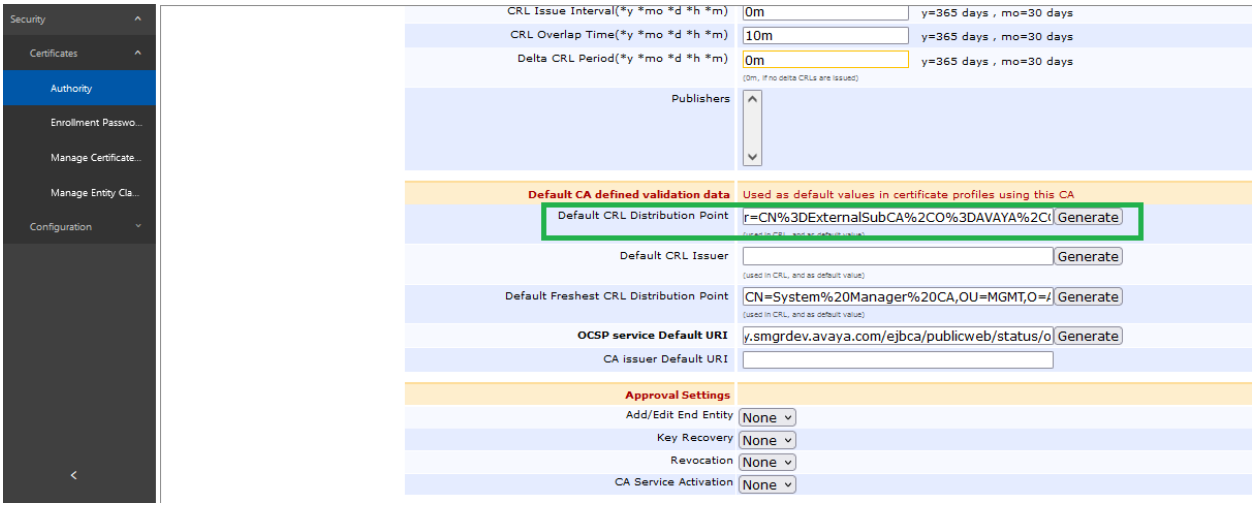
c. Paste the contents in a Notepad, https://<SMGR_IPaddress>/ejbca/adminweb/ca/getcrl/getcrl?cmd=crl&issuer=*CN%3DExternalSubCA%2CO%3DAVAYA%2CC%3DUS*

9. Copy everything after issuer= and paste it after issuer= in the earlier URL.

Note:

```
http://<grsmgr.dsmgrsv.com>/ejbca/publicweb/webdist/certdist?
cmd=crl&issuer=CN%3DExternalSubCA%2CO%3DAVAYA%2CC%3DUS
```

Place this URL in the box **Default CRL Distribution Point**.



10. Click **Save**.

Setting the new CA as the default CA

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **Certification Authorities**.
4. Select the new SubCA, ExternalSubCA, and ensure that the status is **Active**.
5. On the Manage Certification Authorities page, to rename the existing CA, tmdefaultca, do the following:
   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. To rename ExternalSubCA to tmdefaultca, do the following:
   a. From the list, highlight ExternalSubCA.
   b. In the text box at the bottom of the page, type `tmdefaultca`.
   c. 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 on page 852".

Modifying the default end entities to use the new CA

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the 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** > **End Entity Profiles**.

9. Select **INBOUND_OUTBOUND_TLS** and click **Edit End Entity Profile**.
10. On the Edit End Entity page, in **Default CA**, 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 the earlier step, do the following:
    a. Click **End**.
    b. On the Edit End Entity page, in the **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 the four entities.

Importing a third-party certificate in FIPS mode

About this task

You can replace the System Manager identity certificate with a third-party certificate in FIPS mode.

As a part of security hardening in FIPS mode, you cannot import a third-party certificate in the PKCS#12 format.

Procedure

1. On the System Manager web console, navigate to **Services** > **Inventory** > **Manage Elements**.

2. On the Manage Elements page, select the System Manager element from the list and click **More Actions** > **Manage Identity Certificates**.
3. On the Manage Identity Certificates page, select a certificate and click **Replace**.
4. On the Replace Identity Certificate page, click **Generate Certificate Signing Request (CSR) for third party certificate** and do the following:
   a. Select the **Common Name (CN)** check box and enter the name defined in the existing certificate.
   b. Select the key algorithm and key size from the respective fields.

      System Manager uses the SHA2 algorithm to generate certificates.
   c. **(Optional)** In the **Subject Alternative Name** section, select the options such as **DNS Name**, **IP Address**, **URI**, or **id-on-xmppAddr**.
   d. In the **OtherName** field, type the other name for the certificate signing request. The **OtherName** is the value on **id-on-xmppAddr** option.
   e. Click **Generate CSR**.

      Use the downloaded CSR to get an identity certificate in PEM format from the third-party authority.

   Note:

   - To enable the PEM option for importing the third-party certificate, you must generate the CSR.
   - If you generate multiple CSRs for a third-party certificate, use the latest CSR to obtain an identity certificate.
5. On the Replace Identity Certificate page, click **Import third party certificate**.
6. In the **Certificate File Format** field, select the **PEM** option.
7. Choose the file (PEM format) from your local computer, and click **Retrieve Certificate**.

   The Certificate Details section displays the details of the certificate.
8. Review the uploaded certificate details.
9. Click **Commit**.
10. To replace other identity certificates, repeat steps 1 to 9.
11. On the System Manager command line interface, run the `smgr restart` command.

    Note:

    You must restart System Manager for the newly replaced certificates to take effect.

Adding root CA and subordinate CAs to the trusted stores

About this task

After the new SubCA is created, add the root and all intermediate CA certificates in its chain to 'All' the trusted stores of System Manager.

Note:

Add the root and all intermediate CA certificates to all elements in the network that interact with System Manager CA-issued certificates.

Procedure

1. Log in to the System Manager web console with administrator privilege credentials.
2. Click **Services** > **Security** > **Certificates** > **Authority**.
3. Click **CA Functions** > **CA Structure & CRLs**.
4. For the CA = “tmdefaultca”, download the PEM file for the root CA and all subordinate CA(s) by clicking on the **Download PEM file** link associated with each CA.

   Refer to the document for the respective products on how to add the certificates to the store.

   For adding certificates into ‘All’ truststores of System Manager, see Adding trusted certificates on page 1205

Stopping CRL creation after deleting the subordinate CA

Before you begin

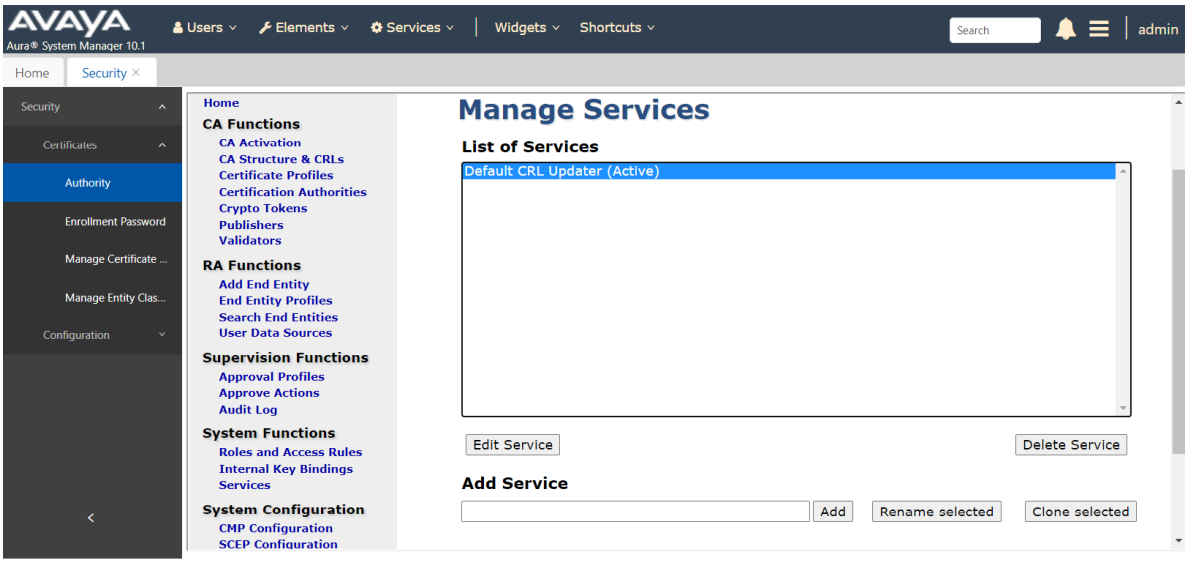
Delete the SubCA from **Services** > **Security** > **Certificates** > **Authority** > **Certification Authorities**. After you delete the SubCA, only the tmdefaultCA status is active. However, in **Supervision Functions** > **Audit Log**, the error log displays CRL creation failure for the deleted SubCA. This error persists even after you restart the Application server.

To stop the CRL creation that causes the error, use the following procedure.

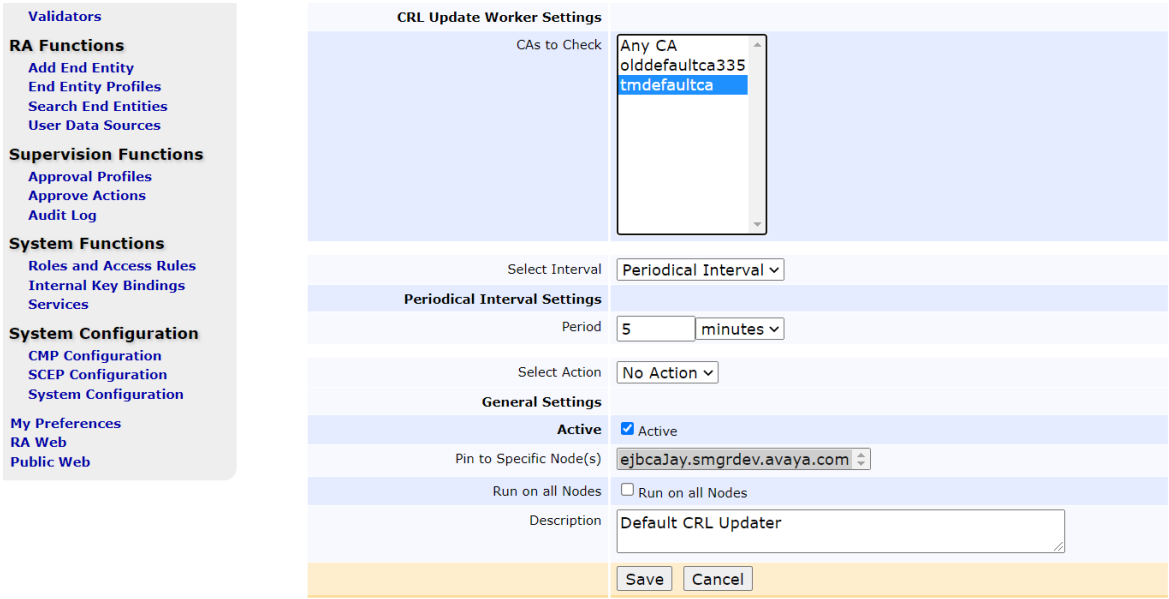
Procedure

1. From the System Manager web console, go to **Services** > **Security** > **Certificates** > **Authority**.
2. In **System Functions**, click **Services**.

3. In **List of Services**, select **Default CRL Updater (Active)** and click **Edit Service**.



4. In **CRL Update Worker Settings**, select **tmdefaultca** and click **Save**.



Generating new identity certificates for System Manager

About this task

After CA is set up to issue certificates by using the new Subordinate CA, 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 truststores.

Procedure

1. Replace all the Service Names listed under **Manage identity certificates** with new CA-signed certificates.

   See "Replacing an identity certificate". Verify the certificates as you replace them. Do not check the **Common Name(CN)** and **Subject Alternative Name(SAN)** check boxes, if they are proper.

   Note:

   While replacing Identity certificates, select the **Replace this Certificate with Internal CA Signed Certificate** option, select **Common Name(CN)**, and **Subject Alternative Name(SAN)** fields with default values. Select **Key Algorithm** as RSA and **Key Size** as 2048.

   Note:

   Replace the container_tls service certificate at the end. After replacing this certificate, you need to restart the Application server immediately.

2. To restart the Application server, type `smgr restart`.

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** > **Manage Identity Certificates**.
3. On the Identity Certificates page, select any of the certificates, 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** > **Manage 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 Application server 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.

Reconfiguring an expired sub CA

About this task

If you configure System Manager as a sub CA and if the sub CA expires, you cannot access all sections of the System Manager web console due to security reasons.

Procedure

From Release 10.1.x, to reconfigure an expired sub CA, the administrator can perform one of the following options:

- Option 1: Click **Create new Default CA**.

  The createCA CLI utility creates a new root CA and makes that CA the default System Manager CA. The utility also issues new certificates for System Manager.

  For information on configuring SubCA in System Manager, see Generating the certificate signing request on page 1247.

  Note:

  Creating a new default CA involves the restart of System Manager.

- Option 2: Click **Exit**.

  Exits the utility.

Note:

The createCA CLI utility works even if the System Manager CA expires. If the CA has not expired, the createCA CLI utility displays four options instead of the two options displayed above.

For information about the four options of the createCA CLI utility, see Overview of System Manager root certificate authority created using SHA256withRSA signing algorithm and 2048 key size on page 1239.

Configuring DTLS for CS 1000

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Select the CS 1000 element.
4. Click **More Actions** > **Manage 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 navigation pane, click **Manage Elements**.
3. Select the CS 1000 element.
4. Click **More Actions** > **Manage 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**.

Managing certificate revocation list

Creating a new CRL

About this task

You can create a new updated Certificate Revocation List (CRL) to immediately revoke or unrevoke a certificate issued by System Manager as a certificate authority.

Note:

System Manager as a certificate authority does not support Delta CRLs and the Avaya Aura® elements also do not validate Delta CRL. Therefore, do not create Delta CRL from System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **CA Structure & CRLs**.
4. Click **Create CRL**.

   The system creates an updated CRL and displays the time stamp of the updated CRL.
5. Click **Get CRL**.

   The **Certificate Revocation List** dialog box displays the serial numbers of revoked certificates.

Configuring HTTP proxy

Certificate revocation list overview

In simple terms, a Certificate Revocation List (CRL) is a type of blocklist of digital certificates that Certificate Authority organizations (CAs) deem as untrustworthy or that they are no longer willing to vouch for. It is a list of digital certificates that have been revoked by the issuing CA.

From release 10.2.1.1 and later, Avaya Aura® supports HTTP proxy to download CRLs. CRL download using a proxy eliminates the requirement for a direct connection to the Certificate Authority (CA), which can be a security risk.

This release supports the HTTP proxy type with basic authentication, which requires a username and password. Alternatively, customers can configure proxy support without authentication. Customers can configure up to three proxies as a maximum at any time.

Customers can configure the frequency with which Avaya Aura® checks for updates to CRLs and downloads a new CRL. To enable this functionality, customers can configure a CRL download job.

System Manager and Session Manager use these configuration settings in tandem. So, it is important to understand the implications of these settings for Session Manager.

Session Manager uses the HTTP proxy settings for both CRL download and Push Notification. The new feature for HTTP proxy overrides any configuration on the Global Settings for Session Manager. Session Manager uses HTTP proxy configurations in priority order, as they appear on the HTTP Proxy screen. For more information, see *Administering Avaya Aura® Session Manager*.

Related links

Adding an HTTP proxy on page 1262
Editing an HTTP proxy on page 1262
Deleting an HTTP proxy on page 1263
HTTP proxy field descriptions on page 1264
HTTP proxy support checklist on page 1261

HTTP proxy support checklist

Use this checklist to configure a HTTP proxy and test the CRL download.

From release 10.2.1.1 and later, Avaya Aura® supports HTTP proxy to download CRLs. CRL download using a proxy eliminates the requirement for a direct connection to the Certificate Authority (CA), which can be a security risk.

No.	Task	Description	Notes	✔
1	Add a new HTTP proxy.		Adding an HTTP proxy on page 1262	
2	Add a new CRL download job.	Ensure that you enable **Use HTTP proxy**.	Configuring CRL download on page 1265	
3	Check the Global Settings in Session Manager.	The new feature for HTTP proxy overrides any configuration on the Global Settings for Session Manager.	For more information, see *Administering Avaya Aura® Session Manager*.	

Related links

Adding an HTTP proxy on page 1262
Editing an HTTP proxy on page 1262

Deleting an HTTP proxy on page 1263
Certificate revocation list overview on page 1260

Adding an HTTP proxy

About this task

You can add a new HTTP Proxy to configure the details and enable them for use within the system.

Multiple proxies can be administered. If more than one proxy is administered, the first accessible proxy in the list will be used.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Configuration** > **HTTP Proxy**.

   System Manager displays **HTTP Proxy Configuration**.
3. In the **HTTP Proxy Configuration**, under the **HTTP Proxy Configuration Data**, click **Add**.

   System Manager displays **Add HTTP Proxy Configuration Data**.
4. In the **Add HTTP Proxy Configuration Data**, under **HTTP Proxy Config Data**, enter or select the following information:
   a. In **Proxy Name**, enter a unique proxy name. For example, Proxy1.
   b. In **FQDN/IP Address**, enter a valid FQDN or IP Address. For example, 10.129.179.83.
   c. In **Port Number**, enter a valid port number. For example, 3130.
   d. In **Proxy Connection Type**, select HTTP.
   e. In **Proxy Authentication Method**, select either **NONE** or **BASIC**.

   Note:

   For **Proxy Authentication Method**, if you select **BASIC**, enter **Username** and **Password**.
5. Click **Commit**.

   An HTTP Proxy is created.

Related links

Certificate revocation list overview on page 1260
HTTP proxy field descriptions on page 1264
HTTP proxy support checklist on page 1261

Editing an HTTP proxy

About this task

You can edit an existing HTTP Proxy configuration to modify the settings, such as the Proxy Server Address, Port Number, or Proxy Authentication Method. You cannot edit Proxy Name. Edit

is not allowed if an HTTP proxy is being used in a CRL download job and the CRL download job is in a running state.

Before you begin

- A minimum of one HTTP Proxy must be listed.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Configuration** > **HTTP Proxy**.

   System Manager displays **HTTP Proxy Configuration**.
3. In **HTTP Proxy Configuration**, under **HTTP Proxy Configuration Data**, select the check box for the required HTTP Proxy and click **Edit**.

   System Manager displays the **Edit HTTP Proxy Configuration Data**.

   Note:

   Only one HTTP Proxy can be edited at a time.
4. In **Edit HTTP Proxy Configuration Data,** under **Edit HTTP Proxy Config Data**, edit one or more of the following fields:
   - **FQDN/IP Address**
   - **Port Number**
   - **Proxy Authentication Method**

   Note:

   For **Proxy Authentication Method**, if you select **BASIC**, enter **Username** and **Password**.
5. Click **Commit**.

   The selected HTTP Proxy is edited, and the status is displayed in the top left corner.

Related links

Certificate revocation list overview on page 1260
HTTP proxy field descriptions on page 1264
HTTP proxy support checklist on page 1261

Deleting an HTTP proxy

About this task

You can delete an existing HTTP Proxy configuration if the HTTP Proxy is no longer needed or obsolete. Delete is not allowed if an HTTP proxy is being used in a CRL download job and only one HTTP proxy configuration is present.

Before you begin

- A minimum of one HTTP Proxy must be listed.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Configuration** > **HTTP Proxy**.

   System Manager displays **HTTP Proxy Configuration**.
3. In **HTTP Proxy Configuration**, under **HTTP Proxy Configuration Data**, select the check box for the required HTTP Proxy and click **Delete**.

   Tip:

   To delete all available HTTP Proxies, click **Select All** and click **Delete**.
4. When prompted with **Are you sure you want to delete the selected proxy?**, click **OK**.

   The selected HTTP Proxy is deleted, and the status is displayed in the top left corner.

Related links

Certificate revocation list overview on page 1260
HTTP proxy field descriptions on page 1264
HTTP proxy support checklist on page 1261

HTTP proxy field descriptions

All fields are mandatory.

The combination of **FQDN/IP Address** and **Port Number** fields must be unique.

Name	Description
Proxy name	A unique name for the proxy.
FQDN/IPAddress	An Internet Protocol (IP) or Fully Qualified Domain Name (FQDN) for the proxy. System Manager supports IPv4 or IPv6. Session Manager does not support IPv6 for either CRL download or Push Notification. The combination of **FQDN/IP Address** and **Port Number** fields must be unique.
Port Number	The port number for the proxy. For example, 3130.
Proxy Connection Type	Avaya Aura® supports HTTP.
Proxy Authentication Method	Choose from: • NONE • BASIC If you choose BASIC, enter a username and password for authentication.

Button	Description
Commit	Click to save updates.
Cancel	Click to exit the screen without saving changes.

Related links

Adding an HTTP proxy on page 1262
Editing an HTTP proxy on page 1262
Deleting an HTTP proxy on page 1263
Certificate revocation list overview on page 1260

Configuring CRL download

About this task

You can schedule a download job to periodically download the updated Certificate Revocation List (CRL) to check for revoked or unrevoked certificates.

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Configuration** > **CRL Download**.
3. On the CRL Download Configuration page, click **Add**.

   System Manager displays the Schedule CRL Download page.
4. In **Job Name**, type the job name.
5. In **Job Frequency**, set the frequency and recurrence.

   For more information, see “Schedule CRL Download field descriptions”.
6. In **Configure CRL Distribution Point**, type the CRL distribution point URL, and click **Add**.

   The URL for **CRL Distribution Point** does not support the Windows Universal Naming Convention (UNC) format.
7. Click **Commit**.

Related links

Schedule CRL Download field descriptions on page 1265

Schedule CRL Download field descriptions

Note:

If Certificate Revocation Validation is set to BEST_EFFORTS or MANDATORY, scheduling a CRL download is necessary when using third party certificates.

Name	Description
Job Details	Expands and collapses the **Job Details** section.
Job Frequency	Expands and collapses the **Job Frequency** section.

Table continues…

Name	Description
Configure CRL Distribution Point	Expands and collapses the **Configure CRL Distribution Point** section.
Expand All	If collapsed, expands all the sections.
Collapse All	If expanded, collapses all the sections.

Job Details

Name	Description
Job Name	The name of the download job.

Job Frequency

Name	Description
Task Time	Options to select the date, time, and time zone.
Recurrence	Options to set the recurrence of the download job.
Range	Options to set the date range for the end of the download job.

Configure CRL Distribution Point

Name	Description
CRL Distribution Point	The option to enter a single or multiple CRL distribution points. The URL for **CRL Distribution Point** does not support the Windows Universal Naming Convention (UNC) format.
Use HTTP Proxy	Check this box to enable HTTP proxy support for this CRL download.

Icon	Description
	Refreshes the information of the CRL distribution points in the table.

Button	Description
Add	Validates and adds the entered CRL distribution point.
Show	Shows the selected number of CRL distribution points.
Previous	Displays the CRL distribution points on the previous page. This button is unavailable on the first page.
Next	Displays the CRL distribution points on the next page. This button is unavailable on the last page.
Commit	Creates the CRL download job and displays the CRL Download Configuration page.
Cancel	Cancels the changes and returns to the CRL Download Configuration page.

Related links

Configuring CRL download on page 1265

Deleting a CRL download job

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Configuration** > **CRL Download**.

   The system displays the CRL Download Configuration page.
3. In **CRL Download Jobs**, select a job and click **Delete**.
4. In the Confirm Job Delete dialog box, click **Ok**.

   The system deletes the selected download job.

Viewing CRL download job

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Configuration** > **CRL Download**.

   The system displays the CRL Download Configuration page.
3. In **CRL Download Jobs**, select a job and click **View**.

   The system displays the CRL Download Job Details page with all the download job details.
4. Click **Done** to return to the CRL Download Configuration page.

CRL Download Configuration field descriptions

Name	Description
Select check box	The option to select a download job.
Job Name	The name of the download job.
HTTP Proxy Used	Indicates if the CRL downloaded using an HTTP proxy. Possible values are YES and NO. • YES indicates that a HTTP proxy is used for the CRL download. • NO indicates that a HTTP proxy is not used.
Last Run Date	Details of the last run download job, such as date, time, and time zone.
Last Run Status	The status of the last run download job, such as date, time, and time zone.
Job State	The current state of the download job.
Frequency	The frequency of the download job.
Scheduled By	The name of the user who scheduled the download job.

Button	Description
Add	Displays the Schedule CRL Download page to create a new download job.
Delete	Displays the Confirm Job Delete dialog box to confirm the deletion of the download job.
View	Displays the CRL Download Job Details page with all the details of the download job.
Show All	Shows all the download jobs.
Select : All	Selects all the download jobs.
Select : None	Clears the selected download jobs.
Previous	Displays the download jobs in the previous page. This button is unavailable on the first page.
Next	Displays the download jobs in the next page. This button is unavailable on the last page.

Icon	Description
	Refreshes the certificate information in the table.

CRL Download Job Details field descriptions

Name	Description
Job Name	The name of the download job.
CRL Distribution Point	The configured CRL distribution point for the download job.
Last Run Date	Details of the last run download job, such as date, time, and time zone.
Last Run Status	The status of the last run download job, such as date, time, and time zone.
Last Successful Download Date	The date when the download job successfully downloaded the CRL.

Button	Description
Done	Displays the CRL Download Configuration page listing all available download jobs.

Security Configuration field descriptions

Global - TLS Configuration

Name	Description
Minimum TLS Version	The option to select the minimum TLS version to be supported. The options are: • **TLSv1.0** • **TLSv1.1** • **TLSv1.2** • **TLSv1.3** **Note:** TLS 1.0 and TLS 1.1 have known vulnerabilities, and Avaya do not recommend to use these TLS versions. If **Minimum TLS Version** is set to **TLSv1.0** or **TLSv1.1**, System Manager displays the following message in the **Notifications** widget: `Warning! TLS <1.0/1.1> is enabled. For increased security, it is recommended that the Minimum TLS Version be set to TLS 1.2 or higher if these protocol levels can be supported in your configuration.` For the new System Manager deployment, the minimum TLS version is set to 1.2. From Release 10.1, **SSLv3** is not supported. On the earlier release system, if the minimum TLS version is configured to: • **SSLv3**, System Manager sets the value to **TLSv1.0** after upgrading to Release 10.1 and later. • Any other TLS version value, System Manager retains the TLS version after upgrading to Release 10.1 and later. For a military hardened system, the minimum TLS version is set to 1.2.

Revocation Configuration

Name	Description
Certificate Revocation Validation	The option to select the validation type for certificate revocation.

Table continues…

Name	Description
Revocation Type	The option to select the certificate revocation type. This option cannot be changed if **Certificate Revocation Validation** is set to **NONE**. **Note:** Only System Manager Release 7.1 and later supports **OCSP**. Other elements of Avaya Aura® Suite do not support **OCSP**. Therefore, Avaya recommends not to change the **Revocation Type** setting to **OCSP**.
Revocation Type Preference	The option to select the certificate revocation type. This option can be edited if **Revocation Type** is set to **BOTH**.
Check method	The option to select the checking method for the certificate. This option cannot be changed if **Certificate Revocation Validation** is set to **NONE**.

SMGR - Cert based authentication

Name	Description
For System Manager User Interface	The option to enable or disable certificate-based authentication for the System Manager user interface.
For Other TLS Ports	The option to enable or disable certificate-based authentication for other TLS ports.

Extended hostname validation

Name	Description
Extended Hostname Validation	The option to enable or disable extended hostname validation.

Button	Description
Commit	Saves and commits any changes made in the security configuration with an automatic restart of the Application server.
Cancel	Cancels any changes made and reverts the security configuration settings to the last saved setting.

Deletion of expired certificates data from System Manager

With Release 8.1.3, you can use the **Number of days after which system deletes expired certificates** field on the **Services** > **Configurations** > **Settings** > **SMGR** > **Trust Management** page to set the number of days after which System Manager deletes the data of expired certificates from the System Manager database.

This only applies to the data of expired certificates that are generated by System Manager which act as a CA or sub CA.

By default, System Manager runs **ExpiredCertificateRemovalJob** once a week at midnight based on the system timezone to check the expired certificates. If the certificate is expired and expiry date is more than the number of configured days, System Manager purges the data of expired certificates.

Extended Hostname Validation

With the Extended Hostname Validation (EHV) feature, the system validates the host name or domain name of the server with the value in the **subject** or **subjectAltName** (SAN) field in the identity certificate for establishing the SSL connection.

Enabling Extended Hostname Validation

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Configuration** > **Security Configuration**.
2. On the Security Configuration page, click **SMGR**.
3. In the Extended hostname validation section, select the **Extended Hostname Validation** check box.
4. 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

Note:

- If you are using Microsoft Active Directory for external authentication with System Manager, the **userPrincipalName** attribute of the user in the external server must contain a valid value.
- If you are using the LDAP server other than Microsoft Active Directory for external authentication with System Manager, the **UID** attribute of the user in the external server must contain a valid value.
- If you have configured external authentication before upgrading to System Manager 10.1.3.3 or 10.2.0.1 and higher releases, reset **Password for Root Binding** through the web console following the upgrade.

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 Kerberos users, then local users
5. External LDAP users, then external RADIUS users, then local users
6. External RADIUS users, then external LDAP users, then local users
7. External KERBEROS users, then external multiple LDAP users, then local users

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 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**.

Provisioning of 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 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 **Provision First LDAP Server** and fill the required details in the fields.
5. **(Optional)** Select **Provision Second LDAP Server** and fill the required details in the fields.
6. Click **Save**.

Note:

Clearing the **Provision First LDAP Server** check box clears all the data in the first and second provision LDAP server sections.

Related links

Authentication Servers field descriptions on page 1275

Provisioning the RADIUS server

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the 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 RADIUS Server option.
5. In the Provision RADIUS Server section, enter the relevant information.

   You must create two records in the external RADIUS server with the same shared secret for both the primary security server and the backup security server IP address.
6. Click **Save**.

   Note:

   Ensure that the Linux iptable firewall setting on both the primary and the backup security service has UDP port as the source port.

Related links

Authentication Servers field descriptions on page 1275

Provisioning the Kerberos server

About this task

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, do the following:
  1. In 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 with admin privileged credentials.

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the 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 Kerberos Server** option.

5. In the **Provision Kerberos Server** section, enter 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.
6. 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

Authentication Servers field descriptions on page 1275

Provisioning user certificate authentication

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the 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 information in the Provision User Certificate Authentication section.
5. Click **Save**.

   Note:

   To use **User Certificate Authentication**, go to the **Provision User Certificate Authentication details** section.

Authentication Servers field descriptions

Provision First and Second 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	The connection type supported by the LDAP server.

Table continues…

Name	Description
Is Active Directory	The field to select if active directory does not support anonymous binding.
Supports Anonymous Binding	The field to select if active directory supports anonymous binding. **Supports Anonymous Binding** field is inactive if **Is Active Directory** field is enabled.
Distinguished Name for Root Binding	The distinguished name for the root binding. For example, type `cn` for Users.
Password for Root Binding	The password for the root binding in this field. From Release 8.1.3, you can enter up to 256 characters for the LDAP server authentication.

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	The shared secret of the RADIUS server.

Provision Kerberos Server

Name	Description
DC Host Name (FQDN)	The FQDN in the following format: machineName.domainName.com/net/.
DC Computer Domain	The domain name of the Kerberos server.
Keytab File	The field to select the encrypted Kerberos server key.

Provision SAML Remote Identity Provider

Name	Description
Entity ID	The entity ID of the provisioned SAML remote identity provider. The text “-- not configured -- ” is displayed if a Remote Identity Provider is not configured.
Metadata Type	The method to query the metadata for Remote Identity Provider. The options are: • URL. A valid HTTP URL. • File. A valid XML file.
Metadata Url	The valid HTTP URL for the metadata of Remote Identity Provider. This field is disabled if the **File** option is selected in the **Metadata Type** field.
Metadata File	The valid XML file for the metadata of Remote Identity Provider. This field is disabled if the **URL** option is selected in the **Metadata Type** field.

Table continues…

Name	Description
Choose File	The field to select an XML file that contains the metadata for Remote Identity Provider.

Provision User Certificate Authentication

Name	Description
Certificate Purpose	The purpose of the certification, such as Client Authentication.
Certificate Field Name to get User Name	The fields that can be used to retrieve the username from the certificate. The left section contains the fields that can be read from the certificate. The right section contains the fields that the system will read from the certificate.

Button	Description
Remove	Removes the selected client purpose.
Add	Adds the typed client purpose.
>>	Moves the selected certificate field to the right pane.
<<	Moves the selected certificate field to the left pane.
Up	Increments the priority of the selected certificate field.
Down	Decrements the priority of the selected certificate field.

Button	Description
Save	Saves your settings on the Authentication Servers page.
Cancel	Cancels your action and takes you to the earlier 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-fqdn>>?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 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 Application server 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

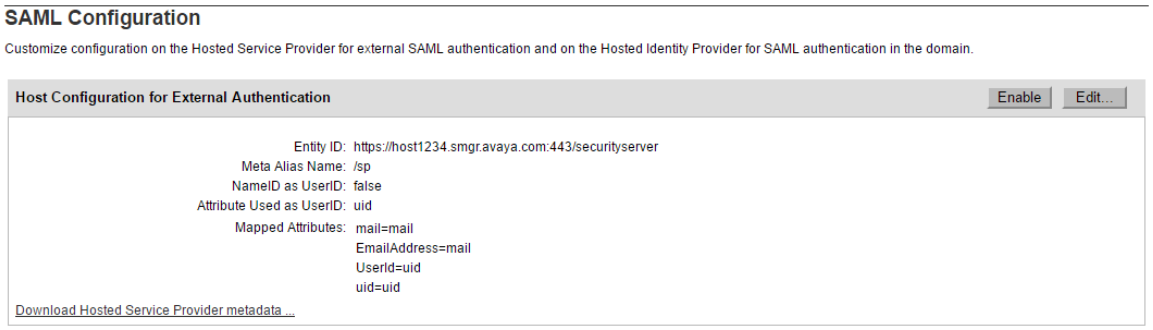
The system automatically configures System Manager as Hosted Service Provider during the installation of System Manager and upgrade of System Manager from Release 6.2.

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 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.



   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.

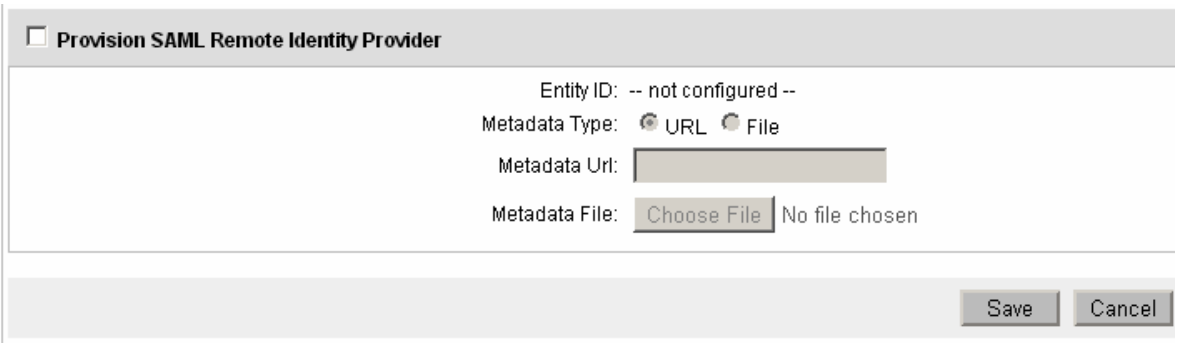
Related links

Adding trusted certificates on page 1205
Provisioning Remote Identity Provider on page 1281

Provisioning Remote Identity Provider

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the 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.



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

Authentication Servers field descriptions on page 1275

SAML setup

Configuring SSO between System Manager and Microsoft ADFS

About this task

Use the following procedure to configure SAML authentication with Single Sign-On (SSO) between System Manager and Microsoft Active Directory Federation Services (ADFS).

In this procedure, the ADFS server is used as an example to configure SAML authentication.

Before you begin

Install Microsoft Windows server with ADFS.

Procedure

1. Establish SSL trust between System Manager and Active Directory Federation Service.
   a. Importing System Manager CA certificate into ADFS.
   b. Importing ADFS CA certificate into System Manager.
2. Configure System Manager as a Relying Party (RP) in ADFS.
   a. Configuring System Manager SAML Service Provider.
   b. Exporting System Manager SAML Service Provider Metadata.
   c. Adding System Manager as a Relying Party.
   d. Defining Claim Rules.
3. Configure ADFS for Form based authentication.
4. Configure ADFS as a Remote Identity Provider (R-IDP) in System Manager.
   a. Exporting ADFS metadata.
   b. Adding ADFS as an R-IDP in System Manager.
5. Use SSO to launch the System Manager web console from ADFS.

Establish SSL trust between System Manager and Active Directory Federation Service

Importing System Manager CA certificate into ADFS

Procedure

1. Log in to the System Manager command-line interface with administrator credentials.
2. Navigate to **Security** > **Certificates** > **Authority** > **CA Structures & CRLs**.
3. Click **Download PEM File** to download and save the CA certificate in the `SystemManagerCA.cacert.pem` format.
4. In the ADFS server, import `SystemManagerCA.cacert.pem` to the **Certificates** folder.

   Note:

   For more information on importing a System Manager CA certificate from your local computer to the ADFS server, see Microsoft website documentation.

Next steps

Import ADFS CA certificate into System Manager. See Importing ADFS CA Certificate into System Manager on page 1283.

Importing ADFS CA certificate into System Manager

Procedure

1. In the ADFS server, export a CA certificate to the required file format.

   Note:

   For more information on exporting a CA certificate from the ADFS server, see Microsoft website documentation.
2. Log in to the System Manager command-line interface with administrator credentials.
3. Navigate to **Inventory** > **Manage Elements**.
4. In **Elements**, click the **System Manager** element.
5. In **More Actions**, select **Manage Trusted Certificates**.
6. Click **Add** to add CA certificates from the ADFS server.

   Note:

   For more information on adding a trusted certificate, see Adding trusted certificates on page 1205.

Configure System Manager as a Relying Party in ADFS

Configuring System Manager for SAML Service Provider

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. Navigate to **User Services** > **External Authentication** > **SAML Configuration**.
3. Click **Edit**.
4. On the SAML Hosted Service Provider page, perform the following:
   a. Select **NameID as UserID** check box or **Attribute Used as UserID** field to use the NameID from SAML response or the attribute name from SAML Response as the UserID of an account in System Manager.
   b. In the **Mapped Attributes** field, enter an attribute to map attributes from SAML Response to user attributes in System Manager.
   c. Click **Save**.

Next steps

Export System Manager SAML Service Provider metadata. See Exporting System Manager SAML Service Provider metadata on page 1284.

Exporting System Manager SAML Service Provider metadata

Procedure

1. Log in to the System Manager command-line interface with the admin credentials.
2. Navigate to **Administrators** > **User Services** > **External Authentication** > **SAML Configuration**.
3. Click the **Download Hosted Service Provider metadata** link to download and save `spMetadata.xml`.

   Note:

   Alternatively, record `https://<smgr_fqdn>/securityserver/saml2/jsp/exportmetadata.jsp` to download the metadata directly to ADFS.

Next steps

Add System Manager as a Relying Party. See Adding System Manager as a Relying Party on page 1284.

Adding System Manager as a Relying Party

Procedure

1. In the ADFS server, import the `spMetadata.xml` file from System Manager.

Note:

For more information on steps to import the `spMetadata.xml` file from System Manager, see documentation in the Microsoft website.

2. To apply the changes, you must restart the Application server. At the prompt, type `smgr restart`.

Next steps

Define Claim Rules. See Defining Claim Rules on page 1285.

Defining Claim Rules

About this task

In the ADFS server, Claim Rules define how an incoming authentication request is processed by ADFS and what user related information is added to the SAML Response.

Procedure

In ADFS, add an outgoing rule and an incoming rule.

Note:

Create an outgoing rule first and then an incoming rule. For more information on steps to add an outgoing and incoming rule, see documentation in the Microsoft website.

Configuring ADFS for Form based authentication

Procedure

1. In the ADFS server, add an authentication type and set a first authenticator.

   Note:

   For more information on steps to add the correct authentication type and authenticator, see documentation in the Microsoft website.

2. Save and close.

Configure ADFS as a Remote Identity Provider (R-IDP) in SMGR

Exporting ADFS metadata

Procedure

1. In the ADFS server, open a browser and type the following URL: https://localhost/federationmetadata/2007-06/Federationmetadata.xml
2. Download and save the `Federationmetadata.xml` file.
3. Edit the xml file to delete elements that System Manager does not need.

Note:

Delete the following sections:

- ds:Signature
- RoleDescriptor
- SPSSODescriptor

4. Save and close the file.

Next steps

Add ADFS as Remote Identity Provider in System Manager. See Adding ADFS as a Remote Identity Provider in System Manager on page 1286

Adding ADFS as a Remote Identity Provider in System Manager

Procedure

1. Log in to the System Manager command-line interface with the administrator credentials.
2. Navigate to **Administrators** > **User Services** > **External Authentication**.
3. On the External Identity Repositories page, in the **Authentication Servers** section, click **Configure**.
4. Select **Provision SAML Remote Identity Provider**.
5. Select **Metadata Type** as **File**.
6. Browse and upload Metadata File from the Exporting ADFS metadata section.

Launching the System Manager web console from ADFS using SSO

Procedure

1. In the ADFS server, open a browser and type the following URL: `https://<<smgr-fqdn>>/?performsso=saml`.
2. In the login page, type user name and password.

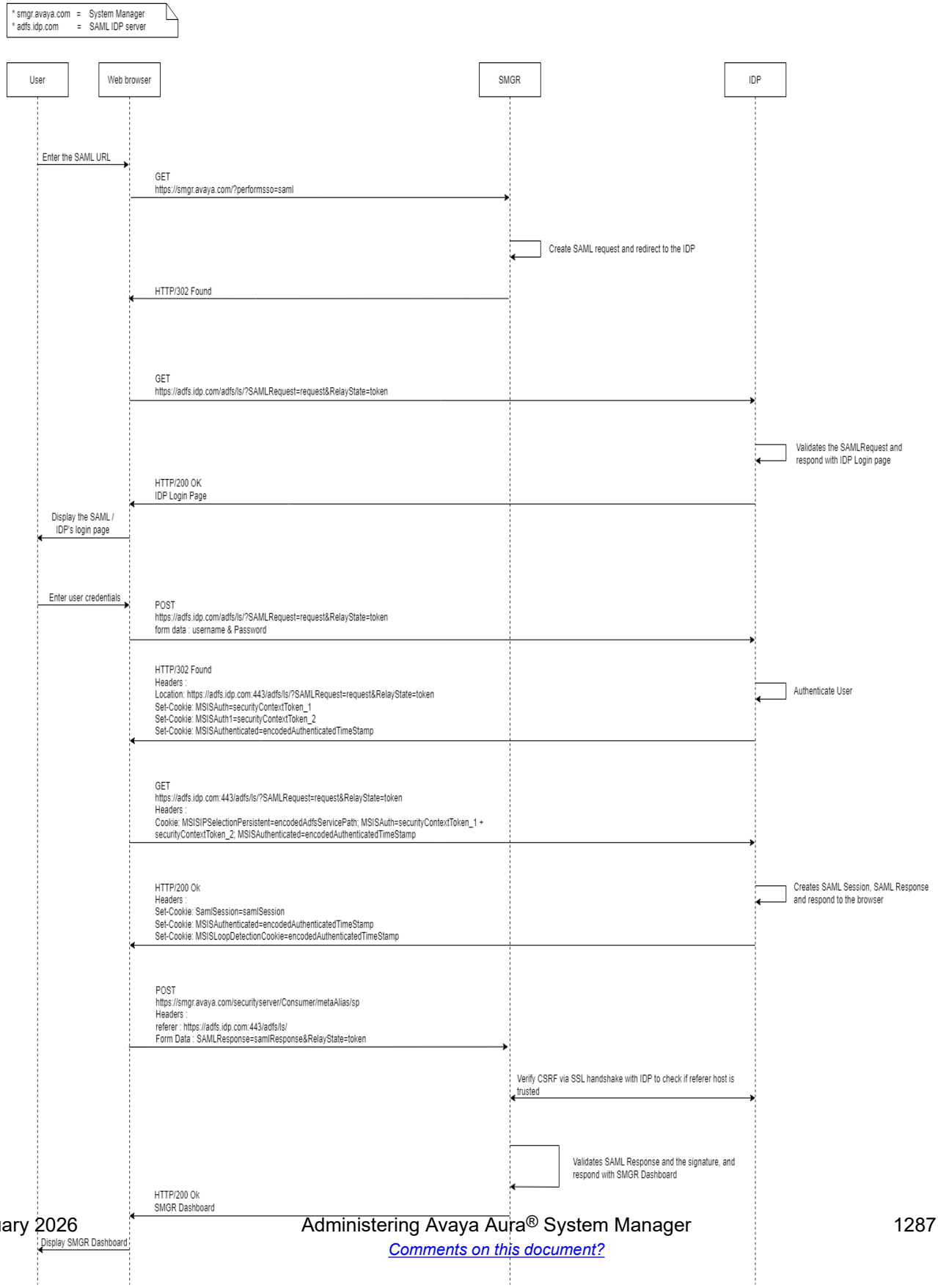
   Note:

   For information about user name and password, see documentation in the Microsoft website.

3. Click **Sign In**.

   ADFS validates login credentials and redirects the user to System Manager. Based on the Claim Rules set in the Defining Claim Rules section, user name mapped to System Manager is the User Principal Name.

SAML sequence and flow diagram for SAML SSO authenticate for System Manager



Active sessions

Viewing active sessions

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the 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 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.

Regenerating data protection keys

Regenerating symmetric keys for System Manager

About this task

Use this procedure to execute the utility to regenerate data protection keys. System Manager administrator must execute the utility manually when one or more of the following conditions are met:

- Commercial grade hardening is enabled in System Manager.
- Sensitive data, such as user or communication profile passwords, are suspected to be compromised.
- The older data encryption keys must be replaced.

Before you begin

- Create a data backup of System Manager before running this utility.

- On Geographic Redundancy-enabled System Manager, disable replication before executing this utility.

  For more information, see “Disabling the Geographic Redundancy replication”.
- Stop the System Manager Application server.

Note:

The utility takes longer when a large amount of data is present on System Manager. Therefore, Avaya recommends that you run this utility during the System Manager maintenance window.

Procedure

1. Log in to the System Manager command line interface.
2. Type `cd $MGMT_HOME/securestore`, and press `Enter`.
3. Type `sudo $MGMT_HOME/securestore/migrateORRegenSecureStores.sh 3600`, and press `Enter`.
4. At the prompt, type one of the following and press `Enter`:
   - `1` to run the utility for all domains
   - `2` to run the utility for specific domains
   - `3` to exit the utility
5. To run the utility for specific domains, enter the domain name and press `Enter`.

   The system executes the utility as a background process. Thus, if the SSH session is terminated, the utility execution is not affected.
6. To view the result, type `vim $AVAYA_LOG/migrateOrRegenSecureStore.log` and press `Enter`.

Related links

Disabling the Geographic Redundancy replication on page 106

Regenerating asymmetric keys for System Manager

About this task

Use this procedure to execute the utility to regenerate asymmetric data protection keys. System Manager administrator must run this shell-based utility in one or more of the following conditions:

- One or more asymmetric keys are suspected to be compromised.
- **Key Management Properties** sends a trap notification.
- Asymmetric keys are outdated and need to be regenerated.

Before you begin

- Stop the System Manager Application server.

Note:

The utility takes more time to run when a large amount of data is present on System Manager. Therefore, Avaya recommends that you run this utility during the System Manager maintenance window.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Type `cd /opt/vsp`, and press `Enter`.
3. Type `sh regenerateSSHKeys.sh`, and press `Enter`.

Next steps

1. Start the System Manager Application server.
2. Using the Solution Deployment Manager client, reestablish connection for all client elements.

Regenerating asymmetric keys for geographic redundancy-enabled System Manager

About this task

Use this procedure to execute the utility to regenerate asymmetric data protection keys. System Manager administrator must run this shell-based utility in one or more of the following conditions:

- One or more asymmetric keys are suspected to be compromised.
- **Key Management Properties** sends a trap notification.
- Asymmetric keys are outdated and need to be regenerated.

Before you begin

- Disable geographic redundancy replication.

  For more information, see “Disabling the Geographic Redundancy replication”.
- Convert the primary System Manager server to a standalone server.

  For more information, see “Converting the primary System Manager server to the standalone server”.
- Stop the System Manager Application server.

Note:

The utility takes more time to run when a large amount of data is present on System Manager. Therefore, Avaya recommends that you run this utility during the System Manager maintenance window.

Procedure

1. Log in to the System Manager command line interface.
2. Type `su - root`, and press `Enter`.

3. Provide the root password, and press `Enter`.
4. Type `cd /opt/vsp`, and press `Enter`.
5. Type `sh regenerateSSHKeys.sh`, and press `Enter`.
6. Start the System Manager Application server.

Next steps

1. Configure System Manager to enable geographic redundancy.

   For more information, see “Enabling the Geographic Redundancy replication”.
2. Using the Solution Deployment Manager client, reestablish connection for all client elements.

Related links

Disabling the Geographic Redundancy replication on page 106
Converting the primary System Manager server to the standalone server on page 114
Enabling the Geographic Redundancy replication on page 105
Re-establishing trust for Solution Deployment Manager elements on page 1400

Chapter 21: Managing tenants

Multi Tenancy

Tenant is a client organization that uses Team Engagement OnAvaya Aura – Unified Communications 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.

- **Multi Tenancy elements:** Communication Manager, Avaya Messaging, and Session Manager
- **Single Tenancy elements:** UCM Applications and Messaging

Note:

The elements that do not support any type of Multi Tenancy must not be configured for the User Provisioning Rule that the user wants to add to the tenant site because the system validates each User Provisioning Rule against the elements that are available in the Tenant site. In case the User Provisioning Rule contains elements, which do not support Single or Multi Tenancy, then the administrator cannot add the User Provisioning Rule to the tenant site.

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 49

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 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.

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 maximum 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.

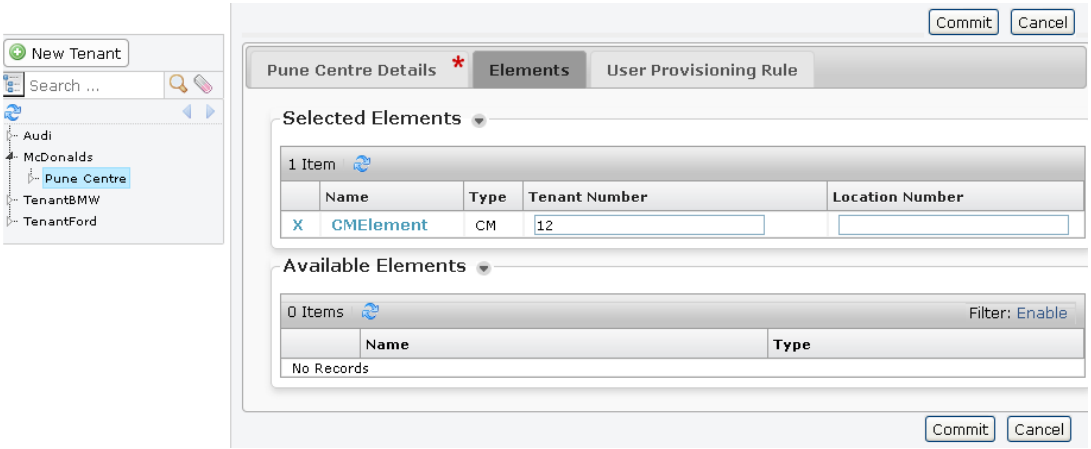
   For more information, see Create Tenant field descriptions.
4. On the Administrators tab, in the Assigned Admin Users section, perform the following:
   a. Click **New**.
   b. In the Create Admin User area, provide the details of the administrator that you want to assign to the tenant.
   c. Click **Commit**.
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:
- To assign an element to the site, click the plus sign (**+**) in the Available Elements section.

  Click X 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.

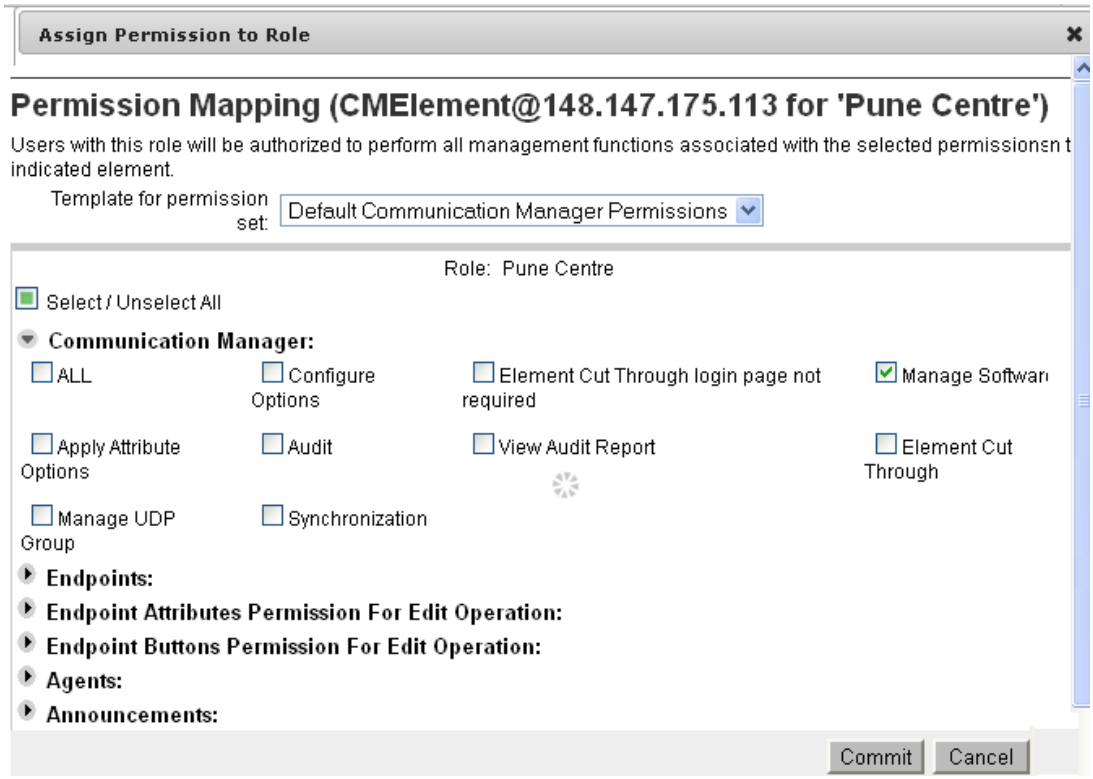


Note:

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.

- 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”.



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 X 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 178
Enabling Multi Tenancy on page 1293
Unassigning the tenant administrator on page 1298
Tenant Management field descriptions on page 1305
Create Tenant field descriptions on page 1305

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 1305
Create Tenant field descriptions on page 1305

Viewing the tenant

Before you begin

- Log on to the 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 want to view.
3. View the details of the tenant, site, department, or team.

Related links

Tenant Management field descriptions on page 1305
Create Tenant field descriptions on page 1305

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 1305
Create Tenant field descriptions on page 1305

Deleting a tenant

The Service Provider Administrator can delete the tenant and the tenant organization hierarchy.

Before you begin

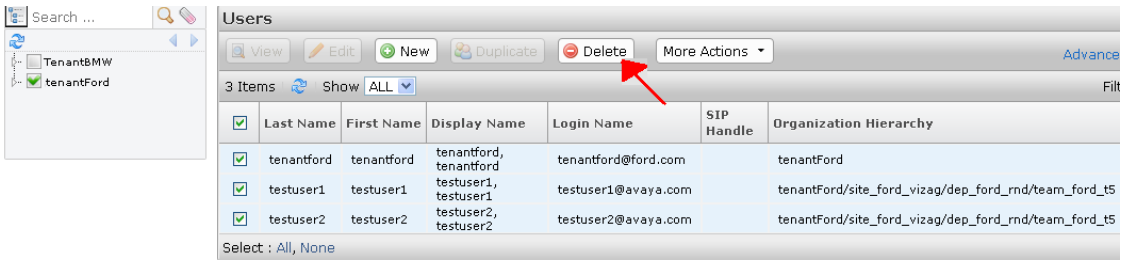
- Log on to System Manager Web Console as Service Provider Administrator.
- Enable the Multi Tenancy feature.
- Delete all users associated with the tenant.

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.



   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 1305
Create Tenant field descriptions on page 1305

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 Port Extension COR Tenant Number
VDN	Extension COR Tenant Number VDN of Origin Annc Extension Return Destination Conference Controller for Meet-me

Table continues…

Communication Manager object	Fields
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.

Field	Description
Level 1	The name for level 1. **Organization level** / **Default** / **Example** Level 1 / Site / Hyderabad Level 2 / Department / Loans Division Level 3 / Team / Customer Relations
Level 2	The name for level 2. The field is optional.
Level 3	The name for level 3. The field is optional.

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.

Table continues…

Name	Description
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.
Selected User Provisioning Rules	
Name	The name of the user provisioning rule that you selected from the Available User Provisioning Rules section.
X	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.

Table continues…

Name	Description
Description	A brief description of the level 3 hierarchy or team.

Chapter 22: 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 System Manager.

- 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

About this task

When you start the shutdown process, you cannot access the System Manager web console.

Before you begin

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

Procedure

1. On the System Manager web console, click **Services** > **Shutdown** > **Shutdown System Manager**.
2. In the Running and Pending Scheduled Jobs section, view the running and pending scheduled jobs.
3. In the Active User Sessions section, view the active user sessions.
4. On the System Manager web console, click **Services** > **Shutdown** > **Shutdown History**.
5. In Initiate Shutdown, click **Shutdown System Manager**.

   System Manager displays the Shutdown System Manager dialog box with the following message.

   ```
   The system initiates System Manager shut down after the grace
   period of 10 minutes, and stops all running jobs. Once you click
   Yes, you cannot abort this operation.
   ```

   ```
   The system notifies all the users who logged in before System
   Manager shuts down is initiated.
   ```

   ```
   Are you sure you want to shutdown System Manager?
   ```

6. To start the shutdown process, click **Yes**.

Related links

Edit Profile:GracefulShutdown field descriptions on page 889
View Profile:GracefulShutdown field descriptions on page 888

Rebooting the System Manager virtual machine from the web console

About this task

When you start the reboot process, you cannot access the System Manager web console.

Important:

If you configured a NFS mount on System Manager for Session Manager Performance Data (perfdata) collection, then, if and when you reboot/boot System Manager virtual machine, you need to ensure that you manually re-mount the NFS store once the System Manager VM is up and you are able to log in to the VM through SSH. Failure to re-mount the NFS partition will result in the Session Manager perfdata to go, by default, into a folder which is in the root (/) partition of the System Manager file system. This might cause the partition to get full which in-turn might cause issues with the System Manager application.

Before you begin

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

Procedure

1. On the System Manager web console, click **Services** > **Shutdown** > **Shutdown System Manager**.
2. In the Running and Pending Scheduled Jobs section, view the running and pending scheduled jobs.
3. In the Active User Sessions section, view the active user sessions.
4. In Initiate Reboot, click **Reboot System Manager**.

   System Manager displays the Reboot System Manager dialog box with the following message.

   ```
   The system initiates System Manager reboot after the grace period
   of 10 minutes, and stops all running jobs. Once you click Yes, you
   cannot abort this operation.

   The system notifies all the users who logged in before System
   Manager reboot is initiated.

   Are you sure you want to Reboot System Manager?
   ```

5. To start the reboot process, click **Yes**.

Rebooting the System Manager virtual machine through command-line interface

About this task

When you start the reboot process, you cannot access the System Manager web console.

Important:

If you configured a NFS mount on System Manager for Session Manager Performance Data (perfdata) collection, then, if and when you reboot/boot System Manager virtual machine, you need to ensure that you manually re-mount the NFS store once the System Manager VM is up and you are able to log in to the VM through SSH. Failure to re-mount the NFS partition will result in the Session Manager perfdata to go, by default, into a folder which is in the root (/) partition of the System Manager file system. This might cause the partition to get full which in-turn might cause issues with the System Manager application.

Procedure

1. Log in to the System Manager command-line interface.
2. Type **`rebootVM`** and press **Enter**.
3. At the **Do you want to continue ? .. (Yes/No)** prompt, type **Yes** and press **Enter**.

   System Manager starts the reboot process.

Viewing the shutdown history from the System Manager web console

Procedure

1. On the System Manager web console, click **Services** > **Shutdown** > **Shutdown History**.
2. On the Shutdown History page, you can view the shutdown history of the last shutdown actions.

   The Shutdown History page displays the date, time, and status of the shutdown action.

Shutdown System Manager field descriptions

Initiate Shutdown

Button	Description
Shutdown System Manager	Displays the Shutdown System Manager dialog box to select an option to start the shutdown process.

Initiate Reboot

Button	Description
Reboot System Manager	Displays the Reboot System Manager dialog box to select an option to start the reboot process.

Running and Pending Scheduled Jobs

Name	Description
Job Name	The job name as displayed on the Scheduler page.
Job Type	The job type as displayed on the Scheduler page.
Job Status	The status of the job.
Scheduled By	The name of the user who created the job
Start Time	The date and time the job is scheduled to start.

Active User Sessions

Name	Description
User Name	The user name who is currently active.
Session Duration	The session duration since when the user is active.
Is Current Session Status	The status of the current session. The status can be: • **true** • **false**

Chapter 23: 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 Avaya Aura® applications. Solution Deployment Manager supports the operations on the customer's Virtualized Environment and the Avaya Aura® Virtualized Appliance model.

Solution Deployment Manager supports migration of Virtualized Environment-based 8.1.x or 10.1.x applications to Release 10.2.x in the customer's Virtualized Environment. For migrating to Release 10.2.x and later, you must use Solution Deployment Manager Release 10.2.x and later.

Release 7.0 and later supports a standalone version of Solution Deployment Manager, the Solution Deployment Manager client. For more information, see *Using the Solution Deployment Manager client*.

System Manager with Solution Deployment Manager runs on:

- Customer-provided Virtualized Environment solution: Avaya Aura® applications are deployed on customer-provided, VMware® certified hardware.
- Software-Only environment: Avaya Aura® applications are deployed on the customer-owned hardware and the operating system.
- Avaya Solutions Platform 130: Avaya Aura® applications are deployed on the Avaya provided hardware.

Note:

- Solution Deployment Manager does not support that application deployment on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 Release 6.0.
- Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

With Solution Deployment Manager, you can do the following in Virtualized Environment, Avaya Solutions Platform 130, and Avaya Aura® Virtualized Appliance Release 8.x or earlier models:

- Deploy Avaya Aura® applications.
- Upgrade and migrate Avaya Aura® applications.

Note:

When an application is configured with Out of Band Management, Solution Deployment Manager does not support upgrade for that application.

For information about upgrading the application, see the application-specific upgrade document on the Avaya Support website.

- 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, and media modules
  - Session Manager
  - Branch Session Manager
  - AE Services

The upgrade process from Solution Deployment Manager involves the following key tasks:

- Discover the Avaya Aura® applications.
- Refresh applications and associated devices and download the necessary software components.
- Run the preupgrade check to ensure successful upgrade environment.
- Upgrade Avaya Aura® applications.
- Install software patch, service pack, or feature pack on Avaya Aura® applications.

For more information about the setup of the Solution Deployment Manager functionality that is part of System Manager 10.2.x, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

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 must be installed on the computer of the technician. The Solution Deployment Manager client provides the functionality to deploy the OVAs or ISOs on an Avaya-provided server, customer-provided Virtualized Environment, or Software-only environment.

A technician can gain access to the user interface of the Solution Deployment Manager client from the web browser.

Use the Solution Deployment Manager client to:

- Deploy System Manager and Avaya Aura® applications on Avaya appliances, VMware-based Virtualized Environment, and Software-only environment.
- Upgrade VMware-based System Manager from Release 8.1.x or 10.1.x to Release 10.2 and later.
- Install System Manager software patches, service packs, and feature packs.
- Configure Remote Syslog Profile.

- Create the Appliance Virtualization Platform Release 8.x or earlier Kickstart file.
- Generate the Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1 Kickstart file.
- Install Appliance Virtualization Platform patches.
- Restart and shutdown the Appliance Virtualization Platform host.
- Start, stop, and restart a virtual machine.
- Change the footprint of Avaya Aura® applications that support dynamic resizing. For example, Session Manager and Avaya Breeze® platform.

Note:

- You can deploy or upgrade the System Manager virtual machine only by using the Solution Deployment Manager client.
- You must always use the latest Solution Deployment Manager client for deployment.
- Solution Deployment Manager does not support that application deployment on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 Release 6.0.
- Solution Deployment Manager and Solution Deployment Manager Client does not support KVM on RHEL 8.10 images for a virtualized environment.

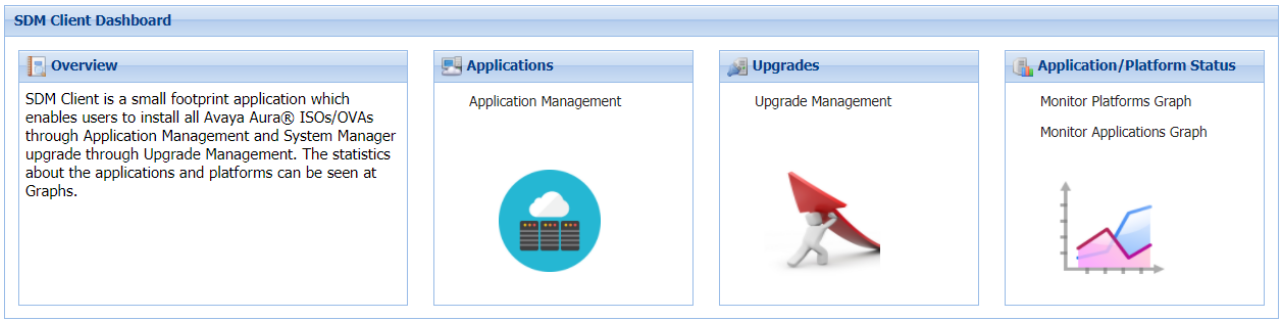


Figure 2: Solution Deployment Manager Client dashboard

Related links

Capability comparison between System Manager Solution Deployment Manager and the Solution Deployment Manager client on page 1317
Accessing the Solution Deployment Manager client dashboard on page 1322
Solution Deployment Manager client capabilities on page 1322

Capability comparison between System Manager Solution Deployment Manager and the Solution Deployment Manager client

Centralized Solution Deployment Manager	Solution Deployment Manager Client
Manage virtual machine lifecycle.	Manage virtual machine lifecycle.
Deploy Avaya Aura® applications excluding the System Manager application.	Deploy Avaya Aura® applications including the System Manager application.

Table continues…

Centralized Solution Deployment Manager	Solution Deployment Manager Client
Deploy hypervisor patches only for Appliance Virtualization Platform Release 8.x or earlier.	Deploy hypervisor patches only for Appliance Virtualization Platform Release 8.x or earlier.
Upgrade Avaya Aura® applications excluding the System Manager application.	Upgrade System Manager. For information, see *Upgrading Avaya Aura® System Manager*.
Install software patches for Avaya Aura® applications excluding the System Manager application.	Install System Manager patches.
Discover Avaya Aura® applications.	-
Analyze Avaya Aura® applications.	-
Create and use the software library.	-

Related links

Solution Deployment Manager Client on page 1316

Installing the Solution Deployment Manager client

Prerequisites for installing the Solution Deployment Manager client

1. If an earlier version of the Solution Deployment Manager client is running on the computer, remove the older version from **Control Panel** > **Programs** > **Programs and Features**.

   For information about uninstalling the Solution Deployment Manager client, see “Uninstalling the Solution Deployment Manager client”.

2. Ensure that Windows 8.1 64-bit, Windows 10 64-bit, Windows 11 64-bit, Windows Server 2016 64-bit, Windows Server 2019 64-bit, or Windows Server 2022 64-bit 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.

3. Ensure that at least 5 GiB of disk space is available to install the client. To deploy applications, you must have additional 15 GiB of disk space on your system.

   Note:

   A gibibyte = 1024^3 and gigabyte = 1000^3

   Tip:

   Using the Windows file explorer, click **Computer**, and verify that the Hard Disk Drives section displays the available disk space.

4. 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 to stop, and click **Stop**.

5. Ensure that the firewall allows the ports that are required to install the Solution Deployment Manager client and use the Solution Deployment Manager functionality.

   Note:

   System Manager 10.2.x Port Matrix lists all the ports and protocols that System Manager uses. You can access the System Manager 10.2.x Port Matrix document on the Avaya Support website at https://support.avaya.com/ by using valid credentials.

6. Ensure that ports support Avaya Aura® 10.2.x supported browsers.
7. Close all applications that are running on your computer.
8. 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 the **Advanced** tab, and click **Environment Variables**.
   c. Verify the system variables.

9. Ensure that the computer on which the Solution Deployment Manager client is running is connected to the network.

   Operations that you perform might fail if the computer is not connected to the network.

Related links

Solution Deployment Manager Client on page 1316

Installing the Solution Deployment Manager client on your computer

About this task

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 of only System Manager and hypervisor patches of Appliance Virtualization Platform.

Use the Solution Deployment Manager client to deploy, upgrade, and update System Manager.

Solution Deployment Manager must be used to deploy or upgrade Avaya Aura® applications on Avaya Aura® Appliance Virtualization Platform.

Note:

Solution Deployment Manager is not supported for Avaya Solutions Platform R6.0 (KVM on RHEL 8.10).

Procedure

1. Download the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.zip` file from the Avaya Support website at https://support.avaya.com or from the Avaya PLDS website, at https://plds.avaya.com/.
2. On the Avaya Support website, click **Product Support** > **Downloads**, and type the product name as **System Manager**, and Release as **10.2.x**.
3. Click the **Avaya Aura® System Manager Release 10.2.x SDM Client Downloads,10.2.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

   You can also copy the zip file to your software library directory, for example, `c:/tmp/Aura`.
4. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_10.2.0.0.xxxxxxx_xx.exe` file.

   The system displays the Avaya Solution Deployment Manager screen.
5. On the Welcome page, click **Next**.
6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.
7. On the Install Location page, perform one of the following:
   - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.

     If the `C:\Program Files\Avaya\AvayaSDMClient` directory is not empty, the installer displays the following message: `To install the SDM client, select an empty directory or manually delete the files from the installation directory.`

     If the file is locked and you are unable to delete it, reboot the machine, and then delete the file.
   - To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

     To restore the path of the default directory, click **Restore Default Folder**.

   The default installation directory of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient`.
8. On the Pre-Installation Summary page, review the information, and click **Next**.

9. On the User Input 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 software library directory on windows, in Select Location of Software Library Directory, click **Choose** and select a directory.

      The default software library of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient\Default_Artifacts`.

      You can save the artifacts in the specified directory.
   c. In **Data Port No**, select the appropriate data port.

      The default data port is 1527. The data port range is from 1527 through 1627.
   d. In **Application Port No**, select the appropriate application port.

      The default application port is 443. If this port is already in use by any of your application on your system, then the system does not enable you to continue the installation. You must assign a different port number from the defined range. The application port range is from 443 through 543.

      Note:

      After installing the Solution Deployment Manager client in the defined range of ports, you cannot change the port after the installation.
   e. **(Optional)** Click **Reset All to Default** to reset all values to default.
10. Click **Next**.
11. On the Summary and Validation page, 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 user must make the required disk space, memory, and the ports available to start the installation process again.
12. Click **Install**.
13. On the Install Complete page, click **Done** to complete the installation of Solution Deployment Manager Client.

    After the installation is complete, the installer automatically opens the Solution Deployment Manager client in the default web browser and creates a shortcut on the desktop.
14. To start the client, click the Solution Deployment Manager client icon,.

Next steps

- Configure the laptop to get connected to the services port if you are using the services port to install.
- Connect the Solution Deployment Manager client to Appliance Virtualization Platform through the customer network or services port.

For information about “Methods to connect the Solution Deployment Manager client to Appliance Virtualization Platform”, see *Using the Solution Deployment Manager client*.

Related links

Solution Deployment Manager Client on page 1316

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, do one of the following:

- On your computer, click **Start** > **All Programs** > **Avaya** > **Avaya SDM Client**.
- On your desktop, click .

Related links

Solution Deployment Manager Client on page 1316

Solution Deployment Manager client capabilities

The Solution Deployment Manager client provides the following capabilities and functionality:

- Runs on the following operating systems:
  - Windows 8.1, 64-bit Professional or Enterprise
  - Windows 10, 64-bit Professional or Enterprise
  - Windows 11, 64-bit Professional or Enterprise
  - Windows Server 2016, 64-bit Professional or Enterprise
  - Windows Server 2019, 64-bit Professional or Enterprise
  - Windows Server 2022, 64-bit Professional or Enterprise
- Supports the same web browsers as System Manager.
- Provides the user interface with similar look and feel as the central Solution Deployment Manager in System Manager.
- Supports deployment of System Manager. The Solution Deployment Manager client is the only option to deploy System Manager.
- Supports the Flexible footprint feature. The size of the virtual resources depends on the capacity requirements of Avaya Aura® applications.
- Defines the physical location for Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier, ESXi host, or Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0), 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 Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier or ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.

  Note:

  For the Avaya Aura® Messaging element, trust re-establishment is not required.

- Deploys the Avaya Aura® applications that can be deployed from the central Solution Deployment Manager for Avaya Aura® Virtualized Appliance and customer Virtualized Environment. You can deploy one application at a time.

  Note:

  - System Manager must be on the same or higher release than the application you are upgrading to. For example, you must upgrade System Manager to 10.2 before you upgrade Communication Manager to 10.2.

    All the applications that are supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for the version of applications that are supported by System Manager, see Avaya Aura® Release Notes on the Avaya Support website.

  - Solution Deployment Manager Client must be on the same or higher release than the OVA you are deploying. For example, if you are deploying Communication Manager 10.2 OVA, Solution Deployment Manager Client version must be on Release 10.2 or higher. Solution Deployment Manager Client cannot be on Release 10.1.

- Configures application and networking parameters required for application deployments.
- Supports selecting the application OVA file from a local path or an HTTPS URL. You do not need access to PLDS.
- Supports changing the hypervisor network parameters, such as IP Address, Netmask, Gateway, DNS, and NTP on Appliance Virtualization Platform.
- Supports installing patches for the hypervisor on Appliance Virtualization Platform.
- Supports installing software patches, service packs, and feature packs only for System Manager.

  Note:

  To install the patch on System Manager, Solution Deployment Manager Client must be on the same or higher release as the patch. For example, if you are deploying the patch for System Manager Release 10.2, you must use Solution Deployment Manager Client Release 10.2 or higher.

  However, to install the patch on System Manager Release 10.2, Solution Deployment Manager Client must be on Release 10.2.

Avaya Aura® applications use centralized Solution Deployment Manager from System Manager to install software patches, service packs, and feature packs. For the applications

that cannot be patched from centralized Solution Deployment Manager, use the application Command Line Interface or web console.

For more information about supported releases and patching information, see Avaya Aura® Release Notes on the Avaya Support website.

- Configures Remote Syslog Profile.
- Creates the Appliance Virtualization Platform Kickstart file.
- Creates the Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1 Kickstart file.
- Supports the Pre-staging feature to prestage the System Manager OVA, service pack or feature pack, or data migration utility files to deploy, upgrade, or update the System Manager application.

Related links

Solution Deployment Manager Client on page 1316

Solution Deployment Manager

Solution Deployment Manager simplifies and automates the deployment and upgrade process.

With Solution Deployment Manager, you can deploy the following applications:

- System Manager
- Session Manager
- Branch Session Manager
- Communication Manager
- Application Enablement Services
- Avaya WebLM
- Avaya Diagnostic Server (Secure Access Link)
- Avaya Session Border Controller Release 8.0 and later
- Avaya Breeze® platform Release 3.3 and later
- Avaya Aura® Media Server

For the latest and most accurate information about other Avaya product compatibility information, go to **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

Note:

When an application is deployed on a KVM host, Solution Deployment Manager does not support that application.

With Solution Deployment Manager, you can migrate, upgrade, and update the following applications:

- Hardware-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
- Session Manager Release 7.1.3.x and later
- Communication Manager Release 7.x and later
- Branch Session Manager Release 7.x and later
- Application Enablement Services Release 7.x and later
- Avaya Breeze® platform Release 3.3 and later
- System Manager Release 7.1.3.x and later (using SDM client only)
- WebLM Release 7.x and later

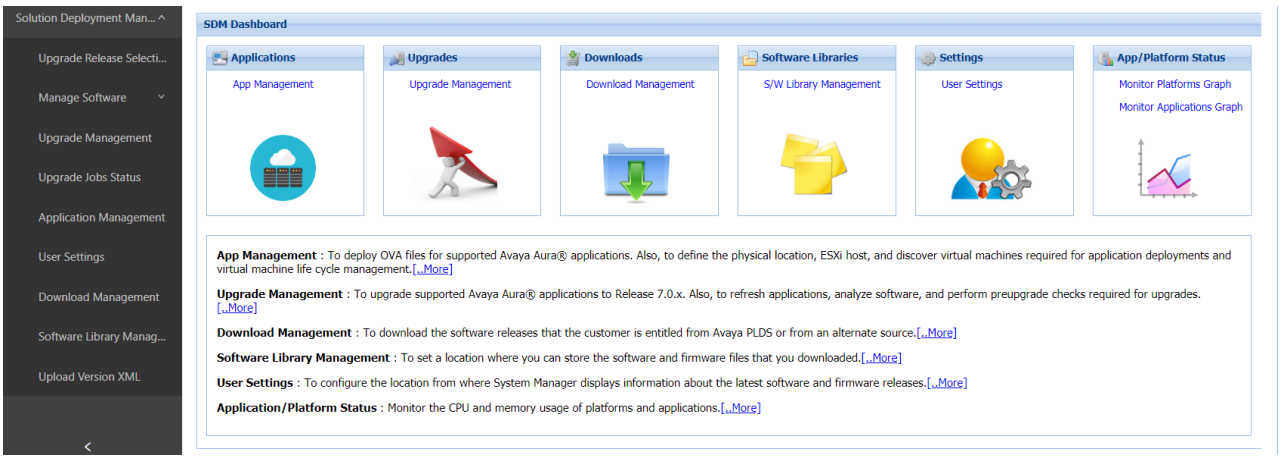
Note:

You must manually migrate the Services virtual machine that is part of the template.

The centralized deployment and upgrade process provides better support to customers who want to upgrade their systems to Avaya Aura® Release 10.2.x. The process reduces the upgrade time and error rate.

Solution Deployment Manager dashboard

You can access 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.x Onwards** or **6.3.8** as the target upgrade. **Release 7.x Onwards** is the default upgrade target.
- **Manage Software**: To analyze, download, and upgrade the IP Office, Unified Communications Module, and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.
- **Application Management**: To deploy OVA files for the supported Avaya Aura® application.
  - Configure Remote Syslog Profile.
  - Generate the Appliance Virtualization Platform Release 8.x or earlier Kickstart file.
  - Generate the platform Kickstart file for the following Appliance Virtualization Platform or Avaya Solutions Platform platforms:
    - Appliance Virtualization Platform 8.0.x
    - Appliance Virtualization Platform 8.1.x
    - Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1
- **Upgrade Management**: To upgrade Avaya Aura® applications to Release 10.2.x.
- **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.
- **Upload Version XML**: To save the `version.xml` file to System Manager. You require the application-specific `version.xml` file to perform upgrades.

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** > **User Settings**.
2. On the User Settings page, click **Edit**.
3. Select the **Use Avaya Support Site** check box, and provide the SSO username and SSO password for PLDS, and the company ID.
4. Configure the PLDS settings and proxy settings for the software download.
5. If your network configuration requires a proxy, select the **Use Proxy** check box, and provide the details.

   Note:

   If you are using a proxy server that uses certificates, add the full CA certificate chain of the identity certificate that is used to secure the proxy server into the System Manager trust store. Failure to do so will result in errors when System Manager tries to connect to the proxy server to reach out to Avaya PLDS.

   For more information about how to add a CA certificate to the System Manager trust store, see Adding trusted certificates on page 1205.
6. Click **Commit**.

Related links

Obtaining a company ID on page 1327
User Settings field descriptions on page 1331

Obtaining a company ID

Before you begin

Ensure that you have 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, click **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 PLDS website, download the `smgr-versionsxmls.zip` file.

   For more information, see “Downloading the smgr-versionsxmls.zip file from PLDS”.
3. Copy the following xml files to the `alternate-source` directory:
   - `versions.xml`
   - `versions_aams.xml`
   - `versions_aes.xml`
   - `versions_avputilities.xml`
   - `versions_bsm.xml`
   - `versions_cmm.xml`
   - `versions_compatibility.xml`
   - `versions_edp.xml`
   - `versions_msg.xml`
   - `versions_others.xml`
   - `versions_sbce.xml`
   - `versions_sp.xml`
   - `versions_systemplatform.xml`
   - `versions_avp.xml`

- `versions_us.xml`
- `versions_weblm.xml`

4. 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 Manager, Appliance Virtualization Platform, Utility Services, 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 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`.

Related links

Downloading the smgr-versionsxmls.zip file from PLDS on page 1330

Downloading the smgr-versionsxmls.zip file from PLDS

Procedure

1. Log on to the PLDS website at https://plds.avaya.com.
2. On the PLDS Home page, click **Assets** > **View Downloads**.
3. **(Optional)** On the Downloads page, in **Company Name**, do one of the following:
   - Type the company name and click **Apply Company Name**.
   - Use the find icon to search for the company name and select the company name.

   If **Company Name** is already configured, you can skip this step.
4. Click **Search by Download**.
5. In **Download pub ID**, type `SMGRSUM0001`.
6. Click **Search Downloads**.
7. In the search results, click **Download**.
8. At the prompt, save the ZIP file on your local computer.
9. Extract the ZIP file on your local computer.

Next steps

Upload one version.xml files at a time.

Related links

Establishing the connection to an alternate source on page 1328

User Settings field descriptions

Source configuration

Name	Description
Use Avaya Support site	The option to find the information and download the software releases from the Avaya Support website. **Note:** • To download the firmware and analyze the software on System Manager, you must gain access to `plds.avaya.com` `pldsxml.avaya.com`, and `downloads.dlavaya.com`. • Select the **Use Avaya Support Site** check box, to use **Avaya Support Site**. Enter the SSO user name, SSO password, and Company ID details. 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 website. You must set the alternate source. For more information, see *Setting up an alternate source*. **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://10.10.10.10/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

Name	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. **Note:** After upgrading System Manager, if the system does not auto populate the **Company ID** field, then you must manually edit the field with appropriate value after the upgrade.

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.

Name	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 website.
Confirm Password	The password of the proxy server that you retype for the Avaya Support website.

Button	Description
Edit	Displays the edit page to change the user settings.
Commit	To save the changes to the user settings.
Reset to Default	To reset the page and clear the values.
Cancel	To cancel the changes 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, 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, SMGR_DEFAULT_LOCAL, resides within System Manager post installation. You require only remote software library for upgrading IP Office. For upgrading other elements, you can use a local or remote library.

Related links

Editing a software library on page 1341
Viewing a software library on page 1341
Deleting a file from the software library on page 1346
System requirements for the external server on page 1347

Software library field descriptions on page 1342
Software Library Files field descriptions on page 1347

Enabling and disabling FTP on System Manager

About this task

You must enable FTP on System Manager only to use System Manager as a local software library for upgrading Media Gateway and Media Modules.

Note:

When the upgrade is complete, disable FTP only to re-enable when you need.

Before you begin

Start an SSH session.

Procedure

1. Log on to the System Manager web console with administrator privilege credentials.
2. To enable the FTP server, do the following:
   a. At the prompt, type `sh/opt/vsp/SDM_FTP_Patch/Setup.sh`.
   b. Type the sdmuser password and press `Enter`.

   You can now use the FTP library to save the software or firmware.
3. To disable the FTP server, type `sh/opt/vsp/SDM_FTP_Patch/Setup.sh stop`.

Configuring System Manager as local software library

About this task

Use the procedure to configure System Manager as local FTP server to save the software for Media Modules and Media Gateways for upgrades. However, you can also use the remote FTP server.

Note:

Use only remote FTP server as software library to save the TN Board firmware. You cannot use System Manager as software library.

Before you begin

Enable FTP on System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Software Library Management**.
3. Select SMGR_DEFAULT_LOCAL and click **Edit**.

   The system displays the Edit Software Library page.

4. On the Library Server Details (L) tab, in **Default Protocol**, click **FTP**.
5. Click the FTP Configuration (F) tab, and select the **Enable FTP** check box.
6. In **User Name**, type `sdmuser`.

   The system preconfigures the ftpuser name when you run the script as described in “Enabling and disabling FTP on System Manager”. You cannot change the user name.
7. In **Password** and **Confirm Password** fields, type the same password that you configured while running the script.
8. Click **Commit**.
9. In the left navigation pane, click **Download Management** and download the required Media Gateway/Media Module firmware in the SMGR_DEFAULT_LOCAL software library.

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® 7.x and later applications	• HTTP/HTTPS • FTP/SCP

Related links

Installing and configuring an HTTP server as a remote server on page 1335
Installing and configuring an FTP server as a remote server on page 1336

Installing and configuring an SCP or SFTP server as a remote server on page 1338

Installing and configuring an HTTP server as a remote server

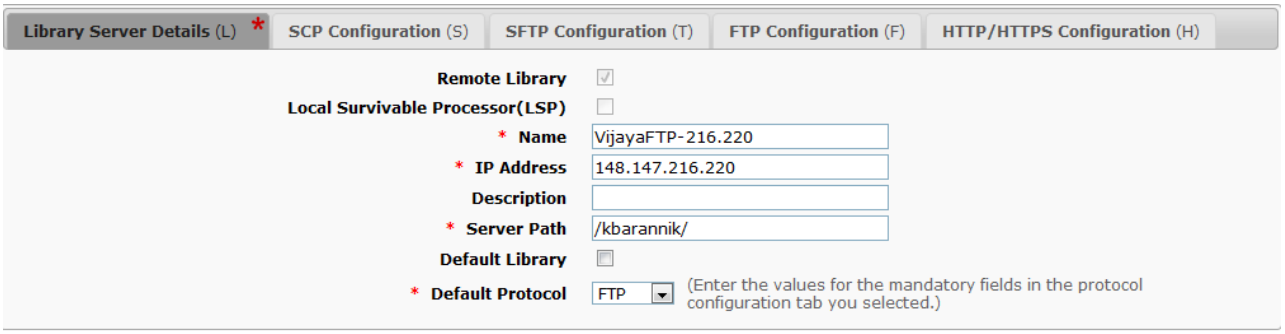
Procedure

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` .

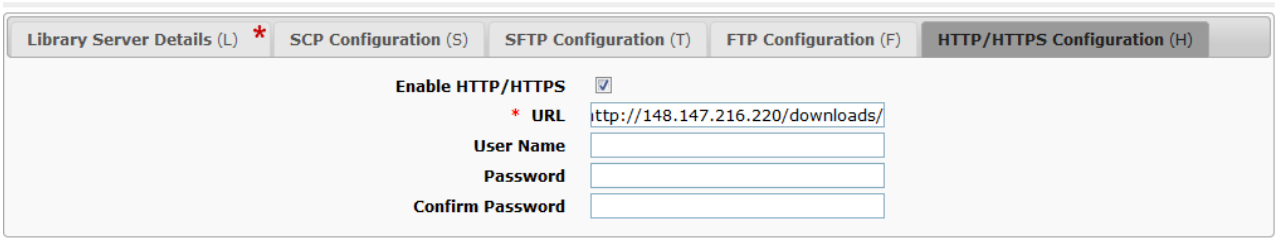
   For example, `C:\Program Files(x86)\Apache Group\Apache2\htdocs\downloads\`
6. Provide the `downloads` folder with full privileges.
7. To verify the privileges, do the following:
   a. Add a file to the `downloads` folder.
   b. Open the file from the browser.

Result

On the System Manager web console, on the Software Library Configuration page, the Library Server Details tab displays the following details:



The HTTP/HTTPS Configuration tab displays the following http/https configuration details:



Related links

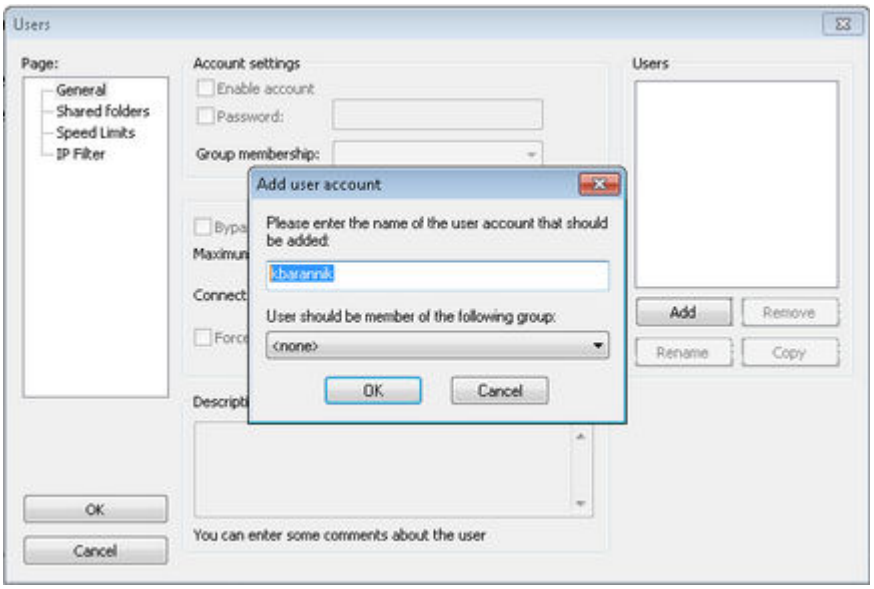
Protocol requirements to configure a remote server on page 1334

Installing and configuring an FTP server as a remote server

Procedure

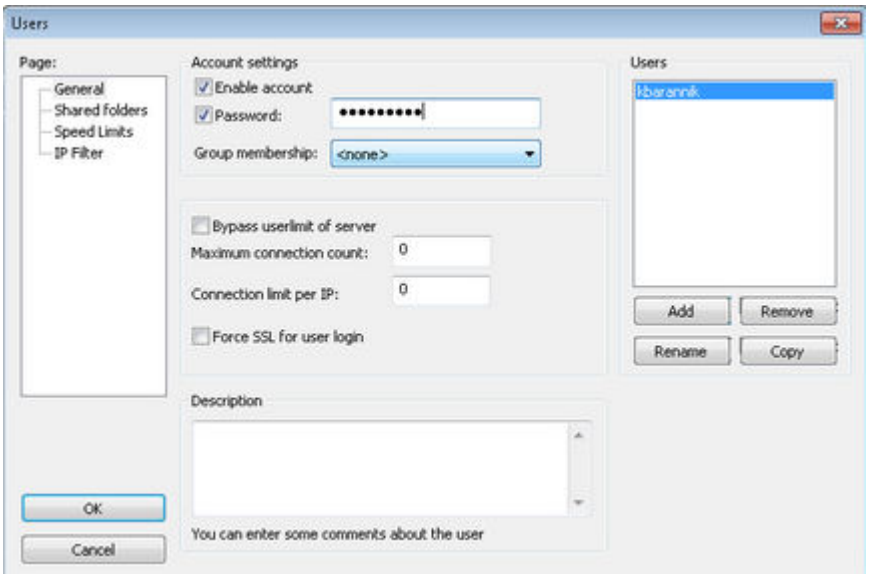
1. Run `FileZilla_Server-0_9_43.exe` as an administrator.

   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**.



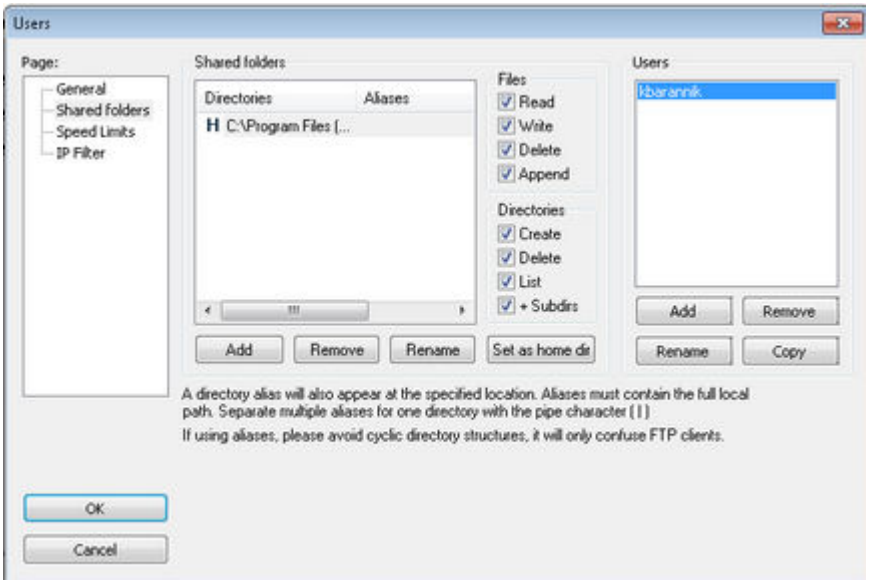
6. In the Add user account dialog box, type a user name and click **OK**.
7. Select the **Password** check box.

8. Type a password and click **OK**.



The system prompts you to provide a folder.

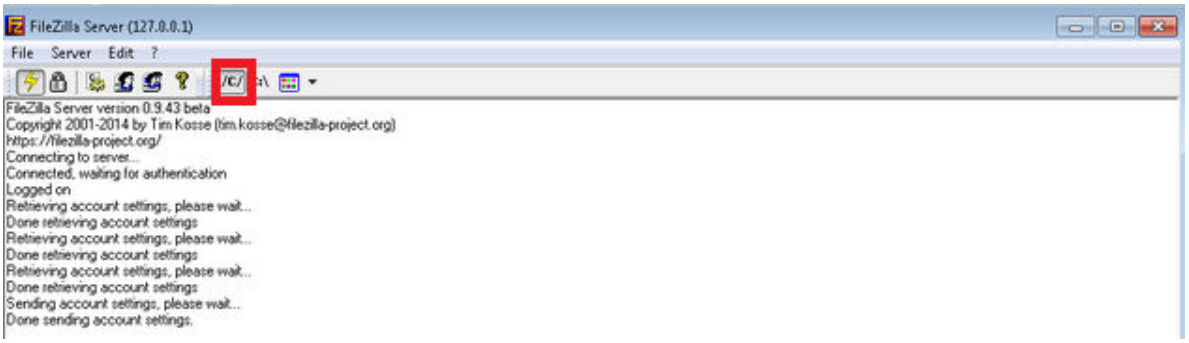
9. In the left pane, click **Shared folders**.
10. In the **Shared folders** section, click **Add** and provide the folder location till the `downloads` folder.
11. Click **OK**.
12. To provide the privileges, in the **Files** section, select the check boxes, such as **Read**, **Write**, and **Delete**.



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:

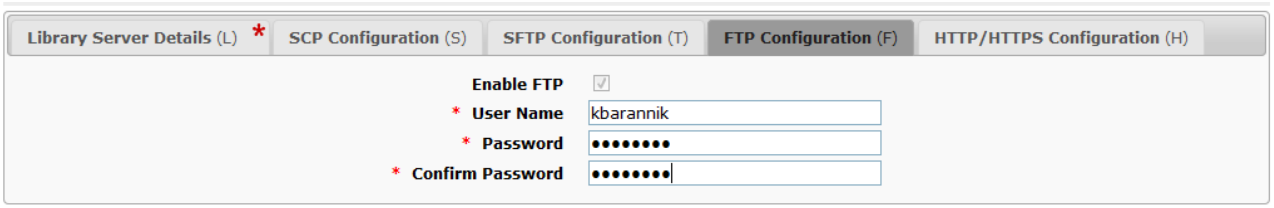
    Ensure that you select a logical file name option. By default, the system selects `/C/`.



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:



Related links

Protocol requirements to configure a remote server on page 1334

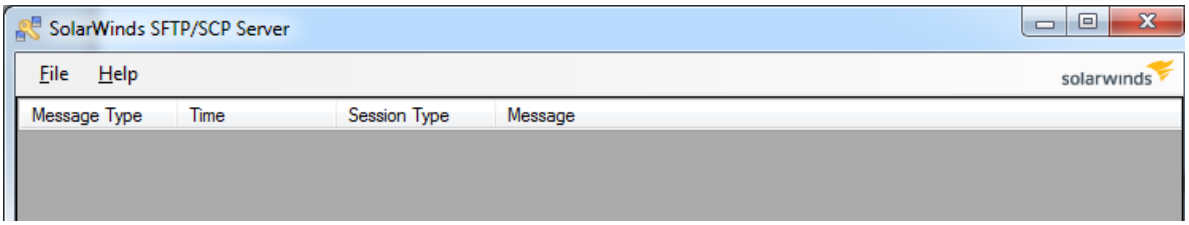
Installing and configuring an SCP or SFTP server as a remote server

Procedure

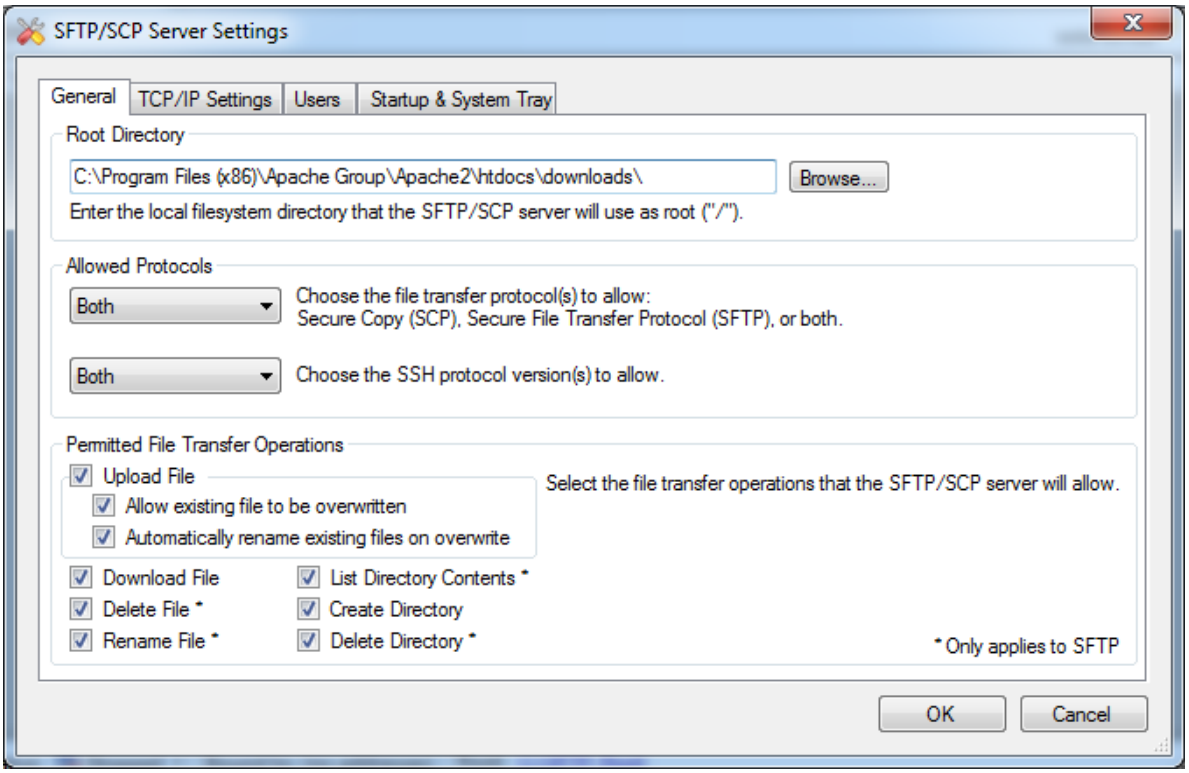
1. Run `SftpServerInstaller.msi` as administrator.

   Wait until the installation is complete.

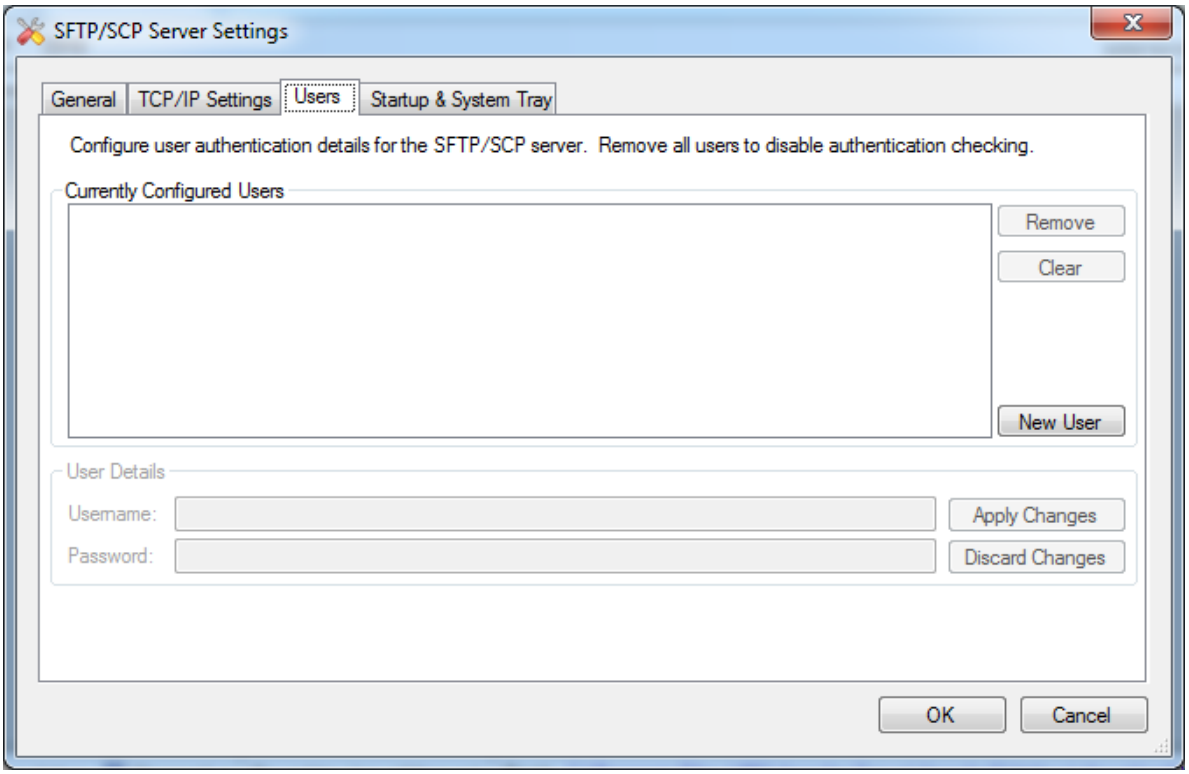
2. Open the **SolarWinds SFTP & SCP Server** server interface.



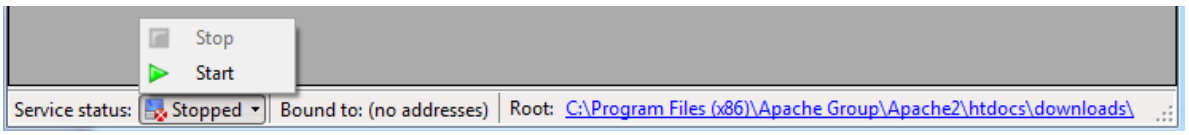
3. On the **File** menu, click **Configure**.
4. Navigate to `C:\Program Files (x86)\Apache Group\Apache2\htdocs\downloads\`.
5. Set the required parameters and click **OK**.



6. Click the Users tab.



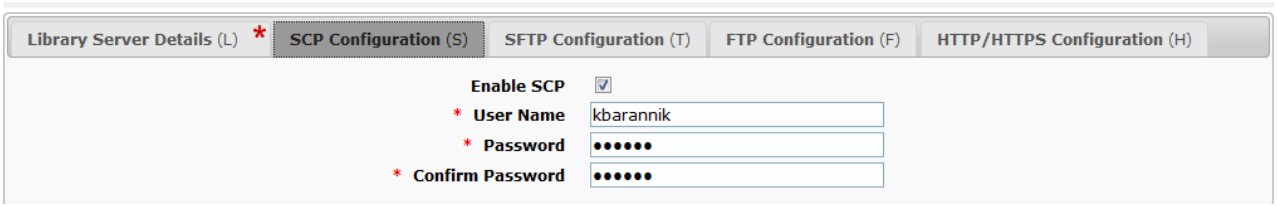
7. Click **New User**.
8. Enter the user name and the password.
9. Click **Apply Changes**.
10. Start the server.



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:



Related links

Protocol requirements to configure a remote server on page 1334

Creating a software library

About this task

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** > **Software Library Management**.
2. Click **New**.
3. Complete the Add Software Library page.
4. 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 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 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 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.

Table continues…

Name	Description
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.
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 returns 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 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.

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 Software/Hardware Types section, select the family name, and click **Show Files**.
   b. In the Select Files Download Details section, in the **Source** field, select **My Computer**.
   c. 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.
8. Provide a valid file type.

   This system uploads the OVA file from local computer to the designated software library on System Manager.

   Note:

   If the file type is invalid, System Manager displays an error.

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

- On the Download Management page, click **Refresh Families**.
- When you add or update details in the application-specific `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 navigation pane, click **Software Library Management**.
3. Click **Manage Files**.
4. On the 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 access 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:
   - **SHA256 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 exist in `versions.xml`, the system does not display the file details. Therefore, you cannot use the file for upgrade in Upgrade Management. You can use the file only for new deployment from Application Management.
6. Select the file.
7. Click **Sync**.

   In File Sync Started Message, the system displays 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 area 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 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.
SHA256 Checksum	The sha256 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 returns 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.

Table continues…

Component	Requirement	Recommendation
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.

Applications pre-upgrade functions

Refreshing elements

Before you begin

- On the User Settings page, configure the user settings.

Note:

For Branch Session Manager, Session Manager, AES, and other elements (excluding Communication Manager), the user must follow these steps in sequence to ensure that the correct options appear in the **Operation** drop-down menu on the **Upgrade Configuration** page.

1. Refreshing elements on page 1348
2. Analyzing software on page 1349
3. Performing the preupgrade check on page 1351

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the 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

About this task

Analyze works on the version of OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitle update or upgrade version, the version field must contain valid value. You can get the version values from versions files that are available on PLDS.

Custom patching does not require the analyze operation.

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 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 **Download Management**.

   The system displays the File Download Manager page.
3. 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.
4. In **Select Software/Hardware Types**, select the software or firmware that you want to download.
5. 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**.
6. Click **Show Files**.
7. 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
Source	The source from where Download Manager gets the software or firmware files. The options are: • **Avaya PLDS/Alternate Source** • **My Computer**

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 of the software or firmware file.
Job Name	The name of the download job.
Current Step	The current status.
Percentage Completed	The status of completion.
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 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, fill in the required information.

   Note:

   To upgrade to different server, in **Target Host**, select the target server host.

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.
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 Platform	The Appliance Virtualization Platform or ESXi host of the virtual machine.
Data Store	The data store. When you set the **Target Host** as **Same Box**, the system enables the **Data Store** field.
New Target Platform	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 or ESXi host from Application Management.
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.

Application management

Application management

The Application Management link from Solution Deployment Manager provides the application management capabilities that you can use to do the following.

- Defines the physical location for Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier, ESXi host, or Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0), and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Supports password change and patch installation of the Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier host. Restart, shutdown, and certificate validation of Appliance Virtualization Platform Release 8.x or earlier and ESXi hosts. Also, enables and disables SSH on the host.
- Manages lifecycle of the OVA applications that are deployed on the Avaya Aura® Appliance Virtualization Platform Release 8.x or earlier or ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.

Note:

For the Avaya Aura® Messaging element, trust re-establishment is not required.

- Deploys Avaya Aura® application OVAs on customer-provided Virtualized Environment and Avaya Aura® Virtualized Appliance environment.
- Removes the Avaya Aura® application OVAs that are deployed on a virtual machine.
- Deploys Avaya Aura® application ISOs in Software-only environment.
- 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 or ISO file on the platform by using System Manager Solution Deployment Manager or the Solution Deployment Manager client.

Managing the location

Viewing a location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click the Locations tab.

   The Locations section lists all locations.

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. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Locations** tab, in the Locations section, click **New**.
3. In the New Location section, do the following:
   a. In Required Location Information, type the location information.
   b. In Optional Location Information, type the network parameters for the virtual machine.
4. Click **Save**.

   System Manager displays the new location in the **Application Management Tree** section.

Related links

New and Edit location field descriptions on page 1355

Editing the location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Locations** 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 1355

Deleting a location

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Locations** tab, in the Locations section, select one or more locations that you want to delete.
3. Click **Delete**.
4. In the Delete confirmation dialog box, click **Yes**.

   The system does not delete the applications that are running on the platform and moves the platform to **Unknown location Platform mapping**.

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/Postal Code	The zip code of the host location.
Country	The country where the host is located.

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 subnet 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 operations, and returns to the Locations section.

Managing the platform

Adding an Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 host

About this task

Use this procedure to add an Appliance Virtualization Platform Release 8.x or earlier, ESXi, or Avaya Solutions Platform 130 Release 5.1 host. You can associate an ESXi host with an existing location.

If you add a standalone ESXi host to the System Manager Solution Deployment Manager or the Solution Deployment Manager client, add the standalone ESXi host using its FQDN.

Note:

You can add a VMware ESXi host in Solution Deployment Manager if the Standard or Enterprise VMware license is applied on the VMware ESXi host.

If the VMware vSphere Hypervisor Free License is applied on the VMware ESXi host or the VMware ESXi host is in the evaluation period, you cannot add that VMware ESXi host in Solution Deployment Manager.

Solution Deployment Manager supports the Avaya Aura® Appliance Virtualization Platform and VMware ESXi hosts. If you try to add another host, System Manager displays the following error message:

```
Retrieving host certificate info is failed: Unable to communicate with
host. Connection timed out: connect. Solution Deployment Manager only
```

```
supports host management of VMware-based hosts and Avaya Appliance
Virtualization Platform (AVP).
```

Solution Deployment Manager 10.2.1 does not support ASP 130/S8300 R6.0.x (KVM on RHEL 8.10). You can add Avaya Solutions Platform 130 Release 5.0 (Avaya Supplied ESXi) similar to VMware ESXi host.

Note:

- To add an Appliance Virtualization Platform host, ensure that you accept the AVP EULA before you add the host to the SDM inventory.
- To add an ESXi host in Solution Deployment Manager, set the vmk0 interface as the IP Address of the ESXi host. Otherwise, Solution Deployment Manager does not support adding the ESXi host in Solution Deployment Manager.
- To add an Avaya Solutions Platform host, ensure that you use the FQDN. Do not use the IP address to add an Avaya Solutions Platform host.

Before you begin

Add a location.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
   a. Provide details such as the platform name, platform FQDN or IP address, username, and password.

      For Appliance Virtualization Platform and VMware ESXi deployment, you can also provide the root username.

   b. In **Platform Type**, select **AVP/ESXi**.
   c. Set the Platform IP address of Appliance Virtualization Platform to 192.168.13.6, if you are connected through the services port.
5. Click **Save**.
6. In the Certificate dialog box, click **Accept Certificate**.

   System Manager generates the certificate and adds the Appliance Virtualization Platform host. For the ESXi host, you can accept the certificate. If the certificate is invalid, Solution Deployment Manager displays the error. To generate the certificate, see the VMware documentation.

   In the Application Management Tree section, System Manager displays the new host in the specified location and discovers applications.

7. To view the discovered application details, such as name and version, do the following to establish trust between the application and System Manager:
   a. On the **Applications** tab, in the Applications for Selected Location <location name> section, select the required application.
   b. Click **More Actions** > **Re-establish connection**.

      For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
   c. Click **More Actions** > **Refresh App**.

   Important:

   To change the IP address or FQDN of the Appliance Virtualization Platform host from the local inventory, you require AVP Utilities. To get the AVP Utilities application name during the IP address or FQDN change, refresh AVP Utilities to ensure it is available.
8. On the **Platforms** tab, select the required platform and click **Refresh Host**.

Next steps

After adding a new host under Application Management Tree, the **Refresh Platform** operation might fail to add the virtual machine entry under **Manage Element** > **Inventory**. This is due to the absence of the **Application Name** and **Application Version** for the virtual machines discovered as part of the host addition. After adding the host, do the following:

1. In Application Management Tree, establish trust for all the virtual machines deployed on the host.
2. Ensure that System Manager populates the **Application Name** and **Application Version** for each virtual machine.

Related links

Add and Edit platform field descriptions on page 1364

Adding an Avaya Solutions Platform S8300 Release host

About this task

This procedure is required for both preloaded or prelicensed Avaya Solutions Platform S8300 and fresh install on Avaya Solutions Platform S8300.

Use this procedure to add an Avaya Solutions Platform S8300 Release 5.1.x host. You can associate an Avaya Solutions Platform S8300 Release 5.1.x and later host with an existing location.

Note:

Select **ASP 130/S8300** in **Platform Type** on the Platforms tab to add an Avaya Solutions Platform S8300 Release 5.1 (Avaya Supplied ESXi 7.0) host in the SDM Application Management.

Before you begin

- If Appliance Virtualization Platform that was migrated to Avaya Solutions Platform S8300 Release 5.1.x is available in Solution Deployment Manager on the **Platforms** tab, remove

that Appliance Virtualization Platform and add the Avaya Solutions Platform S8300 Release 5.1.x host.

- Regenerate the self-signed certificate using the FQDN.

  See "Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface".

- If you are connected to the Avaya Solutions Platform S8300 host through the services port using the SDM client, perform the following:
  1. Edit the `C:\Windows\System32\Drivers\etc\hosts` file in your laptop to add the IP Address and FQDN of the host.
  2. Add the host in the format 192.11.13.6 *<changed FQDNname>*

     For example: `192.11.13.6 esxihost6.hostdomain.com`

- Add Avaya Solutions Platform S8300 host to an existing location or associate it with a new location.
- Install a valid license file on the Avaya Solutions Platform S8300 host.

Procedure

1. To add an Avaya Solutions Platform S8300 host using System Manager SDM or SDM client, choose one of the following:
   - For System Manager SDM, on the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
   - For SDM client, on the **SDM Client** web console, click **Application Management**.
2. In **Application Management Tree**, select an existing location or add a new location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
   a. Provide details of Platform name, Platform FQDN, username, and password.

      For Avaya Solutions Platform S8300 deployment, you can also provide the root username.

   b. In **Platform Type**, select **ASP 130/S8300**.
5. Click **Save**.

   The Avaya Solutions Platform S8300 certificate is updated based on the platform FQDN.

After adding an Avaya Solutions Platform S8300 host using System Manager SDM or SDM client, perform the following:

6. Deploy the required virtual machines.
7. In the Certificate dialog box, click **Accept Certificate**.

   System Manager generates the certificate and adds the Avaya Solutions Platform S8300 host.

In the **Application Management Tree**, System Manager displays the new host in the specified location and discovers applications.

8. To view the discovered application details, such as name and version, establish trust between the application and System Manager doing the following:
   a. On the **Applications** tab, in the Applications for Selected Location <location name> section, select the required application.
   b. Click **More Actions** > **Re-establish connection**.

      See “Re-establishing trust for Solution Deployment Manager elements”.
   c. Click **More Actions** > **Refresh App**.
9. On the **Platforms** tab, select the required platform and click **Refresh**.

Next steps

After adding a new host under Application Management Tree, the **Refresh Platform** operation might fail to add the virtual machine entry under **Manage Element** > **Inventory**. This is due to the absence of **Application Name** and **Application Version** for the virtual machines discovered as part of the host addition. After adding the host, do the following:

1. In Application Management Tree, establish trust for all the virtual machines deployed on the host.
2. Ensure that System Manager populates the **Application Name** and **Application Version** for each virtual machine.

Related links

Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface on page 1395

Re-establishing trust for Solution Deployment Manager elements on page 1400

Adding an Avaya Solutions Platform 130 Release 5.1 host

About this task

Use this procedure to add an Avaya Solutions Platform 130 Release 5.1 host. You can associate an Avaya Solutions Platform 130 Release 5.1 host with an existing location.

Before you begin

- If you are connected to the Avaya Solutions Platform 130 host through the services port using the SDM client, perform the following:
  1. Edit the `C:\Windows\System32\Drivers\etc\hosts` file in your laptop to add the IP Address and FQDN of the host.
  2. Add the host in the format 192.11.13.6 *<changed FQDNname>*

     For example: `192.11.13.6 esxihost6.hostdomain.com`
- If Appliance Virtualization Platform that was migrated to Avaya Solutions Platform 130 Release 5.1 is available in Solution Deployment Manager on the **Platforms** tab, remove that Appliance Virtualization Platform and then add the Avaya Solutions Platform 130 Release 5.1 host.

- Regenerate the self-signed certificate using the FQDN.

  See "Regenerating Avaya Solutions Platform 130 self-signed certificate with FQDN using the command line interface".
- Add Avaya Solutions Platform 130 host to an existing location or associate it with a new location.
- Install a valid license file on the Avaya Solutions Platform 130 Release 5.1 host.

Procedure

1. To add an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, choose one of the following:
   - For System Manager SDM, on the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
   - For SDM client, on the **SDM Client** web console, click **Application Management**.
2. In **Application Management Tree**, select an existing location or add a new location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
   a. Provide details of Platform name, Platform FQDN, username, and password.

      For Avaya Solutions Platform 130 deployment, you can also provide the root username.

   b. In **Platform Type**, select **ASP 130/S8300**.
5. Click **Save**.

   The Avaya Solutions Platform 130 certificate is updated based on the platform FQDN.

After adding an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, perform the following:

6. Deploy the required virtual machines.
7. In the Certificate dialog box, click **Accept Certificate**.

   System Manager generates the certificate and adds the Avaya Solutions Platform 130 host.

   In the **Application Management Tree**, System Manager displays the new host in the specified location and discovers applications.
8. To view the discovered application details, such as name and version, establish trust between the application and System Manager doing the following:
   a. On the **Applications** tab, in the Applications for Selected Location <location name> section, select the required application.
   b. Click **More Actions** > **Re-establish connection**.

      See “Re-establishing trust for Solution Deployment Manager elements”.

c. Click **More Actions** > **Refresh App**.

9. On the **Platforms** tab, select the required platform and click **Refresh**.

Next steps

After adding a new host under Application Management Tree, the **Refresh Platform** operation might fail to add the virtual machine entry under **Manage Element** > **Inventory**. This is due to the absence of **Application Name** and **Application Version** for the virtual machines discovered as part of the host addition. After adding the host, do the following:

1. In Application Management Tree, establish trust for all the virtual machines deployed on the host.
2. Ensure that the system populates **Application Name** and **Application Version** for each virtual machine.

Adding a software-only platform

About this task

Use this procedure to add an operating system to Solution Deployment Manager. In Release 10.2.x, System Manager supports the Red Hat Enterprise Linux (RHEL) 8.4, or RHEL 8.10 (64-bit) operating system.

Before you begin

Add a location.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Platforms** tab, click **Add**.
3. In **Platform Name**, type the name of the platform.
4. In **Platform FQDN or IP**, type the FQDN or IP address of the base operating system.
5. In **User Name**, type the username of the base operating system.

   For a software-only deployment, the username must have the permission to log in through SSH. If the software-only application is already deployed, provide the application CLI user credentials.
6. In **Password**, type the password of the base operating system.
7. In **Platform Type**, select **OS**.
8. Click **Save**.

   Any other application running on the platform is automatically discovered and displayed in the **Applications** tab.

   - If the Solution Deployment Manager cannot establish trust, the application is displayed as Unknown.

- If you add the OS, only **Add** and **Remove** operations are available on the **Platforms** tab. **New** option is enabled on the **Applications** tab. If the application is System Manager, **Update App** is enabled on Solution Deployment Manager Client.

System Manager displays the added base operating system on the **Platforms** tab.

Editing a platform

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select a platform that you want to update.
4. Change the platform information.
5. Click **Save**.

   The system updates the platform information.

Related links

Add and Edit platform field descriptions on page 1364

Refreshing a platform

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Platforms** tab, do the following:
   a. In the Platforms for Selected Location <location name> section, select one or more platforms.
   b. Click **Refresh Host**.
      - If you select less than five platforms, Solution Deployment Manager refreshes the selected platforms and displays the status in the **Current Action** column.
      - If you select more than five platforms, Solution Deployment Manager displays the following message:

        ```
        Refresh Host takes a few minutes for each host. Once started,
        this action cannot be cancelled. Do you want to proceed with
        Refresh for the <number of selected hosts> selected hosts?
        ```

        To proceed with the refresh platform action of more than five platforms, click **Yes**.

        Solution Deployment Manager refreshes the platforms and displays the status in the **Current Action** column.

Add and Edit platform field descriptions

Name	Description
Location	The location where the platform is available. The field is read-only.
Platform Name	The platform name of OS, Appliance Virtualization Platform, ESXi, Avaya Solutions Platform 130, or Avaya Solutions Platform S8300.
Platform FQDN or IP	The IP address or FQDN of the platform. **Note:** To add Avaya Solutions Platform, use the FQDN only. Do not use the IP address to add Avaya Solutions Platform.
User Name	The user name to log in to the platform. **Note:** For Appliance Virtualization Platform, provide the admin credentials you configure when generating the Kickstart file.
Password	The password to log in to the platform.
Platform Type	The options are the following: • **OS**: For Red Hat Enterprise Linux. • **AVP/ESXi**: For Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 Release 5.0. You can add Avaya Solutions Platform 130 Release 5.0 as a standalone ESXi. • **ASP 130/S8300**: For Avaya Solutions Platform 130 Release 5.1 and Avaya Solutions Platform S8300 Release 5.1 hosts. Do not select this option to add Avaya Solutions Platform 130 Release 5.0.

Button	Description
Save	Saves the host information and returns to the Platforms for Selected Location <location name> section.

Removing a platform

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select one or more platforms that you want to delete.
3. Click **Remove**.
4. On the Delete page, click **Yes**.

Generating the Avaya Solutions Platform S8300 kickstart file

About this task

This procedure is not required for preloaded or prelicensed Avaya Solutions Platform S8300.

Generate the kickstart file for the fresh installation of Avaya Solutions Platform S8300.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Kickstart Generation**.
3. On Create AVP/ASP Kickstart, select **ASP S8300 5.1**.
4. In Generate Kickstart for, select **Fresh Installation**.
5. Enter the appropriate information in the fields.

   For information, see “Create ASP S8300 Kickstart field descriptions”.
6. Click **Generate Kickstart File**.

   Solution Deployment Manager prompts you to save the generated kickstart file on your local computer.

   For Avaya Solutions Platform S8300 Release 5.1 and later, the kickstart file name must be `aspks.cfg` and the contents of the generated aspks.cfg file must never be manually edited or modified.

Related links

Create ASP Kickstart field descriptions on page 1365

Create ASP Kickstart field descriptions

This section is not required for preloaded or prelicensed Avaya Solutions Platform S8300.

Name	Description
Choose AVP/ASP Version	The field to select the Avaya Solutions Platform S8300 host. For Avaya Solutions Platform S8300, the option is **ASP S8300 5.1**.
Generate Kickstart for	The field to select the option for generating the Avaya Solutions Platform S8300 kickstart file. Use the **Fresh Installation** option to generate the kickstart file for installing Avaya Solutions Platform S8300 Release 5.1 and later. **Note:** Do not use the **Upgrade** option, it is for future use only.
ASP Management IPv4 Address	The IPv4 address is used to access Avaya Solutions Platform S8300 through SSH.
ASP IPv4 Netmask	The IPv4 subnet mask for the Avaya Solutions Platform S8300 host.

Table continues…

Name	Description
ASP Gateway IPv4 Address	The IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
ASP Hostname	The hostname for the Avaya Solutions Platform S8300 host. The hostname: • Can contain alphanumeric characters and hyphen • Can start with an alphabetic or numeric character • Must contain at least 1 alphabetic character • Must end in an alphanumeric character • Must contain 1 to 63 characters
Main IPv4 DNS Server	The DNS Server IPv4 address for the Avaya Solutions Platform S8300 host.

Button	Description
Generate Kickstart File	Generates the Avaya Solutions Platform S8300 kickstart file and prompts you to save the file on your local computer.

Note:

FQDN is used to add host to SDM.

Related links

Generating the Avaya Solutions Platform S8300 kickstart file on page 1365

Enabling and disabling SSH on Avaya Solutions Platform S8300 Release 5.1.x from Solution Deployment Manager

About this task

This procedure is applicable to both preloaded/prelicensed Avaya Solutions Platform S8300 and fresh install on Avaya Solutions Platform S8300.

Use this procedure to enable SSH on Avaya Solutions Platform S8300 Release 5.1.x from Solution Deployment Manager.

Note:

After installing Avaya Solutions Platform S8300, SSH is enabled automatically. The only time this procedure is necessary is if the ASP SSH enable/disable shell script is executed or if SSH is disabled manually from the ESXi embedded host client or via Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.

3. Select the required host.
4. To enable SSH, do the following:
   a. Click **More Actions** > **SSH** > **Enable SSH**.
   b. In the Confirm dialog box, in **Time (in minutes)**, type the time after which the system times out the SSH connection.

      The range is 10 minutes through 120 minutes.
   c. Click **Ok**.

      Solution Deployment Manager displays `enabled` in the **SSH status** column.
5. To disable SSH, click **More Actions** > **SSH** > **Disable SSH**.

   Solution Deployment Manager displays `disabled` in the **SSH status** column.

ASP_SSH script

If a customer disables SSH for security reasons, use the **`ASP_SSH`** script to enable SSH for troubleshooting.

The following applications support the **`ASP_SSH`** script:

- Communication Manager
- Session Manager
- System Manager
- Application Enablement Services
- Avaya Session Border Controller
- Avaya Diagnostic Server (Secure Access Link)
- Avaya Aura® Device Services
- Avaya Aura® Web Gateway
- Avaya Experience Portal

Enabling SSH and viewing SSH status on Avaya Solutions Platform 130 Release 5.1 from the application CLI

About this task

Use this procedure to enable SSH and to check the SSH status of the Avaya Solutions Platform 130 Release 5.1 host.

Note:

- By default, the SSH is enabled on ASP without a timeout value.
- If **`ASP_SSH`** is run by mistake on a setup with SSH enabled while installation or migration, the script overrides the timeout value, and SSH is disabled after 2 hours window.

Before you begin

- The application must be deployed on the Avaya Solutions Platform 130 Release 5.1 host.
- Start an SSH session.
- Log in to the application command-line interface with administrator privilege CLI user credentials.

Procedure

1. To enable SSH, type **`ASP_SSH`** `enable` and press `Enter`.

   After the script is successfully run, wait for 3 minutes before trying to SSH to ASP.

   The SSH is enabled for 120 minutes.

   By default, the system automatically disables the SSH and blocks any new SSH connections after 120 minutes.

   The system enables the SSH on the Avaya Solutions Platform 130 Release 5.1 host.

2. To view the status of SSH, type **`ASP_SSH`** `status` and press `Enter`.

   If SSH is enabled, the system displays the following:

   ```
   An ASP SSH status is currently:
   active
   ```

   If SSH is disabled, the system displays the following:

   ```
   An ASP SSH status is currently:
   inactive
   ```

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 Platform mapping**. You can configure the location of an ESXi host again.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the left navigation pane, click the **Unknown location Platform 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 and click **Update**.
5. Select the host(s) where location is updated and click **Submit**.

   The system displays the ESXi host in the selected location.

Operations on Appliance Virtualization Platform

Generating the Appliance Virtualization Platform kickstart file

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Kickstart Generation**.
3. On Create AVP/ASP Kickstart, do the following:
   a. Select **AVP 8.1.x**.
   b. Enter the appropriate information in the fields.
   c. Click **Generate Kickstart File**.

   For more information, see “Create AVP Kickstart field descriptions.”

   The system prompts you to save the generated kickstart file on your local computer.

   For Appliance Virtualization Platform Release 8.1.x, the kickstart file name must be `avp81ks.cfg`.

Related links

Create AVP Kickstart field descriptions on page 1369

Create AVP Kickstart field descriptions

Name	Description
Choose AVP Version	The field to select the release version of Appliance Virtualization Platform.
Dual Stack Setup (with IPv4 and IPv6)	Enables or disables the fields to provide the IPv6 addresses. The options are: • **yes**: To enable the IPv6 format. • **no**: To disable the IPv6 format.
AVP Management IPv4 Address	IPv4 address for the Appliance Virtualization Platform host.
AVP IPv4 Netmask	IPv4 subnet mask for the Appliance Virtualization Platform host.
AVP Gateway IPv4 Address	IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.

Table continues…

Name	Description
AVP Hostname	Hostname for the Appliance Virtualization Platform host. The hostname: • Can contain alphanumeric characters and hyphen • Can start with an alphabetic or numeric character • Must contain at least 1 alphabetic character • Must end in an alphanumeric character • Must contain 1 to 63 characters
AVP Domain	Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the default value. Format is alphanumeric string dot separated. For example, mydomain.com.
IPv4 NTP server	IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com
Secondary IPv4 NTP Server	Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.
Main IPv4 DNS Server	Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.
Secondary IPv4 DNS server	Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.
AVP management IPv6 address	IPv6 address for the Appliance Virtualization Platform host.
AVP IPv6 prefix length	IPv6 subnet mask for the Appliance Virtualization Platform host.
AVP gateway IPv6 address	IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
IPv6 NTP server	IPv6 address or FQDN of customer NTP server.
Secondary IPv6 NTP server	Secondary IPv6 address or FQDN of customer NTP server.
Main IPv6 DNS server	Main IPv6 address of customer DNS server. One DNS server entry in each line.
Secondary IPv6 DNS server	Secondary IPv6 address of customer DNS server. One DNS server entry in each line.
Public vLAN ID (Used on S8300E only)	VLAN ID for the S8300E server. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use **Public VLAN ID** only on the S8300E server.

Table continues…

Name	Description
Out of Band Management Setup	The check box to enable or disable Out of Band Management for Appliance Virtualization Platform. If selected the management port connects to eth2 of the server, and applications can deploy in the Out of Band Management mode. The options are: • **yes**: To enable Out of Band Management The management port is connected to eth2 of the server, and applications can deploy in the Out of Band Management mode. • **no**: To disable Out of Band Management. The default option.
OOBM vLAN ID (Used on S8300E only)	• For S8300E, use the front plate port for Out of Band Management • For common server, use eth2 for Out of Band Management.
AVP Super User Admin Password	Admin password for Appliance Virtualization Platform. The password must contain at least 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.
Confirm Password	Admin password for Appliance Virtualization Platform.
Enable Stricter Password (14 char pass length)	The check box to enable or disable the stricter password. The password must contain at least 14 characters.
Validity in Days (Used on AVP Certificate)	The number of days for the Appliance Virtualization Platform certificate validation. The maximum limit for the certificate validation is 825 days. You can configure from 1 through 825 days.
WebLM IP/FQDN	The IP Address or FQDN of WebLM Server.
WebLM Port Number	The port number of WebLM Server. The default port is 52233.

Button	Description
Generate Kickstart File	Generates the Appliance Virtualization Platform kickstart file and the system prompts you to save the file on your local computer.

Related links

Generating the Appliance Virtualization Platform kickstart file on page 1369

Changing the network parameters for an Appliance Virtualization Platform 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 connect to Appliance Virtualization Platform through the public management interface, you might lose connection during the process. Therefore, after the IP address changes, close Solution Deployment Manager and restart Solution Deployment Manager by using the new IP address.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select an Appliance Virtualization Platform host and click **Change Network Params** > **Change Host IP Settings**.
4. In the Host Network/ IP Settings section, change the IP address, subnet mask, and other parameters as appropriate.

   Note:

   An Avaya Aura® Appliance Virtualization Platform host and all virtual machines running on the host must be on the same subnet mask.

   If Out of Band Management is configured in an Avaya Aura® Appliance Virtualization Platform deployment, you need two subnet masks, one for each of the following:

   - Public or signaling traffic, Avaya Aura® Appliance Virtualization Platform, and all virtual machines public traffic.
   - Management, Avaya Aura® Appliance Virtualization Platform, and all virtual machine management ports.
5. To change the gateway IP address, do the following:
   a. Click **Change Gateway**.

      The **Gateway** field becomes available for providing the IP address.

   b. In **Gateway**, change the IP address.

   c. Click **Save Gateway**.
6. Click **Save**.

   The system updates the Appliance Virtualization Platform host information.

Related links

Change Network Parameters field descriptions on page 1376

Changing the network settings for an Appliance Virtualization Platform host from Solution Deployment Manager

About this task

With Appliance Virtualization Platform, you can team NICs together to provide a backup connection when the server NIC or the Ethernet switch fails. You can also perform NIC teaming from the command line on Appliance Virtualization Platform.

Appliance Virtualization Platform supports Active-Standby and Active-Active modes of NIC teaming. For more information, see “NIC teaming modes”.

Note:

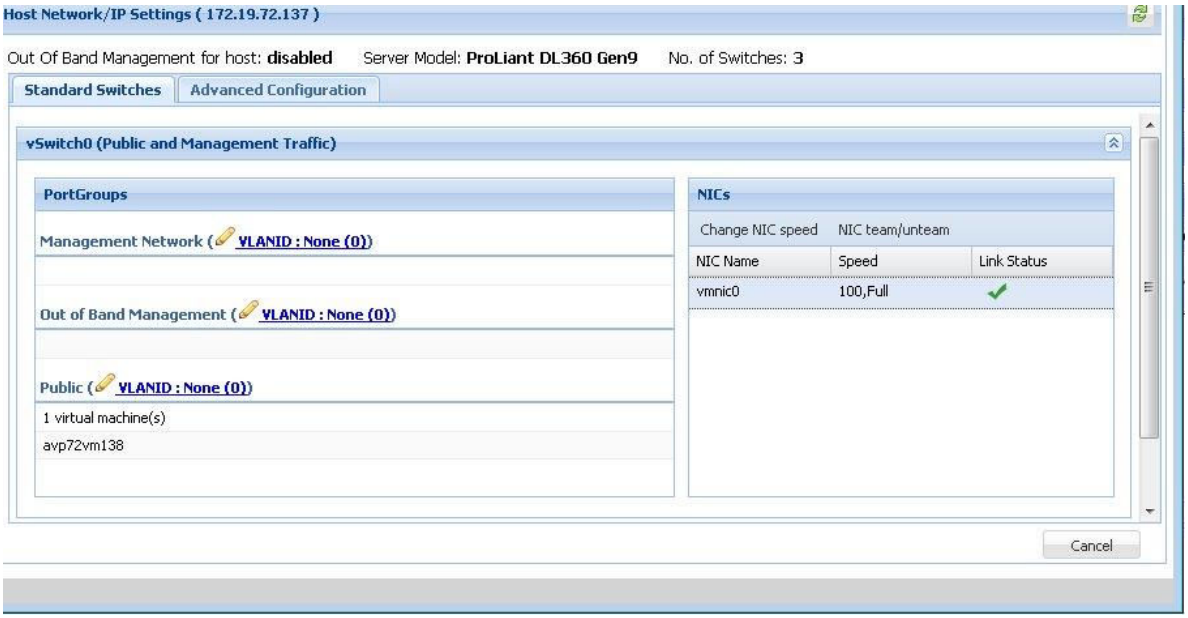
- If you add a host with service port IP address in Solution Deployment Manager and change the IP address of the host to the public IP address by using Host Network/ IP Settings, the system updates the public IP address in the database. Any further operations that you perform on the host fail because the public IP address cannot be reached with the service port. To avoid this error, edit the host with the service port IP address again.
- If FQDN of the Appliance Virtualization Platform host is updated by using Host Network/IP setting for domain name, refresh the host so that the FQDN changes reflect in Solution Deployment Manager.

Use this procedure to change network settings, such as changing VLAN ID, NIC speed, and manage NIC team for an Appliance Virtualization Platform host.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.

4. Click **Change Network params** > **Change Network Settings**.



The Host Network/ IP Settings page displays the number of switches as 4.

You can configure port groups for the following switches:

- **vSwitch0**, reserved for the Public and Management traffic.
- **vSwitch1**, reserved for services port. You cannot change the values.
- **vSwitch2**, reserved for Out of Band Management.
- **vSwitch3**. No reservations.
- **vSwitch4**. No reservations.
- **vSwitch5**. No reservations.

5. To change VLAN ID, click **Standard Switches**, and perform the following:

   a. Expand the vSwitch<n> section by clicking the downward arrow .

      The section displays the vSwitch details.

   b. Click on the VLANID link or the edit icon ( ).

      The system displays the Port Group Properties page where you can edit the VLAN ID port group property.

   c. In **VLAN ID**, select an ID.

      For more information about the value, see NIC teaming.

   d. Click **OK**.

The system displays the new VLAN ID.

6. To change the NIC speed, click **Standard Switches**, and perform the following:
   a. Ensure that the system displays a vmnic in the **NIC Name** column.
   b. Click **Change NIC speed**.

      The system displays the selected vmnic dialog box.
   c. In **Configured speed, Duplex**, click a value.
   d. Click **OK**.

      For more information, see VLAN ID assignment.

   The system displays the updated NIC speed in the **Speed** column.

   If the NIC is connected, the system displays a check mark ✔ in **Link Status**.

   Note:

   You can change the speed only for common servers. You cannot change the speed for the S8300E server.
7. To change the NIC teaming, click **Standard Switches**, and perform the following:
   a. Select a vmnic.
   b. Click **NIC team/unteam**.

      The system displays the Out of Band Management Properties page.
   c. To perform NIC teaming or unteaming, select the vmnic, and click **Move Up** or **Move Down** to move the vmnic from **Active Adapters**, **Standby Adapters**, or **Unused Adapters**.

      For more information, see “NIC teaming modes”.
   d. Click **OK**.

      The vmnic teams or unteams with **Active Adapters**, **Standby Adapters**, or **Unused Adapters** as required.
   e. To check the status of the vmnic, click **NIC team/unteam**.
8. To get the latest data on the host network IP settings, click **Refresh**.

   The system displays the current status of the vmnic.

   Note:

   You cannot perform NIC teaming for the S8300E server.

Related links

Host Network / IP Settings field descriptions on page 1376

Change Network Parameters field descriptions

Network Parameters

Name	Description
Name	The name of the Appliance Virtualization Platform host. The field is display-only.
IPv4	The IPv4 address of the Appliance Virtualization Platform host.
Subnet Mask	The subnet mask of the Appliance Virtualization Platform host.
IPv6	The IPv6 address of the Appliance Virtualization Platform host (if any).
Host Name	The host name of the Appliance Virtualization Platform host
Domain Name	The domain name of the Appliance Virtualization Platform host
Preferred DNS Server	The preferred DNS server
Alternate DNS Server	The alternate DNS server
NTP Server1 IP/FQDN	The NTP Server1 IP address of the Appliance Virtualization Platform host.
NTP Server2 IP/FQDN	The NTP Server2 IP address of the Appliance Virtualization Platform host.
IPv4 Gateway	The gateway IPv4 address. The field is available only when you click **Change IPv4 Gateway**.
IPv6 Default Gateway	The default gateway IPv6 address (if any). The field is available only when IPv6 has been configured for the system. The user, also needs to click **Change IPv6 Gateway**.

Button	Description
Change IPv4 Gateway	Makes the **IPv4 Gateway** field available, and displays **Save IPv4 Gateway** and **Cancel IPv4 Gateway Change** buttons.
Change IPv6 Gateway	Makes the **IPv6 Default Gateway** field available, and displays **Save IPv6 Default Gateway** and **Cancel IPv6 Default Gateway Change** buttons.
Save IPv4 Gateway	Saves the gateway IPv4 address value that you provide.
Cancel IPv4 Gateway Change	Cancels the changes made to the IPv4 gateway.
Save IPv6 Default Gateway	Saves the default IPv6 gateway address value that you provide.
Cancel IPv6 Default Gateway Change	Cancels the changes made to the IPv6 default gateway.

Button	Description
Save	Saves the changes that you made to network parameters.

Host Network / IP Settings field descriptions

Standard Switches

vSwitch <n> displays the PortGroups and NICs sections.

PortGroups

Name	Description
or **VLAN ID** link	Displays the Port Group Properties page where you configure VLAN ID.
VLAN ID	Displays the VLAN ID. The options are: • **None (0)** • **1 to 4093** The field displays only unused IDs.

Button	Description
OK	Saves the changes.
Cancel	Returns to the **Platforms** tab.

NICs

Name	Description
NIC Name	Displays the name of the NIC. For example, vmnic0.
Speed	Displays the speed of the NIC. For example, 100,Full.
Link Status	Displays the status of the NIC.

Button	Description
Change NIC speed	Displays the vmnic<n> dialog box.
NIC team/unteam	Displays the Out of Band Management Properties vSwitch<n> dialog box.

NIC speed

Name	Description
Configured speed, Duplex	Displays the NIC speed. The options are: • **Autonegotiate** • **10,Half** • **10,Full** • **100,Half** • **100,Full** • **1000,Full**

Button	Description
OK	Saves the changes.

NIC teaming

Button	Description
Move Up	Moves the VMNIC from unused adapters to standby or active adapters or from standby to active adapter.
Move Down	Moves the VMNIC from active to standby adapter or from standby to unused adapter.
Refresh	Refreshes the page.
OK	Saves the changes.

Advanced Configuration

Displays the Unused PortGroups section.

Name	Description
Port Group	Displays the port group.
Virtual Switch	Displays the virtual switch.

Button	Description
Delete	Deletes the selected port group.
Cancel	Returns to the **Platforms** tab.

Deleting the unused port

About this task

Use this procedure to delete the unused port of Solution Deployment Manager that is no longer used by applications that are deployed on an Appliance Virtualization Platform host.

For example, you can delete the unused port, if an application is deleted from the Appliance Virtualization Platform host, and the system still has those ports available on the Appliance Virtualization Platform host.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **Change Network params** > **Change Network Settings**.
5. Click **Advanced Configuration**.
6. In the Unused PortGroups section, select the portgroup.
7. Click **Delete**.

Changing the password for an Appliance Virtualization Platform host

About this task

Use this procedure to change the password for the Appliance Virtualization Platform host. This is the password for the administrator that you provide when deploying the Appliance Virtualization Platform host.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, do the following:
   a. Select a host.
   b. Click **More Actions** > **Change Password**.
4. In the Change Password section, type the current password and the new 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

Password policy on page 1379
Change Password field descriptions on page 1380

Password policy

The password must meet the following requirements:

- Must contain at least eight characters.
- Must contain at least one of each: an uppercase letter, a lowercase letter, a numerical, and a special character.
- Must not contain an uppercase letter at the beginning and a digit at the end.

Note:

An Uppercase letter at the beginning of a password is not counted for the password complexity rule. The Uppercase letter must be within the password.

Example of a valid password is *myPassword$*.

If the password does not meet the requirements, the system prompts you to enter a new password. Enter the existing password and the new password in the correct fields.

Ensure that you keep the admin password safe. You need the password while adding the host to Solution Deployment Manager and for troubleshooting.

Related links

Changing the password for an Appliance Virtualization Platform host on page 1379

Change Password field descriptions

Name	Description
Current Password	The password for the user you input when adding the host.
New Password	The new password
Confirm New Password	The new password

Button	Description
Change Password	Saves the new password.

Enabling and disabling SSH on Appliance Virtualization Platform from Solution Deployment Manager

About this task

For security purpose, SSH access to Appliance Virtualization Platform shuts down in the normal operation. To continue access, enable the SSH service on Appliance Virtualization Platform from Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. Select an Appliance Virtualization Platform host.
4. To enable SSH, do the following:
   a. Click **More Actions** > **SSH** > **Enable SSH**.
   b. In the Confirm dialog box, in the **Time (in minutes)** field, type the time after which the system times out the SSH connection.

      The range is 10 minutes through 120 minutes.
   c. Click **Ok**.

      The system displays `enabled` in the **SSH status** column.
5. To disable SSH, click **More Actions** > **SSH** > **Disable SSH**.

   The system displays `disabled` in the **SSH status** column.

Activating SSH from AVP Utilities

About this task

For security purpose, SSH access to Appliance Virtualization Platform shuts down in the normal operation. You must activate SSH on Appliance Virtualization Platform.

When you install or preinstall Appliance Virtualization Platform on a server, SSH is enabled. After you accept the license terms during Appliance Virtualization Platform installation, SSH shuts down within 24 hours. After SSH shuts down, you must reactivate SSH by using the **`AVP_SSH enable`** command from AVP Utilities.

Before you begin

Start an SSH session.

Procedure

1. Log in to the AVP Utilities virtual machine running on Appliance Virtualization Platform with administrator privilege credentials.
2. Type the following:

   ```
   AVP_SSH enable
   ```

   Within 3 minutes, the SSH service starts on the Appliance Virtualization Platform, and runs for two hours from AVP Utilities. After two hours, you must reactivate SSH from AVP Utilities.

   When SSH is enabled, you can use an SSH client, such as PuTTY, to gain access to Appliance Virtualization Platform on customer management IP address or the services port IP address of 192.168.13.6.
3. **(Optional)** To find the status of SSH, type `AVP_SSH status`.
4. To disable SSH, type `AVP_SSH disable`.

Enabling and disabling SSH on Appliance Virtualization Platform from System Manager CLI

About this task

For security purpose, SSH access to Appliance Virtualization Platform shuts down in the normal operation. You must enable the SSH service on Appliance Virtualization Platform.

You can enable SSH, disable SSH, and check the SSH status on the Appliance Virtualization Platform host.

Before you begin

Start an SSH session.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Navigate to the `$MGMT_HOME/infra/bin/avpSSHUtility` location.
3. Type `./enableDisableSSHOnAVP.sh`.

   The system displays the following options:

   - Enable SSH on the Appliance Virtualization Platform host.
   - Disable SSH on the Appliance Virtualization Platform host.
   - Check the SSH status on the Appliance Virtualization Platform host.
4. To enable SSH, perform the following:

   a. At the prompt, type `1` and press `Enter`.

b. Type the IP address of the Appliance Virtualization Platform host.

c. Type the time in minutes.

The time is the duration after which the system blocks any new SSH connections. The valid range 10 to 120 minutes.

The system displays the message and enables SSH on Appliance Virtualization Platform host.

For example, if you set the time to 50 minutes, after 50 minutes, the system blocks any new SSH connections. If you reenable SSH before completion of 50 minutes, the system adds 50 minutes to the initial 50 minutes to reenable connections.

5. To disable SSH, perform the following:

   a. At the prompt, type `2` and press `Enter`.

   b. Type the IP address of the Appliance Virtualization Platform host.

   If SSH is already disabled, the system displays `False` and the message `SSH is already disabled. No operation performed. Exiting`.

6. **(Optional)** To view the status of SSH, perform the following:

   a. At the prompt, type `3` and press `Enter`.

   b. Type the IP address of the Appliance Virtualization Platform host.

   If SSH is enabled, the system displays `Is SSH enable — false`.

   If SSH is disabled, the system displays `Is SSH disable — true`.

Changing the IP address and default gateway of the host

About this task

When you change the default gateway and IP address from the vSphere web client, the change might be unsuccessful.

You cannot remotely change the IP address of the Appliance Virtualization Platform host to a different network. You can change the IP address remotely only within the same network.

To change the Appliance Virtualization Platform host to a different network, perform Step 2 or Step 3.

Before you begin

Connect the computer to the services port.

Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.

3. At the command prompt of the host, do the following:
   a. To change the IP address, type the following:

      ```
      esxcli network ip interface ipv4 set -i vmk0 -I <old IP address of the host>
      -N <new IP address of the host> -t static
      ```

      For example:

      ```
      esxcli network ip interface ipv4 set -i vmk0 -I 135.27.162.121 -N 255.255.25
      5.0 -t static
      ```

   b. To change the default gateway, type `esxcfg-route <new gateway IP address>`.

      For example:

      ```
      esxcfg-route 135.27.162.1
      ```

4. Enable SSH on Appliance Virtualization Platform and run the **`/opt/avaya/bin/./serverInitialNetworkConfig`** command.

   For more information, see Configuring servers preinstalled with Appliance Virtualization Platform.

Appliance Virtualization Platform license

From Appliance Virtualization Platform Release 7.1.2, you must install an applicable Appliance Virtualization Platform host license file on an associated Avaya WebLM server and configure Appliance Virtualization Platform to obtain its license from the WebLM server. WebLM Server can be either embedded System Manager WebLM Server or standalone WebLM Server. Appliance Virtualization Platform licenses are according to the supported server types.

For information about Appliance Virtualization Platform licenses and supported server types, see “Appliance Virtualization Platform licenses for supported servers”.

To configure the Appliance Virtualization Platform license file:

1. Obtain the applicable license file from the Avaya PLDS website.
2. Install the license file on the System Manager WebLM Server or Standalone WebLM Server.

   Note:

   The Appliance Virtualization Platform license file can contain multiple Appliance Virtualization Platform licenses that is for four different server types. One Appliance Virtualization Platform license file contains all the necessary licenses for the complete solution.

3. Configure the applicable **WebLM IP Address/FQDN** field for each Appliance Virtualization Platform host by using either System Manager Solution Deployment Manager, Solution Deployment Manager Client, or Appliance Virtualization Platform host command line interface.

You can view the license status of the Appliance Virtualization Platform host on the **Platforms** tab of the System Manager Solution Deployment Manager or Solution Deployment Manager Client interfaces. The Appliance Virtualization Platform license statuses on the **Platforms** tab are:

- **Normal:** If the Appliance Virtualization Platform host has acquired a license, the **License Status** column displays **Normal**.
- **Error:** If the Appliance Virtualization Platform host has not acquired a license. In this case, the Appliance Virtualization Platform enters the License Error mode and starts a 30-day grace period. The **License Status** column displays **Error - Grace period expires: <DD/MM/YY> <HH:MM>**.
- **Restricted:** If the 30-day grace period of the Appliance Virtualization Platform license expires, Appliance Virtualization Platform enters the License Restricted mode and restricts the administrative actions on the host and associated virtual machines. The **License Status** column displays **Restricted**. After you install a valid Appliance Virtualization Platform license on the configured WebLM Server, the system restores the full administrative functionality.

  Note:

  Restricted administrative actions for:

  - **AVP Host: AVP Update/Upgrade Management**, **Change Password**, **Host Shutdown**, and **AVP Cert. Management**.
  - **Application: New**, **Delete**, **Start**, **Stop**, and **Update**.

Appliance Virtualization Platform licensing alarms

If the Appliance Virtualization Platform license enters either License Error Mode or License Restricted Mode, the system generates a corresponding Appliance Virtualization Platform licensing alarm. You must configure the Appliance Virtualization Platform alarming. For information about how to configure the Appliance Virtualization Platform alarming feature, see *Administering Avaya Aura® AVP Utilities*.

Configuring WebLM Server for an Appliance Virtualization Platform host using Solution Deployment Manager

Before you begin

1. Add an Appliance Virtualization Platform host.

   For information about adding a host, see *Administering Avaya Aura® System Manager*.
2. Obtain the license file from the Avaya PLDS website.
3. Install the license file on the System Manager WebLM Server or Standalone WebLM Server.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.

3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section:
   a. Select the Appliance Virtualization Platform host.
   b. Click **More Actions** > **WebLM Configuration**.

      The system displays the WebLM Configuration dialog box.
4. In **WebLM IP Address/FQDN**, type the IP address or FQDN of WebLM Server.

   For WebLM configuration, if you select:

   - Only one host then **WebLM IP Address/FQDN** displays the existing WebLM Server IP Address.
   - Multiple hosts then **WebLM IP Address/FQDN** will be blank to assign the same WebLM Server IP Address for all the selected Appliance Virtualization Platform hosts.
5. In **Port Number**, type the port number of WebLM Server.

   Embedded System Manager WebLM Server supports both 443 and 52233 ports.
6. Click **Submit**.

   The system displays the status in the **Current Action** column.

   The system takes approximately 9 minutes to acquire the Appliance Virtualization Platform host license file from the configured WebLM Server. On the **Platforms** tab, click **Refresh**.

   When the Appliance Virtualization Platform host acquires the license, on the **Platforms** tab, the **License Status** column displays **Normal**.

WebLM Configuration field descriptions

Name	Description
WebLM IP Address/FQDN	The IP Address or FQDN of WebLM Server.
Port Number	The port number of WebLM Server. The default port is 52233.

Button	Description
Submit	Saves the WebLM Server configuration.
Cancel	Closes the WebLM Configuration dialog box.

Viewing the Appliance Virtualization Platform host license status using Solution Deployment Manager

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, view the Appliance Virtualization Platform host license status in the **License Status** column.

Viewing Appliance Virtualization Platform firewall rules

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select an Appliance Virtualization Platform host, and click **More Actions** > **AVP Firewall Rules**.

   System Manager displays the Firewall Settings page.
4. To view the additional details, select a row.

   System Manager displays the details in the separate section on the Firewall Settings page.

Configuring the login banner for the Appliance Virtualization Platform host

About this task

You can configure a login banner message on one or more Appliance Virtualization Platform hosts at a time.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the Host tab, in Platforms for Selected Location <location name>, select one or more Appliance Virtualization Platform hosts on which you want to configure the message.
4. Click **More Actions** > **Push Login Banner**.

   You can change the login banner text only on the Security Settings page from **Security** > **Policies** on System Manager.
5. On the Message of the Day window, click **Push Message**.

   The system updates the login banner on the selected Appliance Virtualization Platform hosts.

Applying third-party AVP certificates

Applying third-party certificates to Appliance Virtualization Platform

About this task

Use this procedure to create, download, upload, and push third-party certificates to Appliance Virtualization Platform hosts.

Before you begin

- Add a location.
- Add an Appliance Virtualization Platform host to the location.

- Ensure that the certificate on the Appliance Virtualization Platform host is valid.

Note:

If you are using a third-party generated CSR, add the private key for the CSR in the file `/etc/vmware/ssl/rui_csr_temp.key` before installing the certificate from Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. **(Optional)** Add the details of the generic CSR.

   If you add the generic CSR details, the system pre-populates the values in the View/Generate CSR dialog box.

   For more information about creating the generic CSR, see “Creating or editing generic CSR”.
5. To generate CSR, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
   b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
   c. Click **View/Generate CSR**.

      System Manager displays the View/Generate CSR dialog box.
   d. If the generic CSR details are not added for the Appliance Virtualization Platform host, add the details of the generic CSR.
   e. Click **Generate CSR**.

      The system generates CSR for the Appliance Virtualization Platform host.
   f. In the **Current Action** column, click **Status Details** to view the status.
6. To download CSR, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
   b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
   c. Click **Download CSR**.

      In case of Firefox browser, the system prompts you to save the `CSR.zip` file.
   d. In the **Current Action** column, click **Status Details** to view the status.

      In the Download CSR Status dialog box, the system displays the path of the downloaded `CSR.zip` file.

7. Extract the downloaded certificates, and ensure that the third-party signs them.
8. To upload and push the signed certificate from a third-party CA, do the following:
   a. Click **More Actions** > **AVP Cert. Management** > **Manage Certificate**.
   b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
   c. Click **Browse** and select the required certificates from the local computer.
   d. Click **I Agree to accept to add the same certificate in SDM**.
   e. Click **Push Certificate**.
   f. In the **Current Action** column, click **Status Details** to view the status.

Creating or editing generic CSR

About this task

Use this procedure to create or edit a generic CSR for third-party Appliance Virtualization Platform certificates. With a generic CSR, you can apply the same set of data for more than one Appliance Virtualization Platform host.

Procedure

1. In **Application Management Tree**, select a location.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
3. Click **More Actions** > **AVP Cert. Management** > **Generic CSR**.
4. In the Create/Edit CSR dialog box, add or edit the details of the generic CSR, such as organization, organization unit, locality, state, country, and email.
5. Click **Create/Edit CSR** and then click **OK**.

Next steps

Complete the CSR generation, download, third-party signing and push the certificates to the Appliance Virtualization Platform hosts.

Load Certificate field descriptions

Name	Description
Platform IP	The IP address of the Appliance Virtualization Platform host.
Platform FQDN	The FQDN of the Appliance Virtualization Platform host.
Certificate	The option to select the signed certificate for the Appliance Virtualization Platform host.
I agree to accept to add the same certificate in SDM.	The option to accept the certificate in Solution Deployment Manager.

Button	Description
View/Generate CSR	Displays the View/Generate CSR dialog box to generate CSR.
Download CSR	Downloads CSR for the selected host.
Browse	Displays the dialog box where you can choose the signed certificate file. The accepted certificate file formats are: • `.crt` • `.pki`
Retrieve Certificate	Displays the Certificate dialog box with the details of the uploaded signed certificate.
Push Certificate	Pushes the uploaded signed certificate to the selected Appliance Virtualization Platform host.
Cancel	Cancels the push operation.

Create or edit CSR field descriptions

Name	Description
Organization	The organization name of the CSR.
Organization Unit	The organization unit of the CSR.
Locality	The locality of the organization associated with the CSR.
State	The state of the organization associate with the CSR.
Country	The country of the organization associate with the CSR. In the Edit mode, you can specify only two letters for the country name.
Email	The email address associate with the CSR.

Button	Description
Create/Edit CSR	Saves or edits the information entered associated to the CSR.
Cancel	Cancels the add or edit operation of the CSR.

Virtual Machine snapshot on Appliance Virtualization Platform

When you apply an update by using Solution Deployment Manager, snapshots are left on Appliance Virtualization Platform. If a snapshot is left on Appliance Virtualization Platform, it is detrimental to system performance and over time can utilize all the available disk space. Therefore, ensure that snapshots are not left on Appliance Virtualization Platform for an extended period of time and are removed on a timely manner.

You can review and delete Virtual Machine snapshots from Appliance Virtualization Platform by using Solution Deployment Manager Snapshot Manager.

Related links

Deleting the virtual machine snapshot by using Solution Deployment Manager on page 1390
Snapshot Manager field descriptions on page 1390

Deleting the virtual machine snapshot by using Solution Deployment Manager

About this task

Use this procedure to delete the virtual machine snapshots that reside on the Appliance Virtualization Platform host by using Solution Deployment Manager.

Procedure

1. To access Solution Deployment Manager, do one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   - On the desktop, click the Solution Deployment Manager icon ( ).
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select the Appliance Virtualization Platform host.
4. Click **More Actions** > **Snapshot Manager**.

   The system displays the Snapshot Manager dialog box.
5. Select one or more snapshots, and click **Delete**.

   You must review all listed snapshots and remove snapshots that are more than 24 hours old.

   The system deletes the selected snapshots.

Related links

Virtual Machine snapshot on Appliance Virtualization Platform on page 1389

Snapshot Manager field descriptions

Name	Description
VM ID	The ID of the virtual machine.
Snapshot Age	The duration of snapshot creation. For example: 75 days 19 hours
VM Name	The name of the virtual machine.
Snapshot Name	The name of the snapshot.
Snapshot Description	The description of the snapshot.
SDM Snapshot	The snapshot taken from Solution Deployment Manager. The options are **Yes** and **No**.

Button	Description
Cancel	Exits from the Snapshot Manager dialog box.
Delete	Deletes the selected snapshot.

Related links

Virtual Machine snapshot on Appliance Virtualization Platform on page 1389

Update Host field descriptions

Name	Description
Patch location	The location where the Appliance Virtualization Platform patch is available. The options are: • **Select Patch from Local SMGR**: To use the Appliance Virtualization Platform patch that is available on the local System Manager. • **Select Patch from software library**: To use the Appliance Virtualization Platform patch that is available in the software library.
Ignore Signature Validation	Ignores the signature validation for the patch. **Note:** If the Appliance Virtualization Platform patch is unsigned, you must select the **Ignore signature validation** check box.
Select patch file	The absolute path to the Appliance Virtualization Platform patch file.

Button	Description
Update Host	Installs the patch on the Appliance Virtualization Platform host.

Shutting down the Appliance Virtualization Platform host

About this task

You can perform the shutdown operation on one Appliance Virtualization Platform host at a time. You cannot schedule the operation.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Lifecycle Action** > **Host Shutdown**.

   The Appliance Virtualization Platform host and virtual machines shut down.

Restarting Appliance Virtualization Platform or an ESXi host

About this task

The restart operation fails, if you restart the host on which System Manager itself is running. If you want to restart the host, you can do this either through vSphere Web Client or through the Solution Deployment Manager client.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
4. Click **More Actions** > **Lifecycle Action** > **Host Restart**.
5. On the confirmation dialog box, click **Yes**.

   The system restarts the host and virtual machines running on the host.

Managing certificates

Certification validation

With System Manager Solution Deployment Manager and Solution Deployment Manager client, you can establish a certificate-based TLS connection between the Solution Deployment Manager service and a host that is running Avaya Aura® 7.x and later applications. This provides secure communications between System Manager Solution Deployment Manager or the Solution Deployment Manager client and Appliance Virtualization Platform or ESXi hosts or vCenter.

The certificate-based sessions apply to the Avaya Aura® Virtualized Appliance offer using host self-signed certificates and the customer-provided Virtualization Environment using host self-signed or third-party certificates.

You can check the following with certificate-based TLS sessions:

- Certificate valid dates
- Origin of Certificate Authority
- Chain of Trust
- CRL or OCSP state
- Log Certificate Validation Events

Solution Deployment Manager checks the certificate status of hosts. If the certificate is incorrect, Solution Deployment Manager does not connect to the host.

For the correct certificate:

- The fully qualified domain or IP address of the host to which you are connecting must match the value in the certificate SAN or the certificate Common Name and the certificate must be in date.
- Appliance Virtualization Platform and VMware ESXi hosts do not automatically regenerate their certificates when host details such as IP address or hostname and domain changes. The certificate might become incorrect for the host.

If the certificate is incorrect:

- For the Appliance Virtualization Platform host, Solution Deployment Manager regenerates the certificate on the host and then uses the corrected certificate for the connection.

- For the VMware ESXi host or vCenter, the system denies connection. The customer must update or correct the certificate on the host or vCenter.

  For more information about updating the certificate, see “Updating the certificate on the ESXi host from VMware”.

Note:

Solution Deployment Manager:

- Validates certificate of vCenter
- Validates the certificates when a virtual machine is deployed or upgraded on vCenter managed hosts

With Solution Deployment Manager, you can only accept certificate while adding vCenter. If a certificate changes, the system gives a warning that the certificate does not match the certificate in the trust store on Solution Deployment Manager. You must get a new certificate, accept the certificate as valid, and save the certificate on the system.

To validate certificates, you can open the web page of the host. The system displays the existing certificate and you can match the details.

Generating and accepting the Appliance Virtualization Platform host certificates

About this task

With Solution Deployment Manager, you can generate certificates only for Appliance Virtualization Platform hosts.

If the certificate is invalid:

- Get a correct certificate for the host and add the certificate.
- Regenerate a self-signed certificate on the host.

Before you begin

Get permissions to add a host to generate certificates.

Procedure

1. To access Solution Deployment Manager, do one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   - On the desktop, click the Solution Deployment Manager icon ( ).
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions** > **Generate/Accept Certificate**.

5. To accept the certificate, in the Certificate dialog box, click **Generate Certificate**, and do the following:
   a. In the Generate Certificate dialog box, in the **Validity in Days** field, type the validity of the certificate in days.
   b. Click **Generate Certificate**.

      The system displays the message: `Certificate is generated`.
   c. Click **Ok**.
6. To accept the certificate, click **Accept Certificate**.
7. To view the certificate validity status, click the **View link** in the **Platform Certificate Status** column.

   Appliance Virtualization Platform places an IP address and FQDN in generated certificates. Therefore, from Solution Deployment Manager, you can connect to Appliance Virtualization Platform hosts through IP address or FQDN.

   In the Platforms for Selected Location <location name> section, the **Platform Certificate Status** column must display a check mark ✔.

   Note:

   An alarm is generated everyday if the certificate expiry is below 60 days. This alarm can be cleared by installing a new identity certificate, which has the validity more than 60 days.

Generating and updating the certificate on the ESXi host from VMware

About this task

Generate new certificates only if you change the host name or accidentally delete the certificate. Under certain circumstances, you must force the host to generate new certificates.

To receive the full benefit of certificate checking, particularly if you want to use encrypted remote connections externally, do not use a self-signed certificate. Instead, install new certificates that are signed by a valid internal certificate authority or purchase a certificate from a trusted security authority.

Procedure

To generate and update ESXi host and vCenter certificates, see the VMware documentation.

Next steps

Note:

The host certificate must match the fully qualified domain name of the host.

VMware places only FQDN in certificates that are generated on the host. Therefore, use a fully qualified domain name to connect to ESXi hosts and vCenter from Solution Deployment Manager.

The connection from Solution Deployment Manager 7.1 and later to a vCenter or ESXi host by using an IP address fails because the IP address is absent in the certificate and the connection is not sufficiently secure.

Managing certificates for existing hosts

About this task

By default, the certificate status of the host or vCenter that is migrated from earlier release is invalid. To perform any operation on the host from Solution Deployment Manager, you require a valid certificate. Therefore, you must get the valid certificate and accept the certificate.

Before you begin

Gain permissions to add a host to generate certificates.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
4. For the ESXi host, do one of the following:
   - If the certificate is valid, on the Certificate dialog box, click **More Actions** > **Generate/ Accept Certificate**, and click **Accept Certificate**.
   - If the certificate is invalid, log in to the ESXi host, validate the certificate, and then from Solution Deployment Manager, accept the certificate.

     For more information, see “Generating and updating the certificate on the ESXi host from VMware”.

Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface

About this task

This procedure is required for both preloaded/prelicensed ASP S8300 and fresh install on ASP S8300.

Before adding an Avaya Solutions Platform S8300 host, to regenerate the Avaya Solutions Platform S8300 self-signed certificate with FQDN, perform the following steps:

For information about adding an Avaya Solutions Platform S8300 host, see Adding an Avaya Solutions Platform S8300 Release host on page 1358.

Procedure

1. Log in to the Avaya Solutions Platform S8300 command line interface.
2. To change the FQDN, type the following command:

   ```
   esxcli system hostname set --fqdn=server.abc.com
   ```

Here, `server.abc.com` is the FQDN of the ESXi host.

For more information, see Changing the host name on the VMware documentation website.

3. To regenerate the self-signed certificate, do the following:
   a. Enable SSH on the ESXi host, then put the ESXi host into the maintenance mode.
   b. SSH to the ESXi host and use the following commands to take backups of the current certificate file and private key file.

      ```
      cd /etc/vmware/ssl
      mv rui.crt rui.crt.bkp
      mv rui.key rui.key.bkp
      ```

   c. To regenerate a new certificate, type the following command:

      ```
      /sbin/generate-certificates
      ```

      Verify that the new certificate file and private key file are generated.
   d. To restart the ESXi Server management agent, reboot the host.

      The ESXi host generates a new self-signed certificate.

For more information, see Generating new self-signed certificates for the ESXi host.

Managing the application

Deploying an OVA file for an Avaya Aura® application

About this task

Use the procedure to deploy an OVA file for an Avaya Aura® application on the virtual machine.

To deploy an Avaya Aura® application, you can use Solution Deployment Manager from System Manager or the Solution Deployment Manager client if System Manager is unavailable.

Before you begin

- Add a location.
- Add a required host to the location.

  Note:

  Before starting the new virtual machine deployment, you must perform the **Refresh Host** operation on the selected host.
- Ensure that the certificate is valid on the host or vCenter managed hosts.
- Download the required OVA file to System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.

2. In **Application Management Tree**, select a platform.
3. On the **Applications** tab, in the Applications for Selected Location <location name> section, click **New**.

   Solution Deployment Manager displays the Applications Deployment window.
4. In the Select Location and Platform section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Platform**, select a platform.

      Solution Deployment Manager displays the host name in the **Platform FQDN** field.
5. In **Data Store**, select a data store, if not displayed upon host selection.

   The Capacity Details section displays the capacity details.
6. Click **Next**.
7. To get the OVA file, select the **OVA** tab, and click one of the following:
   - **URL**, in **OVA File**, type the absolute path to the application OVA file, and click **Submit**.
   - **S/W Library**, in **File Name**, select the application OVA file.
   - **Browse**, select the required application OVA file from a location on the computer, and click **Submit File**.

   If the OVA file does not contain a valid Avaya certificate, then the system does not parse the OVA and displays the following message: `Invalid file content. Avaya Certificate not found or invalid`
8. In **Flexi Footprint**, select the footprint size that the application supports.
9. **(Optional)** To install the patch file for the Avaya Aura® application, click **Service or Feature Pack**, and enter the appropriate parameters.
   - **URL**, and type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the latest service or feature pack.
   - **S/W Library**, and select the latest service or feature pack from the drop-down list.
   - **Browse**, and select the latest service or feature pack from your local computer, and click **Submit File**.

   You can install the patch file for the Avaya Aura® application now or after completing the Avaya Aura® application OVA deployment.
10. Click **Next**.

    In Configuration Parameters and Network Parameters sections, Solution Deployment Manager displays the fields that are specific to the application that you deploy.
11. In the Network Parameters section, ensure that the following fields are preconfigured:
    - **Public**
    - **Services**: Only for AVP Utilities.

- **Duplicate Link**: Only for duplex Communication Manager.
- **Private**: Only for Application Enablement Services.
- **Out of Band Management**.

For more information, see “Application Deployment field descriptions”.

12. In the Configuration Parameters section, complete the fields.

    For each application that you deploy, fill the appropriate fields. For more information, see “Application Deployment field descriptions”.

13. Click **Deploy**.
14. Click **Accept the license terms**.

    In the Platforms for Selected Location <location name> section, Solution Deployment Manager displays the deployment status in the **Current Action Status** column.

    Solution Deployment Manager displays the virtual machine on the Applications for Selected Location <location name> page.

15. To view details, click **Status Details**.

Next steps

Perform the following for Communication Manager:

1. From the Manage Elements link on System Manager, update the credentials corresponding to the element that you added.
2. Before the synchronization and after deployment, add an SMNP profile on Communication Manager.

   Note:

   If you fail to update the password, the synchronization operation fails.

Related links

Installing software patches by using Solution Deployment Manager on page 1401
Application Deployment field descriptions on page 1408

Refreshing elements

Before you begin

- On the User Settings page, configure the user settings.

Note:

For Branch Session Manager, Session Manager, AES, and other elements (excluding Communication Manager), the user must follow these steps in sequence to ensure that the correct options appear in the **Operation** drop-down menu on the **Upgrade Configuration** page.

1. Refreshing elements on page 1348
2. Analyzing software on page 1349

3. Performing the preupgrade check on page 1351

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the 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

About this task

Analyze works on the version of OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitle update or upgrade version, the version field must contain valid value. You can get the version values from versions files that are available on PLDS.

Custom patching does not require the analyze operation.

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 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.

Re-establishing trust for Solution Deployment Manager elements

About this task

Use this procedure to re-establish trust with an application.

Before you begin

- Add a location.
- Add an Appliance Virtualization Platform host to the location.

Procedure

1. To access Solution Deployment Manager, do one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   - On the desktop, click the Solution Deployment Manager icon ( ).
2. Click **Application Management**.
3. In **Application Management Tree**, select a platform.
4. On the **Applications** tab, in the Applications for Selected Location <location name> area, select an application.
5. Click **More Actions** > **Re-establish connection**.
6. Select the release version of the product deployed on the application.

   The options are:

   - **6.3 and below**: When you select this, the system displays the following message:

     ```
     Trust cannot be established for this version VM.
     ```
   - **7.0**
   - **7.1 and above**
   - **others**

   Note:

   When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.
7. When you select the version **7.0** or **others**, in **User Name**, type the user name of the application.
8. When you select the version **7.0** or **others**, in **Password**, type the password of the application.

9. Click **Reestablish Connection**.

Installing software patches by using Solution Deployment Manager

About this task

Use the procedure to install software patches and service packs that are entitled for an Avaya Aura® application, and commit the patches that you installed.

Note:

- When you are installing an element patch and the patch installation fails or the patch information is unavailable in **Upgrade Actions** > **Installed Patches** on the Upgrade Management page, then perform the following:
  1. Ensure that the element is reachable on System Manager Solution Deployment Manager.
  2. Refresh the element.

Before you begin

- Perform refresh and analyze operations.
- If you upgrade an application that was not deployed from Solution Deployment Manager:
  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 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 **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.

   Note:

   If an application is unreachable, the auto commit operation might fail and the Update Patch Status window displays a warning message. You must wait for some time, select the same patch in the Installed Patches section, and perform the commit operation again.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.

10. Click **Save**.
11. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

    If the field displays , review the information on the Edit Upgrade Configuration page.
12. Click **Upgrade**.
13. 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.
14. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display .
15. 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 .
16. Click **Upgrade Actions** > **Installed Patches**.
17. 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.
18. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

    You can schedule to commit the patch at a later time by using the **Schedule later** option.
19. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.
20. Ensure that **Update status** and **Last Action Status** fields display .

    Note:

    If the patch commit fails or auto commit is not executed even after 24 hours, delete the snapshot that are not required. For information about deleting the virtual machine snapshot from host, see “Deleting the virtual machine snapshot”.

Editing an application

Before you begin

- Install the Solution Deployment Manager client.

- An ESXi host must be available.
- When you change the IP address or FQDN:
  - AVP Utilities must be available and must be discovered.
  - If AVP Utilities is discovered, the system must display AVP Utilities in the **App Name** column. If the application name in **App Name** is empty, click **More Actions** > **Re-establish connection** to establish trust between the application and System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Location <location name> section, select an application, and click **Edit**.

   The system displays the Edit App section.
4. To update the IP address and FQDN of the application in the local Solution Deployment Manager inventory, perform the following:
   a. Click **More Actions** > **Re-establish connection**.

      Note:

      To update IP address or FQDN for AVP Utilities, establish trust on all applications that are running on the host on which AVP Utilities resides.

   b. Click **More Actions** > **Refresh App**.

      Note:

      To update IP address or FQDN for AVP Utilities, refresh all applications that are running on the host on which AVP Utilities resides.

   c. Click **Update IP/FQDN in Local Inventory**.
   d. Click **Update App IP/FQDN**.
   e. Provide the IP address and FQDN of the application.

      Update IP/FQDN in Local Inventory updates the IP address or FQDN of the application 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 **Platforms** tab to update the IP address or FQDN of the host.
5. Click **Save**.

Deleting an application

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.

2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, select one or more application.
4. Click **Delete**.

   System Manager displays the following message:

   ```
   Software Only application will be deleted from inventory only.
   Other application(s) will be power off and deleted from Platform.
   Are you sure you want to delete application(s) ?
   ```

   ```
   Note : If you selected VM for which VM deployment has failed due to
   VM Validation Error then that VM entry will be deleted from local
   inventory only.
   ```

5. Click **Yes** to confirm.

   System Manager turns off the applications and deletes the selected applications from the platform.

Updating Services Port Static Routing on an Avaya Aura® application

About this task

You might have to change the static routing if the Avaya Aura® application that is running on the Appliance Virtualization Platform host is:

- Deployed by using the vSphere Web Client and does not have the route.
- Non-operational or unreachable when you start the Avaya Aura® application update.

Before you begin

- Update network parameters of AVP Utilities if applicable.
- Ensure that the Avaya Aura® application resides on the same subnet as AVP Utilities.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the Applications tab, in the Applications for Selected Location <location name> section, select an Avaya Aura® application.
3. Click **More Actions** > **Update Static Routing**.

   The VM Update Static Routing page displays the details of Avaya Aura® application and AVP Utilities. The fields are read-only.
4. Click **Update**.
5. On the Success dialog box, click **OK**.

   The system updates the Avaya Aura® application with the new IP address of AVP Utilities for Services Port static routing.

Related links

Update Static Routing field descriptions on page 1413

Starting an application from Solution Deployment Manager

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. From the **Application Management Tree**, select a platform to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to start.
4. Click **Start**.

   In **Application State**, the system displays `Started`.

Stopping an application from Solution Deployment Manager

About this task

System Manager is operational and ESXi or vCenter is added to the Application Management page to deploy Avaya Aura® Application OVA on ESXi applications.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. From the **Application Management Tree**, select a ESXi or vCenter host to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to stop.
4. Click **Stop**.

   In **Application State**, the system displays `Stopped`.

Restarting an application from Solution Deployment Manager

Before you begin

- System Manager is operational, and ESXi or vCenter is added to the Application Management page to deploy Avaya Aura® Application OVA on ESXi applications.
- Applications must be in the running state.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. From the application management tree, select a host to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to restart.
4. Click **Restart**.

   In **Application State**, the system displays `Stopped` and then `Started`.

VM Console overview

From Release 8.1.1, you can open the VM console in a new browser window or on a new browser tab.

To open and manage the application through the console, ensure that the:

- Application must be in running state. The application status must be **Started** for the application on the **Applications** tab in the **Application State** column.
- Application must reside on the Appliance Virtualization Platform host Release 7.1.2 and later.
- Appliance Virtualization Platform host certificate must be added in your browser.

You cannot view the VM Console of the application if the application resides on the customer-provided VMware ESXi host.

Opening a VM console from Solution Deployment Manager

About this task

Use the following procedure to open the VM console in a new browser window or on a new browser tab.

Before you begin

- Add a location.
- Add the Appliance Virtualization Platform host.
- Ensure that the application is hosted on the Appliance Virtualization Platform host.
- Add the Appliance Virtualization Platform host certificate in your browser.

  If you do not add the host certificate in your browser, the system displays the following message when you try to open the VM console in a browser:

  ```
  To open VM Console of an application, add the Platform certificate
  in the browser. Following is the URL of the platform to accept the
  certificate: https://<Host URL where the application resides>:443
  ```

Procedure

1. To access Solution Deployment Manager, do one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager**.
   - On the desktop, click the Solution Deployment Manager icon ( ).
2. Click **Application Management**.
3. In **Application Management Tree**, select a location.
4. On the **Applications** tab, in the **Applications for Selected Location <location name>** section, select the application.
5. To open the VM console in a new:
   - Browser window, click **VM Console** > **Open VM Console in New Window**.

- Tab of the browser, click **VM Console** > **Open VM Console in New Tab**.

When you open the console for the very first time, if the Appliance Virtualization Platform host certificate is not added in your browser, the system opens the browser instance with the following message:

```
To open VM Console of an application, add the Platform certificate
in the browser. Following is the URL of the platform to accept the
certificate: https://<Host URL where the application resides>:443
```

If you open the VM console after accepting the Appliance Virtualization Platform host certificate in the browser, the system opens the VM console without any warning message.

If the browser displays the same error message even after accepting the Appliance Virtualization Platform host certificate, see *Troubleshooting Avaya Aura® System Manager*.

Next steps

On VM Console, log in to the application and perform the required operations.

VM Console field descriptions

Name	Description
Full Screen	Opens the console in full screen mode. You can press the **Esc** key to exit from the full screen mode.
Send Keys	These keys are applied to the VM Linux system and not to your local computer from where you are accessing the VM Console. The options are: • **Send Ctrl+Alt+Del** • **Send Ctrl+c** • **Send Escape**
KeyBoard Layout	Sets the keyboard layout based on the selected language. The options are: • English • Japanese • German • Italian • Spanish • Portuguese • French • Swiss-French • Swiss-German

Common causes for application deployment failure

If the application is not reachable from System Manager Solution Deployment Manager or Solution Deployment Manager Client, the OVA deployment fails at the sanity stage, because you might have:

- Provided an IP which is not on the network.
- Provided wrong network values that causes the network configuration for the application to not work properly.
- Chosen a private virtual network.

The following are some examples of wrong network values and configuration that can result in the OVA deployment failure:

- Using an IP which is already there on the network (duplicate IP).
- Using an IP which is not on your network at all.
- Using a DNS value, such as `0.0.0.0`.
- Deploying on an isolated network on your VE deployment.

You can check the deployment status in the **Current Action Status** column on the **Applications** tab.

Application Deployment field descriptions

Select Location and Platform

Name	Description
Select Location	The location name.
Select Platform	The platform name that you must select.
Platform FQDN	The platform FQDN.
Data Store	The data store for the application. The page populates the capacity details in the Capacity Details section.
Next	Displays the OVA/ISO Details section where you provide the details required for OVA or ISO deployment.

Capacity Details

The system displays the CPU and memory details of the Avaya Solutions Platform 130 or ESXi host. The fields are read-only.

Note:

If the host is in a cluster, the system does not display the capacity details of CPU and memory. Ensure that the host resource requirements are met before you deploy the virtual machine.

Name	Description
Name	The name

Table continues…

Name	Description
Full Capacity	The maximum capacity
Free Capacity	The available capacity
Reserved Capacity	The reserved capacity
Status	The configuration status

Provide admin and root Credentials

The system displays the Provide admin and root Credentials section for OS.

Name	Description
Platform IP	The platform IP.
Platform FQDN	The platform FQDN
Admin User of OS	The admin user name of OS.
Admin Password of OS	The admin password of OS.
Root User of OS	The root user of OS.

Deploy OVA using System Manager Solution Deployment Manager

Name	Description
ME Deployment	The option to perform the Midsize Enterprise deployment. The option to perform the Midsize Enterprise deployment. The option is available only while deploying Communication Manager simplex OVA.
Enable enhanced security	The option to enable JITC mode deployment.
Select Software Library	The software library where the `.ova` file is available.
Select OVAs	The `.ova` file that you want to deploy. **Note:** System Manager validates any file that you upload during deployment, and accepts only OVA file type. System Manager filters uploaded files based on file extension and mime types or bytes in the file.
Flexi Footprint	The footprint size supported for the selected application. **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.
Next	Displays the Configuration Parameters tab in the OVA Details screen where you provide the OVA details.

Deploy OVA using the Solution Deployment Manager client

Name	Description
ME Deployment	The option to perform the Midsize Enterprise deployment. The option to perform the Midsize Enterprise deployment. The option is available only while deploying Communication Manager simplex OVA.

The system displays the following options for deployment by providing OVA path.

Name	Description
Browse	The option to enter the full/absolute path of the `.ova` file to install it as a virtual machine on the system that hosts the Solution Deployment Manager client.
OVA File	The absolute path to the `.ova` file on the system that hosts the Solution Deployment Manager client. The field is available only when you click **Provide OVA Path**.
Submit File	Selects the `.ova` file of System Manager that you want to deploy.

With the **S/W Library** option you can select a `.ova` file that is available in the local software library of windows machine where the Solution Deployment Manager client is installed.

The system displays the following options for deployment using local software library.

Name	Description
File Name	The file name of the `.ova` file that is to be installed on the system that hosts the Solution Deployment Manager client. The field is available only when you click **S/W Library**.

With the **URL** option, you can type the URL of the OVA or ISO file. The system displays the following options.

Name	Description
URL	The URL of the OVA or ISO file. The field is available only when you click **URL**.
Submit	Selects the OVA or ISO file to be deployed that is extracted from the URL.

The system displays the following common fields.

Name	Description
Flexi Footprint	The footprint size supported for the selected application. The field is available for all three types of deployment. **Important:** Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory.
Next	Displays the **Configuration Parameters** tab in the OVA Details section where you provide the OVA details.

Configuration Parameters

The system populates most of the fields depending on the OVA file.

Name	Description
Application Name	The name of the application.
Product	The name of the Avaya Aura® application that is being deployed. The field is read-only.
Version	Release number of the Avaya Aura® application that is being deployed. The field is read-only.

Communication Manager Configuration Parameters

Name	Description
CM IPv4 Address	The IPv4 address of the Communication Manager virtual machine.
CM IPv4 Netmask	The IPv4 network mask of the Communication Manager virtual machine.
CM IPv4 Gateway	The IPv4 default gateway of the Communication Manager virtual machine.
CM IPv6 Address	The IPv6 address of the Communication Manager virtual machine. The field is optional.
CM IPv6 Network Prefix	The IPv6 network prefix of the Communication Manager virtual machine. The field is optional.
CM IPv6 Gateway	The IPv6 gateway of the Communication Manager virtual machine. The field is optional.
Out of Band Management IPv4 Address	The IPv4 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 IPv4 Netmask	The IPv4 subnet mask of the Communication Manager virtual machine for out of band management.

Table continues…

Name	Description
Out of Band Management IPv6 Address	The IPv6 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 IPv6 Network Prefix	The IPv4 subnet mask of the Communication Manager virtual machine for out of band management.
CM Hostname	The hostname of the Communication Manager virtual machine.
NTP Server(s)	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,). You can type up to three NTP servers. The application supports only the NTP server. It does not support the NTP pool.
DNS Server(s)	The DNS IP address of the Communication Manager 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 IPv4 address of the reachable WebLM server. The field is mandatory.
EASG User Access	Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks. The options are: • 1: To enable EASG. • 2: To disable EASG. Avaya recommends that you enable EASG. You can also enable EASG after deploying or upgrading the application using the command: **`EASGManage --enableEASG`**.
CM Privileged Administrator User Login	The login name for the privileged administrator. You can change the value at any point of time. The field is mandatory.
CM Privileged Administrator User Password	The password for the privileged administrator. You can change the value at any point of time. The field is mandatory.
Confirm Password	The password required to be confirmed. The field is mandatory.

Customer Root Account

Note:

The **Customer Root Account** field is applicable only in case of deploying application OVA on Appliance Virtualization Platform Release 8.x or earlier, Avaya Solutions Platform 130, and VMware by using Solution Deployment Manager. The system does not display the **Customer Root Account** field, when you deploy an application:

- OVA on VMware by using vSphere Client (HTML5).
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

Name	Description
Enable Customer Root Account for this Application	Enables or disables the customer root account for the application. Displays the ROOT ACCESS ACCEPTANCE STATEMENT screen. To accept the root access, click **Accept**. When you accept the root access statement, the system displays the **Customer Root Password** and **Re-enter Customer Root Password** fields.
Customer Root Password	The root password for the application
Re-enter Customer Root Password	The root password for the application

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.
Duplication Link	The connection for server duplication. The field is available only when you deploy duplex Communication Manager.
Private	The field is available only when you deploy Application Enablement Services.
Create Port Group	The field to create new port group for interface.
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.

Update Static Routing field descriptions

Name	Description
VM Name	The application name.
VM IP/FQDN	The IP address or FQDN of the application.
Utility Services IP	The IP address of AVP Utilities.

Button	Description
Update	Updates the static IP address for routing.

Installed Patches field descriptions

Name	Description
Application Name	The name of the application on which you want to install the patch.
Application IP	The IP address of the application 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
Action to be performed	The operation that you want to perform on the software patch, service pack, or feature pack that you installed. The options are: • **All**: Displays all the software patches. • **Commit**: Displays the software patches that you can commit. • **Rollback**: Displays the software patches that you can rollback.
Get Patch Info	Displays software patches, service packs, and feature packs that you installed.
Commit	Commits the selected software patch.
Rollback	Rolls back the selected software patch.

Update App 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.

Table continues…

Name	Description
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.
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
Select Version	Select the required version. The options are: • **6.3 and below** • **7.0** • **7.1 and above** • **others** **Note:** When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.
Application Name	The name of the application.
VM IP/FQDN	The IP address or FQDN of the application.
User Name	The user name of the application. **Note:** When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.
Password	The password of the application. **Note:** When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.

Button	Description
Reestablish Connection	Establishes connection between System Manager and the application.
Cancel	Cancels the changes and returns to the previous page.

Virtual machine report

You can generate a report of virtual machines that are installed on the Appliance Virtualization Platform host.

The script to generate the virtual machine report is in the `/swlibrary/reports/generate_report.sh` folder.

Important:

If you run the report generation script when an upgrade is in progress on System Manager, the upgrade might fail.

generate_report.sh command

The **`generate_report.sh`** generates the virtual machine report.

Syntax

```
sh ./generate_report.sh [-g] [-u Provide SMGR UI user name] [-p Provide SMGR UI
password] [-s] [-a]
```

-g	The option to generate the report.
-u, SMGR UI user name	System Manager Web console user name.
-p, SMGR UI password	System Manager Web console password.
-s	The option to view the status of the generated report.
-a	The option to abort the generated report.

Generating a virtual machine report

Before you begin

If the application is of prior to Release 7.1, you must establish the trust with all applications before running the Report Generation utility.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the `/swlibrary/reports/` directory.
3. Type the `./generate_report.sh -g -u <SMGR UI Username> -p <SMGR UI Password>` command:

   For example: `./generate_report.sh -g -u admin -p password`

   The system displays the following message: `Executing the Report Generation script can cause the failure of upgrade that is running on the System Manager system. Do you still want to continue? [Y/N].`
4. To proceed with report generation, type `Y`, and press `Enter`.

The system generates the report in the `.csv` format in the `/swlibrary/reports/vm_app_report_DDMMYYYYxxxx.csv` folder.

Note:

If you re-run the report generation script when the report generation process is in progress, the system displays the following message: `Report Generation Process is Already Running, Kindly try after some time`.

5. **(Optional)** To view the logs, go to `/swlibrary/reports/generate_report-YYYYMMDDxxxx.log`.

Viewing the status of the virtual machine report

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the `/swlibrary/reports/` directory.
3. Type the `./generate_report.sh -s` command.

   If the virtual machine report generation is in progress, the system displays the following message: `Report Generation Process is Running`.

Aborting the virtual machine report generation

About this task

If the virtual machine report generation process is in progress and you want to abort the report generation process, use the following procedure.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the `/swlibrary/reports/` directory.
3. Type the `./generate_report.sh -a` command.

   The system aborts the virtual machine report generation process.

Monitoring a host and virtual machine

Monitoring a platform

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click **Monitor Platforms**.

3. On 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 an application

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click **Monitor Applications**.
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

Creating a role for a user

About this task

To manage a vCenter or ESXi in Solution Deployment Manager, you must provide complete administrative-level privileges to the user.

Use the following procedure to create a role with administrative-level privileges for the user.

Procedure

1. Log in to vCenter Server.
2. On the Home page, click **Administration** > **Roles**.

   The system displays the Create Role dialog box.
3. In **Role name**, type a role name for the user.
4. To provide complete administrative-level privileges, select the **All Privileges** check box.
5. **(Optional)** To provide minimum mandatory privileges, do the following.
   a. In All Privileges, select the following check boxes:
      - **Datastore**
      - **Datastore cluster**

- **Distributed switch**
- **Folder**
- **Host profile**
- **Network**
- **Resource**
- **Tasks**
- **Virtual machine**
- **vApp**

Note:

You must select all the subprivileges under the list of main set of privileges. For example, when you select the **Distributed switch** check box, ensure that you select all the related subprivileges. This is applicable for all the main privileges mentioned above. If you do not select all the subprivileges, the system might not work properly.

b. In All Privileges, expand **Host**, and select the **Configuration** check box.

Note:

You must select all the subprivileges under **Configuration**.

6. Click **OK** to save the privileges.

Next steps

Assign this role to the user for mapping vCenter in Solution Deployment Manager. To assign the role to the user, see the VMware documentation.

Adding a vCenter to Solution Deployment Manager

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 6.0, 6.5, 6.7, 7.0, and 8.0. When you add vCenter, System Manager discovers the ESXi hosts that this vCenter manages, adds them to the repository, and displays in the Managed Hosts section. Also, System Manager 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. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.

2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **Add**.
4. In the New vCenter section, provide the following vCenter information:
   a. In **vCenter FQDN**, type FQDN of vCenter.
      - For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.
      - The FQDN value must match the value of the **SAN** field of the vCenter certificate. The FQDN value is case-sensitive.
   b. In **User Name**, type the username to log in to vCenter.
   c. In **Password**, type the password to log in to vCenter.
   d. In **Authentication Type**, select **SSO** or **LOCAL** as the authentication type.

      If you select the authentication type as **SSO**, Solution Deployment Manager displays the **Is SSO managed by Platform Service Controller (PSC)** field.
   e. **(Optional)** If PSC is configured to facilitate the SSO service, select **Is SSO managed by Platform Service Controller (PSC)**.

      PSC must have a valid certificate.

      The system enables **PSC IP or FQDN**, and you must provide the IP or FQDN of PSC.
   f. **(Optional)** In **PSC IP or FQDN**, type the IP or FQDN of PSC.
5. Click **Save**.
6. On the certificate dialog box, click **Accept Certificate**.

   The system generates the certificate and adds vCenter.

   In the Managed Hosts section, the system displays the ESXi hosts that this vCenter manages.

   Note:

   - System Manager does not support vCenter with Cluster level.
   - If there is a large data center with multiple hosts in a vCenter, there can be a delay in discovering all the VMs of those hosts when mapping that vCenter in the Solution Deployment Manager. If you select a smaller number of hosts rather than all hosts, this process can be faster.

Related links

Editing vCenter on page 1421
Map vCenter field descriptions on page 1421
New vCenter and Edit vCenter field descriptions on page 1422

Editing vCenter

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select a vCenter server and click **Edit**.
4. In the Edit vCenter section, change the vCenter information as appropriate.
5. If vCenter is migrated from an earlier release, on the Certificate page, click **Save**, and then click **Accept Certificate**.
6. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:
   - Select an ESXi host and click the edit icon ( ).
   - Select one or more ESXi hosts, select the location, click **Bulk Update** > **Update**.
7. Click **Commit** to get an updated list of managed and unmanaged hosts.

   If you do not click **Commit** after you move the host from Managed Hosts to Unmanaged Hosts or vice versa, and you refresh the table, the page displays the same host in both the tables.

Deleting vCenter from Solution Deployment Manager

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
4. Click **Yes** to confirm the deletion of servers.

   The system deletes the vCenter from the inventory.

Map vCenter field descriptions

Name	Description
Name	The name of the vCenter server.
IP	The IP address of the vCenter server.

Table continues…

Name	Description
FQDN	The FQDN of the vCenter server. **Note:** Use FQDN to successfully map and log in to vCenter from Solution Deployment Manager. With IP address, the system displays an error message about the incorrect certificate and denies connection.
License	The license type of the vCenter server.
Status	The license status of the vCenter server.
Certificate Status	The certificate status of the vCenter server. The options are: • : The certificate is correct. • : The certificate is not accepted or invalid.

Button	Description
View	Displays the certificate status details of the vCenter server.
Generate/Accept Certificate	Displays the certificate dialog box where you can generate and accept a certificate for vCenter. For vCenter, you can only accept a certificate. You cannot generate a certificate.

Button	Description
Add	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 vCenter and Edit vCenter field descriptions

Name	Description
vCenter FQDN	The FQDN of vCenter.
User Name	The user name to log in to vCenter.
Password	The password that you use to log in to vCenter.

Table continues…

Name	Description
Authentication Type	The authentication type that defines how Solution Deployment Manager performs user authentication. The options are: • **SSO**: Global username used to log in to vCenter to authenticate to an external Active Directory authentication server. • **LOCAL**: User created in vCenter If you select the authentication type as **SSO**, Solution Deployment Manager displays the **Is SSO managed by Platform Service Controller (PSC)** field.
Is SSO managed by Platform Service Controller (PSC)	The check box to specify if PSC manages SSO service. When you select the check box, the system enables **PSC IP or FQDN**.
PSC IP or FQDN	The IP or FQDN of PSC.

Button	Description
Save	Saves any changes you make to FQDN, username, and authentication type of vCenter.
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.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

Button	Description
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	Displays the versions of the ESXi host linked to **vCenter FQDN**. **Note:** • For Release 10.2 and later, do not select the 6.7 version. • For Release 10.1 and later, do not select the 6.0 and 6.5 versions. • For Release 8.1 and later, do not select the 5.0 and 5.1 versions.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

Button	Description
Commit	Saves all changes that you made to vCenter on the Map vCenter page.

Managing syslog profiles

Adding a remote Syslog server profile

About this task

Use this procedure to configure a remote Syslog server details in System Manager such that it receives system logs from Appliance Virtualization Platform host through AVP Utilities.

Before you begin

To view the Syslog data from AVP Utilities or application, ensure that:

- The firewall on the Syslog server is configured correctly.
- The Syslog service on the server is running.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click **Application Management**.
3. In the lower pane, click **Configure Remote Syslog Profile**.
4. On the Syslog Receiver Configuration page, click **Add**.

   System Manager displays the Add Syslog Receiver dialog box
5. In **Profile Name**, type the profile name of the Syslog server.
6. In **IP/FQDN**, type the IP address or FQDN of the Syslog server.
7. In **Port**, type the port of the Syslog server.
8. In **Protocol**, click **TCP** or **UDP**.

9. If the remote host is TLS based, select **TLS Authentication**.
10. In **Authentication options**, click **Server certificate authentication** or **Mutual TLS authentication**.
11. Click **Save**.

Syslog Receiver Configuration field descriptions

Name	Description
Profile Name	The name of the Syslog server configuration.
IP/FQDN	The IP address or host name of the Syslog server configuration.
Port	The port number of the Syslog server configuration. The default port is 514.
Protocol	The type of port used for the Syslog server configuration. The options are: • **TCP** • **UDP** When the **tcp** protocol is selected, the system enables the **TLS Authentication** option.
TLS Authentication	The option to select if the remote host is TLS based. When **TLS Authentication** is selected, the system displays the following options: • **Server certificate authentication** • **Mutual TLS authentication** When you select **TLS Authentication**, the port value is 6514.
Server certificate authentication	The server certificate authentication. This option is available, if **TLS Authentication** is selected.
Mutual TLS authentication	The mutual certificate authentication. This option is available, if **TLS Authentication** is selected.

Button	Description
Add	Displays the Add Syslog Receiver dialog box where you can add the Syslog server configuration.
Edit	Displays the Add Syslog Receiver dialog box where you can edit the configuration of the selected Syslog server.
Delete	Deletes the selected Syslog server configuration.

Pushing system logs to Syslog servers

About this task

Use this procedure to a send log files to Syslog servers.

From Release 8.1, you can push more than one Syslog profiles to Syslog servers

Note:

The feature to push, view, and delete syslog server profile on virtual machine is supported only for AVP Utilities, System Manager (through Solution Deployment Manager Client), and Session Manager applications.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Host <host name> area, select an application.
4. Click **More Actions** > **Syslog config** > **Push**.
5. In the Push Syslog Configuration dialog box, select one or more Syslog profile, and click **Push**.

   The system sends the system log to the selected Syslog server.

Viewing configured Syslog servers

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Host <host name> area, select an application.
4. Click **More Actions** > **Syslog config** > **View**.
5. In the View Syslog Configuration dialog box, select the required Syslog profile to view it.

Deleting configured Syslog servers

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Host <host name> area, select an application.
4. Click **More Actions** > **Syslog config** > **Delete**.
5. In the Delete Syslog Configuration dialog box, select the required Syslog profile, and click **Delete**.
6. On the confirmation dialog box, click **Yes**.

Viewing the job history of virtual machine operations

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. On the desktop, click the SDM icon (), and then click **Application Management**.
3. In the lower pane, click **Job History**.
4. On the Job History page, in **Operation**, select one or more operations.
5. Click **Submit**.

   The page displays the details of jobs that you selected.

Related links

Job History field descriptions on page 1432

Application Management field descriptions

Name	Description
Auto-Reload Application Management Tree	The option to automatically reload Application Management Tree after completing an operation, such as refreshing applications.

Locations

Name	Description
Location Name	The location name.
City	The city where the platform is located.
Country	The country where the platform 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 platforms associated with the deleted locations to unknown location.

Platforms

Name	Description
Platform Name	The name of the platform.
Platform IP	The IP address of the platform.

Table continues…

Name	Description
Platform FQDN	The FQDN of the platform.
IPv6	The IPv6 address of the platform. If the IP address of the ESXi platform only supports IPv4, the column does not display any value.
vCenter FQDN	The FQDN of vCenter.
Current Action	The operation that is currently being performed on the platform.
Last Action	The last operation completed on the platform.
License Status	The status of the license.
Platform Version	The platform version.
Offer Type	The platform type. The options are: • **ASP**: An Avaya Solutions Platform 130 Release 5.1 platform. • **Customer VE**: A customer-provided VMware ESXi platform • **SWONLY**: A customer-provided operating system platform • **AVP**: An Appliance Virtualization Platform platform
SSH Status	The SSH service status. The values are enabled and disabled.
Platform Certificate Status	The certificate status of Appliance Virtualization Platform, Avaya Solutions Platform 130, or standalone ESXi. If the ESXi is managed by vCenter, the system displays the value of this field as NA. The options are: • ✔: The certificate is added in Solution Deployment Manager and is correct. • ✖: The certificate is not accepted or is invalid. You can click **View** for details of the certificate status.
vCenter Certificate Status	The certificate status of the ESXi host. The options are: • ✔: The certificate is correct. The system enables all the options in **More Actions** that apply to VMware ESXi host. • ✖: The certificate is not accepted or is invalid. You can click **View** for details of the certificate status.

Note:

Depending on the Appliance Virtualization Platform, Avaya Solutions Platform 130, standalone ESXi, and vCenter certificate status, the system enables the options in **More Actions**.

Button	Description
Auto Refresh	Automatically refreshes the page with the latest changes. For example, the page updates: • The Application state when an application changes. • The license status or certificate status of the platform when the platform changes. The system refreshes the data every minute.
Add	Displays the **Add Platform** section where you can provide the details of the platform that you want to add.
Edit	Displays the Platform Information section where you can change the details of an existing platform.
Remove	Removes the platforms that you select only from the Solution Deployment Manager client. The system moves the platforms associated with the deleted locations to an unknown location.
Change Network Params > **Change Host IP Settings**	Displays the Host Network/IP Settings section where you can change the host IP settings for the Appliance Virtualization Platform host.
Change Network Params > **Change Network Settings**	Displays the Host Network Setting section where you can change the network settings for the Appliance Virtualization Platform host.
Refresh Host	Refreshes one or more of the platforms. Solution Deployment Manager displays the following status in the **Current Action** column. • **Refresh Completed**: When the refresh platform action completes. • **Refresh Failed**: When the refresh platform action fails if Solution Deployment Manager is unable to communicate with the platform. • **Refresh Queued**: When the refresh platform action takes time.
More Actions > **AVP Update/ Upgrade Management**	Displays the Update host page where you can provide the Appliance Virtualization Platform patch file for updating the Appliance Virtualization Platform host.
More Actions > **Change Password**	Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host.
More Actions > **SSH** > **Enable SSH**	Enables SSH for the Appliance Virtualization Platform 8.x or earlier and Avaya Solutions Platform 130 Release 5.1 hosts.
More Actions > **SSH** > **Disable SSH**	Disables SSH on the Appliance Virtualization Platform 8.x or earlier and Avaya Solutions Platform 130 Release 5.1 hosts.
More Actions > **Syslog config** > **Push**	Displays the Push Syslog Configuration section where you can push the syslog configuration on the application host. Syslog is only for Appliance Virtualization Platform. You can select multiple platforms and Push syslog configuration on selected platforms.

Table continues…

Button	Description
More Actions > **Syslog config** > **View**	Displays the View Syslog Configuration section where you can view syslog profiles of selected Appliance Virtualization Platform platforms.
More Actions > **Syslog config** > **Delete**	Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.
More Actions > **Lifecycle Actions** > **Host Restart**	Restarts the platform and applications that are running on the Appliance Virtualization Platform host.
More Actions > **Lifecycle Actions** > **Host Shutdown**	Shuts down the platform and applications that are running on the Appliance Virtualization Platform host.
More Actions > **Generate/ Accept Certificate**	Displays the Certificate dialog box where you can manage certificates for the platform. Depending on the platform type, the options are: • **Generate Certificate**: To generate a certificate for the Appliance Virtualization Platform 8.x or earlier and Avaya Solutions Platform 130 Release 5.1 hosts. • **Accept Certificate**: To accept a valid certificate for the platform or vCenter. • **Decline Certificate**: To decline the certificate for the Appliance Virtualization Platform 8.x or earlier and Avaya Solutions Platform 130 Release 5.1 hosts. You must regenerate the certificate and accept if you decline a platform certificate.
More Actions > **AVP Cert. Management** > **Manage Certificate**	Displays the Load Certificate dialog box from where you can view/ generate certificates for Appliance Virtualization Platform hosts, and download them. You can also upload and push third-party signed certificates to the selected platform.
More Actions > **AVP Cert. Management** > **Generic CSR**	Displays the Create/Edit CSR dialog box from where you create or edit the generic CSR data.
More Actions > **Snapshot Manager**	Displays the Snapshot Manager dialog box from where you can view and delete the application snapshot.
More Actions > **WebLM Configuration**	Displays the WebLM Configuration dialog box from where you configure WebLM Server for an Appliance Virtualization Platform host.
More Actions > **AVP Firewall Rules**	Displays the Firewall Settings dialog box from where you can view the firewall rules details for an Appliance Virtualization Platform host.
More Actions > **Set Login Banner**	Displays the Message of the Day dialog box from where you can push the login banner text to the selected platform. **Note:** This feature is only available in System Manager Solution Deployment Manager. Solution Deployment Manager Client does not support **Set Login Banner**.

Applications

Name	Description
Application Name	The name of the application.
Application IP	The IP address of the application.
Application FQDN	The FQDN of the application.
Application IPv6	The IPv6 address of the application, if any.
App Name	The name of the application. For example, Session Manager.
App Version	The version of the application. For example, 8.1.
Application State	The state of the application. The states are: • **Started** • **Stopped**
Current Action Status	The status of the current operation. The options are: • **Deploying** • **Starting** • **Stopping** The **Status Details** link provides the details of the operation in progress.
Last Action	The last action performed on the application.
Platform Name	The platform name of the operating system, VMware host, or Appliance Virtualization Platform host on which the application resides.
Platform Type	The platform type of the operating system.
Trust Status	The status of the connection between System Manager and the application. The options are: • **Success** • **Failed** When the connection between System Manager and the application is established, **Trust Status** changes to **Success**. Only when the trust status is **Success**, you can perform other operations.
Data Store	The data store name.

Button	Description
New	Displays the Application Deployment section where you can provide the platform and deploy an application.
Edit	Displays the Application Deployment section where you can change the details of an application.
Delete	Turns off the applications and deletes the selected application from platform and Solution Deployment Manager Client.

Table continues…

Button	Description
Start	Starts the selected applications.
Stop	Stops the selected applications.
Show Selected	Displays only the selected applications.
VM Console > **Open VM Console in New Window**	Opens the application VM console in the new browser window.
VM Console > **Open VM Console in New Tab**	Opens the application VM console in the new tab of the browser.
More Actions > **Restart**	Starts the selected applications that were stopped earlier.
More Actions > **Refresh App**	Updates the status of the applications.
More Actions > **Re-establish connection**	Establishes the connection between System Manager and the application. The **Trust Status** then changes to **Success**.
More Actions > **Update Static Routing**	Displays the VM Update Static Routing section where you can update the IP address of AVP Utilities for static routing.
More Actions > **Syslog config** > **Push**	Displays the Push Syslog Configuration section where you can push the syslog configuration on the selected application.
More Actions > **Syslog config** > **View**	Displays the View Syslog Configuration section where you can view all configured syslog profiles.
More Actions > **Syslog config** > **Delete**	Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.

Job History field descriptions

Name/Button	Description
Operation	The operation that is performed on a virtual machine. You can select one or more operations that are performed on a virtual machine, such as host restart, virtual machine deployment, and patch installation.
Submit	Provides details of jobs that you selected.

History

Name	Description
Job ID	The unique name of the virtual machine management job.
IP/FQDN	The IP address or host name of the virtual machine or the host where the operation is performed.
Operation	The operation performed on the virtual machine or host. For example, host refresh, virtual machine deployment, and patch installation.
Status	The status of the job.
Start Time	The start time of the job.
End Time	The end time of the job.

Upgrading Avaya Aura® applications

Upgrade Management overview

Upgrade Management in Solution Deployment Manager is a centralized upgrade solution of System Manager, provides an automatic upgrade of Avaya Aura® applications. You can upgrade Communication Manager, Session Manager, and Branch Session Manager directly to Release 10.2.x from a single view. Communication Manager includes associated devices, such as Gateways, and media modules. The centralized upgrade process minimizes repetitive tasks and reduces the error rate.

Important:

Ensure that upgrade or update of host should not be simultaneously run with upgrade and updates of application. You can check the Job status on the **Home** > **Services** > **Solution Deployment Manager** > **Upgrade Jobs Status** page. Any scheduled, pending, or running jobs for host must be completed before performing upgrade or update operations on host.

With Upgrade Management, you can perform the following:

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 and media modules.
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.

   Note:

   In Geographic Redundancy configured System Manager, if Communication Manager or LSP has the **Unknown** status in the **Managed By** column on the **Inventory** > **Manage Elements** page, then you cannot perform the analyze operation. To change the **Unknown** status in the **Managed By** column to either **Primary** or **Secondary** depending upon from which system this action is performed, select the entry on the **Inventory** > **Manage Elements** page, and click **More Actions** > **Manage**.
3. Download files: To download files that are required for upgrading applications.

   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, checks whether:
   - The new release supports the hardware
   - The RAID battery is sufficient
   - The bandwidth is sufficient

Note:

You must have the minimum network speed of 2Mbps with up to 100ms delay (WAN).

- The files are downloaded

5. Upgrade applications: To upgrade Avaya Aura® applications to Release 10.2.x.
6. Install patches: To install the software patches, service packs, and feature pack, if applicable.

Upgrade automation level

- The upgrade of Communication Manager, Session Manager, and Branch Session Manager to Release 10.2.x is automated. The upgrade process includes creating a backup, deploying OVA, upgrading, installing software patches, feature packs, or service packs, and restoring the backup.
- Upgrade of all other Avaya Aura® applications that Solution Deployment Manager supports can automatically deploy OVA files.

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 applications combined together in an upgrade or update job is considered a group.
- 20 applications in a job group: Maximum applications that can be combined in an upgrade or update job group is 20. You can combine any application type for upgrade in a group.

The capacity also includes applications that are in the paused state. If five upgrade job groups are running or are 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 10.2.x:

- Communication Manager
- Session Manager
- Branch Session Manager

Note:

- You must upgrade System Manager to Release 10.2.x by using the Solution Deployment Manager client before you upgrade the Avaya Aura® applications to Release 10.2.x.
- When an application is deployed on a KVM host, Solution Deployment Manager does not support that application.

Related links

Guidelines for upgrading and updating elements on page 1435

Guidelines for upgrading and updating elements

Upgrading elements

For System Manager that is on the latest major release, to upgrade the elements to an intermediate element release, download the latest recommended major release of element OVA in the software library.

For example, for System Manager Release 10.1, to upgrade Communication Manager Release 8.x to Release 10.1, download Release 10.1 Communication Manager OVA in the software library.

Updating elements

For System Manager that is on the latest release patch, to upgrade the elements to an intermediate element patch release, download the latest recommended major release of element patch in the software library.

Related links

Avaya Aura applications upgrade on page 1434

Upgrade checklist for Avaya Aura® Virtual Appliance

This is a reference checklist for Virtual Appliance. For detailed steps, see the application specific upgrading guides.

From Release 10.1 and later, Appliance Virtualization Platform is no longer available for deploying or upgrading the Avaya Aura® applications. To upgrade the Avaya Aura® applications, migrate Appliance Virtualization Platform to Avaya Solutions Platform 130 (KVM on RHEL 8.10) Release 6.0.

Nos.	Tasks	Notes	✔
1	Download the OVA files, ISO files, and feature pack files of Avaya Aura® applications that you want to deploy or upgrade from the Avaya Support website at http://support.avaya.com. **Note:** For information about the upgrade sequence and the required patches, see the latest *Avaya Aura® Release Notes* for the specific release on the Avaya Support website.	-	
2	If you need to deploy or upgrade the System Manager, download the Solution Deployment Manager client.	-	
3	Install the Solution Deployment Manager client.	-	
4	To upgrade on an Avaya-provided server, use Solution Deployment Manager client for Appliance Virtualization Platform.	-	

Table continues…

Nos.	Tasks	Notes	✔
5	If System Manager is: • Unavailable: On Appliance Virtualization Platform, deploy the System Manager OVA file, and install the latest bin file by using the Solution Deployment Manager client. • Available: Upgrade System Manager and install the bin file.	-	
6	Discover the applications and associated devices that you want to upgrade by enabling SNMP or manually add the elements from **Manage Elements** > **Discovery**.	For more information, see “Discovering elements” in *Administering Avaya Aura® System Manager*	
7	Configure user settings.	For more information, see “User settings” in *Administering Avaya Aura® System Manager*	
8	Use a local System Manager library or create a remote software library. **Note:** For local, the software local library for media gateway upgrades is not supported.	For more information, see “User settings” in *Administering Avaya Aura® System Manager*	
9	Refresh the elements in the inventory.	For more information, see “Refreshing elements” in *Administering Avaya Aura® System Manager*	
10	Analyze the software.	For more information, see “Analyzing software” in *Administering Avaya Aura® System Manager*	
11	Perform the preupgrade check.	For more information, see “Performing the preupgrade check” in *Administering Avaya Aura® System Manager*	
12	Download the required firmware for the Avaya Aura® application upgrade.	For more information, see “Downloading the software” in *Administering Avaya Aura® System Manager*	
13	Perform the upgrade.	-	
14	Verify that the upgrade is successful.	-	

Upgrade target release selection

By default, the target version is set to **SMGR 7.x Onwards**.

All elements will be upgraded to Release 7.x and later releases using the Upgrade Management page.

Related links

Selecting the target release for upgrade on page 1437

Selecting the target release for upgrade

About this task

Use the following procedure to upgrade applications to Release 7.0 or later.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 7.x Onwards**.

   By default, the target version is set to **SMGR 7.x Onwards**.

   Important:

   Do not select the **SMGR 6.3.8** option for upgrading the application.
4. Click **Commit**.
5. Click **OK**.
6. To perform the upgrade, click **Upgrade Management**.

Related links

Upgrade target release selection on page 1436

Installing software patches by using Solution Deployment Manager

About this task

Use the procedure to install software patches and service packs that are entitled for an Avaya Aura® application, and commit the patches that you installed.

Note:

- When you are installing an element patch and the patch installation fails or the patch information is unavailable in **Upgrade Actions** > **Installed Patches** on the Upgrade Management page, then perform the following:
  1. Ensure that the element is reachable on System Manager Solution Deployment Manager.
  2. Refresh the element.

Before you begin

- Perform refresh and analyze operations.

- If you upgrade an application that was not deployed from Solution Deployment Manager:
  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 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 **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.

   Note:

   If an application is unreachable, the auto commit operation might fail and the Update Patch Status window displays a warning message. You must wait for some time, select the same patch in the Installed Patches section, and perform the commit operation again.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. Click **Save**.
11. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

    If the field displays , review the information on the Edit Upgrade Configuration page.
12. Click **Upgrade**.
13. 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.
14. Click **Schedule**.

    On the Upgrade Management page, the **Update status** and **Last Action Status** fields display .
15. 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 ✓.

16. Click **Upgrade Actions** > **Installed Patches**.
17. 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.
18. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

    You can schedule to commit the patch at a later time by using the **Schedule later** option.
19. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.
20. Ensure that **Update status** and **Last Action Status** fields display ✓.

    Note:

    If the patch commit fails or auto commit is not executed even after 24 hours, delete the snapshot that are not required. For information about deleting the virtual machine snapshot from host, see “Deleting the virtual machine snapshot”.

Installing custom software patches

About this task

The custom patching option is for advanced administrators so that they can fully control the installation of hot fixes, patches, service pack, and feature packs.

While installing custom patches, you do not need to perform the analyze and preupgrade check options that are available under **Pre-upgrade Actions** on the Upgrade Management page. Performing the preupgrade check while using Custom patches will result in a failure.

Use this procedure to install a single software file, such as software patch, service pack, or a feature pack to an Avaya Aura® application.

You can install custom patches for the following Avaya Aura® applications:

- Communication Manager
- Session Manager
- Branch Session Manager
- Utility Services
- Communication Manager Messaging
- WebLM
- Application Enablement Services

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions** > **Custom Patching**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. In the End User License Agreement section, click **I Agree to the above end user license agreement**.
11. Click **Save**.
12. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

    If the field displays , review the information on the Edit Upgrade Configuration page.
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 later time by using the **Schedule later** option.

20. Click **Schedule**.

    The Upgrade Management page displays the last action as **Commit**.

21. Ensure that **Update status** and **Last Action Status** fields display ✅.

    Note:

    If the patch commit fails or auto commit is not executed even after 24 hours, delete the snapshot that are not required. For information about deleting the virtual machine snapshot from host, see “Deleting the virtual machine snapshot”.

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.
Patch Type	The type of the software patch. The options are: • service pack or feature pack or software patch • Security
Patch State	The state of the software patch. The options are: • Active (when patch is activated) • Installed (when patch is unpacked) • Pending (when patch is pending a commit)

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.

Table continues…

Name	Description
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** > **Communication Manager**.
Sub-Type	The sub type of the device. For example, **TN2302AP** > **Communication Manager simplex**.
IP Address	The IP address of the device.

Table continues…

Name	Description
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.
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.
VM 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/ Update**	Displays the Upgrade Configuration page where you can configure the details of an upgrade or patch installation.
Upgrade Actions > **Commit/ Rollback Upgrade**	Displays the Job Schedule page where you can run the upgrade job immediately or schedule it.
Upgrade Actions > **Installed 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 > **Custom Patching**	Displays the Upgrade Configuration page where you configure the custom patch details. You can then install and commit the custom patch.
Upgrade Actions > **Cleanup**	Clears the current pending or pause state of applications. The system displays a message to check if Appliance Virtualization Platform is already installed for the same-server migration. If Appliance Virtualization Platform is already installed, you must cancel the cleanup operation and continue with the upgrade. If you continue the cleanup, the system clears the states, and you can start the upgrade process again.
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 Platform host.
Download > **Download**	Displays the File Download Manager page with the list of downloaded software required for upgrade or update.
Download > **Bulk Import Spreadsheet**	Downloads the `Bulk_Import_Spreadsheet_Template.xlsx` file on your local computer.
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.

Table continues…

Name	Description
Type	The device type.
IP Address	The IP Address of the device.
Current 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**.
Override Delete VM on Upgrade Check	The option to override upgrade check recommendations. When you select this option, the system deletes the old virtual machine after the upgrade check.
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
Import Configuration(s)	Imports the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet. The system displays the Upload Xlsx File Configuration dialog box to upload the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet.
Save Configuration	Saves the upgrade configuration. **Note:** The system saves the configuration as a job. You can edit the job on the Upgrade Jobs Status page.
Upgrade	Commits the upgrade operation.

Edit Upgrade Configuration field descriptions

Edit Upgrade Configuration has following tabs:

- **Element Configuration**
- **AVP Configuration**

Element Configuration: General Configuration Details

Name	Description
System	The system name.

Table continues…

Name	Description
IP Address	The IP address of the device.
Operation	The operation that you want to perform on the device. The options are: • Upgrade/Migration • Update
ESXI/AVP host/Platform	The host on which you want to run the device. The options are: • Same Box • Software Only • List of hosts that you added from Application Management
New Target ESXI/AVP host/ Platform	The new target host on which you want to run the device.
Migrate With AVP Install	The option to migrate System Platform-based Communication Manager Release 6.3.x or 6.4.x to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager.
Upgrade Source	The source where the installation files are available. The options are: • SMGR_DEFAULT_LOCAL • Remote Software Library
Upgrade To	The 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.
Service/Feature Pack for auto-install after upgrade/ migration	The service pack or feature pack that you want to install.

Element Configuration: Upgrade Configuration Details

The page displays the following fields when you upgrade application 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
Existing Administrative User	The user name with appropriate admin 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.
Hostname	The IP address of the virtual machine.

Table continues…

Name	Description
DNS Search Path	The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).
Password for cust	The password of the cust user.
Password for root	The password of the root user.
Timezone	The timezone of the virtual machine.
NTP server(s)	The IP Address or FQDN of the NTP server. Separate the IP addresses with commas (,). The application supports only the NTP server. It does not support the NTP pool.
EASG User Access	**Enable: (Recommended)** `By enabling Avaya Logins you are granting Avaya access to your system.` `This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.` `In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.` **Disable** `By disabling Avaya Logins you are preventing Avaya access to your system.` `This is not recommended, as it impacts Avaya's ability to provide support for the product.` `Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.` Enter 1 to Enable EASG (Recommended) or 2 to **Disable** EASG.
Default Gateway	The default gateway of the virtual machine.
DNS Servers	The DNS IP address of the virtual machine.
Public IP Address	The IP Address of AE Services virtual machine.
Public Netmask	The network mask of AE Services virtual machine.
Private IP Address	This field is optional and can be configured to be used for private network.
Private Netmask	This field is optional, and can be configured to be used for private network.

Table continues…

Name	Description
Out of Band Management Netmask	The subnet mask of the virtual machine for out of band management.
Out of Band Management IP 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.
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	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.

Element Configuration: Data Encryption

Name	Description
Data Encryption	Enables or disables the data encryption. The options are: • **1**: To enable the data encryption. • **2**: To disable the data encryption. **Important:** • An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa. • While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to vCenter limitation. Therefore, ensure that you enter the encryption passphrase, if data encryption is enabled.

Table continues…

Name	Description
Encryption Pass-Phrase	This field is applicable when data encryption is enabled. The passphrase for data encryption. When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules. When you deploy the application by using vCenter or ESXi, the system does not apply the passphrase complexity rules.
Re-enter Encryption Pass-Phrase	The passphrase for data encryption.
Require Encryption Pass-Phrase at Boot-Time	If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default, the **Require Encryption Pass-Phrase at Boot-Time** check box is selected. **Important:** You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA. If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure. You can also set up the remote key server by using the `encryptionRemoteKey` command after the deployment of the application.

Element Configuration: End User License Agreement

Name	Description
I Agree to the above end user license agreement	The end user license agreement. You must select the check box to accept the license agreement.

AVP Configuration: Existing Machine Details

Name	Description
Source IP	The source IP address.
Source Administrative User	The source user name with appropriate admin privileges.

Table continues…

Name	Description
Source Administrative Password	The source password of the administrator.
Source Root User	The source user name with appropriate root privileges.
Source Root Password	The source password of the root.

AVP Configuration: Configuration Details

Name	Description
Upgrade Source	The source where the installation files are available. The options are: • SMGR_DEFAULT_LOCAL • Remote Software Library
Upgrade To	The 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 Configuration Details section.
Dual Stack Setup (with IPv4 and IPv6)	Enables or disables the fields to provide the IPv6 addresses. **Note:** IPv6 is only supported in a dual stack configuration.
AVP Management IPv4 Address	IPv4 address for the Appliance Virtualization Platform host.
AVP IPv4 Netmask	IPv4 subnet mask for the Appliance Virtualization Platform host.
AVP Gateway IPv4 Address	IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
AVP Hostname	Hostname for the Appliance Virtualization Platform host. The hostname: • Can contain alphanumeric characters and hyphen • Can start with an alphabetic or numeric character • Must contain at least 1 alphabetic character • Must end in an alphanumeric character • Must contain 1 to 63 characters
AVP Domain	Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the default value. Format is alphanumeric string dot separated. For example, mydomain.com.
IPv4 NTP server	IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com
Secondary IPv4 NTP Server	Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.

Table continues…

Name	Description
Main IPv4 DNS Server	Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.
Secondary IPv4 DNS server	Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.
AVP management IPv6 address	IPv6 address for the Appliance Virtualization Platform host.
AVP IPv6 prefix length	IPv6 subnet mask for the Appliance Virtualization Platform host.
AVP gateway IPv6 address	IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
IPv6 NTP server	IPv6 address or FQDN of customer NTP server.
Secondary IPv6 NTP server	Secondary IPv6 address or FQDN of customer NTP server.
Main IPv6 DNS server	Main IPv6 address of customer DNS server. One DNS server entry in each line.
Secondary IPv6 DNS server	Secondary IPv6 address of customer DNS server. One DNS server entry in each line.
Public vLAN ID (Used on S8300E only)	VLAN ID for the S8300E server. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use **Public VLAN ID** only on the S8300E server.
Enable Stricter Password (14 char pass length)	The check box to enable or disable the stricter password. The password must contain at least 14 characters.
AVP Super User Admin Password	Admin password for Appliance Virtualization Platform. The password must contain at least 8 characters and can include alphanumeric characters and @!$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.

Table continues…

Name	Description
Enhanced Access Security Gateway (EASG)	**Enable: (Recommended)** By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming. **Disable** By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled. Enter 1 to Enable EASG (Recommended) or 2 to **Disable** EASG.
WebLM IP/FQDN	The IP Address or FQDN of WebLM Server.
WebLM Port Number	The port number of WebLM Server. The default port is 52233.

Button	Description
Save	Saves the changes that you made to the Edit Upgrade Configuration page.
Cancel	Cancels the changes that you made to the Edit Upgrade Configuration page.

Uploading a custom patch

About this task

If the file size exceeds 300 MB, the upload operation fails.

Analyze works on the version of OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitle update or upgrade version, the version field must contain valid value. You can get the version values from versions files that are available on PLDS.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the left navigation pane, click **Download Manager**.

3. In **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**.
5. In the **Select Files Download Details** section, enter **My Computer**.
6. Click **Download**.
7. On the Upload File page, enter the details of the patch file you want to upload.
8. Click **Commit**.
9. On the Upload Remote Warning page, perform one of the following actions:
   - Click **Now** to upload the file to the remote software library.
   - Click **Schedule** to upload the file at the scheduled time.
   - Click **Cancel** to cancel the upload file operation and return to the previous page.

Uploading custom patch field descriptions

Name	Description
Software Library	The remote software library where you want to upload the custom patch file.
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.
File Version	The software file version that you want to upload. For example, OVA, service pack, and feature pack. Version number is mandatory if you are uploading files, such as OVA, service pack, and feature pack because analyze operation works on version number and the system might have to install the version of the file. Custom patching does not require the analyze operation, and therefore, the file version number is optional.
Hardware Compatibility	The hardware compatibility for the file you upload. For IP Office, this field can be null.
File Size (in bytes)	The file size of the patch file you want to upload.
File	The patch file you want to upload to the remote software library. Click **Choose File** to browse to the file you want to upload.

Button	Description
Commit	Click to go to the upload file scheduler page.
Cancel	Click to cancel the upload operation and return to the Download Manager page.

Rolling back to Utility Services

About this task

Use this procedure to rollback Utility Services to 7.x if the upgrade from Utility Services to AVP Utilities fails from Release 7.x to Release 8.1 and later.

Before you begin

- Add a location.
- Select Location and add a host.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Location<location name> section, select the Utility Services application, and click **More Actions** > **Rollback/Retry**.

   If the **Current Action Status** column displays the `VM Upgrade Failed` message, the system enables **More Actions** > **Rollback/Retry** after selecting the Utility Services application.
4. In the Import Configuration Excel File dialog box, click **Rollback**.

   To upgrade Utility Services to AVP Utilities, use the Upgrade Management page of System Manager Solution Deployment Manager.

   The system displays the confirmation message to accept the rollback.

Retrying Utility Services to AVP Utilities upgrade

About this task

If the upgrade from Utility Services to AVP Utilities fails, use this procedure to retry the upgrade of Utility Services to AVP Utilities.

Before you begin

- Add a location.
- Select Location and add a host.
- Download a copy of the `hostUSUpgradeInfo.xlsx` spreadsheet from Avaya PLDS website at https://plds.avaya.com/or from Avaya Support website at https://support.avaya.com. Fill the required system details in the spreadsheet.

  Note:

  If you provide the incorrect data in the spreadsheet, the upgrade might fail.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.

2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Location<location name> section, select the Utility Services application, and click **More Actions** > **Rollback/Retry**.

   If the **Current Action Status** column displays the `VM Upgrade Failed` message, the system enables **More Actions** > **Rollback/Retry** after selecting the Utility Services application.
4. On the Import Configuration Excel File dialog box, do the following:
   a. Click **Browse** and select the file from the local computer.
   b. To upload the spreadsheet, click **Open**.

      The system displays the file size and percentage complete for the uploaded file. When the file upload is in-progress, do not navigate away from the page.
   c. Click **Submit File**.

      Once the file is successfully uploaded, the system enables the **Retry** button.
   d. Click **Retry**.

      The system starts the upgrade of Utility Services to AVP Utilities.

Upgrading Branch Session Manager instances in bulk

Downloading the bulk import spreadsheet template

About this task

Use the following procedure to download the `Bulk_Import_Spreadsheet_Template.xlsx` file.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, click **Download** > **Bulk Import Spreadsheet**.

   The system downloads the `Bulk_Import_Spreadsheet_Template.xlsx` file on your local computer.

Filling the bulk import spreadsheet for upgrading Branch Session Manager instances in bulk

Before you begin

- Download a copy of the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet. For information, see “Downloading the bulk import spreadsheet template”.

Procedure

1. On the **Element Info** sheet, do the following:
   a. In **SP/AVP/ESXi IP Address**, type the host IP Address of Branch Session Manager.

      This field supports the AVP and ESXi platforms.
   b. In **Element Type**, type `BSM`.
   c. In **Element IP Address**, type the IP Address of Branch Session Manager.
   d. In **Operation**, type `Upgrade/Migration`.
   e. In **ESXi/AVP host**, type the host IP Address of Branch Session Manager.

      The value of the field must match with **SP/AVP/ESXi IP Address**.
   f. In **Migrate with AVP Install**, type `false`.

      For Branch Session Manager, migration is not applicable.
   g. In **Upgrade Source**, type `SMGR_DEFAULT_LOCAL`.
   h. In **Upgrade To**, type the upgrade version of Branch Session Manager OVA.

      For example: `BSM-8.1.0.0.xxxxxx-exx-0x.ova`.
   i. In **EULA**, type `true`.
   j. **(Optional)** In **ESXi/AVP New**, type the host IP Address of AVP or ESXi.

      This field is not applicable for the same host upgrade. If you want to migrate from one AVP or ESXi host to the other, you must fill the following fields on the **BSM_Prepopulate_Data** sheet:

      - **New ESXi datacentre**
      - **New ESXi datastore**
      - **New ESXi deployment type**

      ESXi/AVP New host IP on the AVP_VM_MAPPING sheet.
2. On the **AVP_Info** sheet, do the following:
   a. In **SP/AVP/ESXi IP Address**, type the IP Address of AVP or ESXi host.

      You can also fill the new ESXi host here.
   b. In **Source IP**, type the IP Address of the Appliance Virtualization Platform.
   c. In **Upgrade Source**, type the source where the installation files are available.

      The options are:

      - `SMGR_DEFAULT_LOCAL`
      - `Remote Software Library`
   d. In **Upgrade To**, type the OVA file name to which you want to upgrade.

e. In **Dual Stack Setup (with IPv4 and IPv6)**, enable or disable the fields to provide the IPv6 addresses.

   The options are:

   - **true**: To enable the encryption pass-phrase at boot-time.
   - **false**: To disable the encryption pass-phrase at boot-time.

f. In **EASG**, type `1` to enable the EASG.

g. In **WebLM Port Number**, type the port number of WebLM Server.

   The default port is `52233`.

h. In **EULA**, type `true`.

3. On the **CM_Prepopulate_Data** sheet, do the following:

   a. In **SP/AVP/ESXi IP Address**, type the IP Address of AVP or ESXi host.

      You can also fill the new ESXi host here.

   b. In **Element IP Address**, type the IP Address of Communication Manager.

   c. In **NTP Server(s)**, type the IP address or FQDN of the NTP server.

      Separate the IP addresses with commas (,). You can type up to three NTP servers.

   d. In **Search Domain List**, type the search list of domain names.

      For example, mydomain.com. Separate the search list names with commas (,).

   e. In **EASG**, type `1` to enable the EASG.

   f. In **Flexi Footprint**, type the footprint of Communication Manager.

      For example, CM Main Max users 1,000.

   g. **(Optional)** In **Customer Root Account Password**, type the customer root password.

      This field is only applicable for DOD build.

      Note:

      In **Data Encryption**, type `1` to enable. Fill the encryption pass-phrase and type `true` for encryption pass-phrase at boot-time.

4. On the **US_Prepopulate_Data** sheet, do the following:

   a. In **SP/AVP/ESXi IP Address**, type the host IP Address of Utility Services.

   b. In **Element IP Address**, type the IP Address of Utility Services.

   c. In **Primary WebLM IP address for Licensing**, type the IP Address or FQDN of WebLM Server.

   d. In **OOBM Mode**, select the Out of Band Management mode in which you want to deploy.

The options are:

- **OOBM_Enabled**: To enable Out of Band Management.
- **OOBM_Disabled**: To disable Out of Band Management

e. In **EASG**, type `1` to enable the EASG.

f. **(Optional)** In **Customer Root Account Password**, type the customer root password.

This field is only applicable for DOD build.

Note:

In **Data Encryption**, type `1` to enable. Fill the encryption pass-phrase and type `true` for encryption pass-phrase at boot-time.

5. On the **BSM_Prepopulate_Data** sheet, do the following:

a. In **SP/AVP/ESXi IP Address**, type the host IP Address of Branch Session Manager.

b. In **Search Domain List**, type `platform.avaya.com`.

c. In **LSP IP**, type the Communication Manager IP Address.

d. In **EASG User Access**, type `1` to enable the EASG.

e. In **Flexi Footprint**, type the footprint of Branch Session Manager.

For example, BSM Profile 1 Max Devices 1,000.

f. **(Optional)** In **Customer Root Account Password**, type the customer root password.

This field is only applicable for DOD build.

Note:

In **Data Encryption**, type `1` to enable. Fill the encryption pass-phrase and type `true` for encryption pass-phrase at boot-time.

6. On the **AVP_VM_MAPPING** sheet, do the following:

a. In **AVP/ESXi IP Address**, type the IP Address of the AVP or ESXi host.

You can also fill the new ESXi host here.

b. In **Authentication Type**, type `SSO` or `LOCAL`.

c. In **PSC URL**, type FQDN of PSC.

7. Save the values in the sheet.

Related links

Downloading the bulk import spreadsheet template on page 1455

Sample scenario for filling AVP Bulk Import Spreadsheet Template

Example

SP IP Address is a primary key that is common in all sub sheets. Let us consider the following element details for Setup 1 Avaya Aura® System Platform LSP in Figure 1:

	SP-1	Dom-0	CM (LSP)	US	BSM
IP	148.147.162.100	148.147.162.99	148.147.162.101	148.147.162.102	148.147.162.103
FQDN			spcm.smgrdev.avaya.com	spus.smgrdev.avaya.com	sidtsm2.smgrdev.avaya.com
					SIP:148.147.162.104

Figure 3: Figure 1. Setup 1 – Avaya Aura® System Platform LSP

The corresponding mapping information of Setup 1 in Element_Info sub sheet is shown in Figure 2:

SP IP Address	Elem	Element IP Ad	Operation	ESXI/	Mig	Upgrade Source	Upgrade To
148.147.162.100	CM	148.147.162.101	Upgrade/Migrat	Same Bo	true	SMGR_DEFAULT_L	CM-Simplex-07.1.0.0.532-e65-0.ova
148.147.162.100	US	148.147.162.102	Upgrade/Migrat	Same Bo	true	SMGR_DEFAULT_L	US-7.1.0.0.0.18-e55-379_OVF10.ova
148.147.162.100	BSM	148.147.162.103	Upgrade/Migrat	Same Bo	true	SMGR_DEFAULT_L	BSM-7.1.0.0.710028-e65-01.ova

Figure 4: Figure 2. Setup 1 – Element_Info sub sheet

The corresponding mapping information of Setup 1 in AVP_Info sub sheet is shown in Figure 3:

SP IP Address	Source IP	Source	Source A	Sour	Source	Upgrade Source	Upgrade To
148.147.162.100	148.147.162.99	admin	admin01	root	root01	SMGR_DEFAULT_L	avaya-avp-7.1.2.0.0.07.iso

Figure 5: Figure 3. Setup 1 – AVP_Info sub sheet

Note:

For Avaya Aura® System Platform, the **Source IP** and **AVP_Mgmt_IPv4_Address** is the same as **Dom–0 IP**, which is assigned to the target Appliance Virtualization Platform IP after installation.

The corresponding mapping information of Setup 1 in CM_Prepopulate_Data sub sheet is shown in Figure 4:

SP IP Address	Element IP Address	CM IPv4 Address	CM IPv4 Netmask	CM IPv4 Gateway
148.147.162.100	148.147.162.101	148.147.162.101	255.255.255.0	148.147.162.1

Figure 6: Figure 4. Setup 1 – CM_Prepopulate_Data sub sheet

Note:

The values added in the **Element IP Address** and **CM IPv4 Address** columns in the above image must be the same as the **Element IP Address** of CM (LSP) in the Figure 1.

The corresponding mapping information of Setup 1 in US_Prepopulate_Data sub sheet is shown in Figure 5:

SP IP Address	Element IP Ad	Hostname	Public IP Addre	Public Netma	Public Default
148.147.162.100	148.147.162.102	us	148.147.162.102	255.255.255.0	148.147.162.1

Figure 7: Figure 5. Setup 1 – US_Prepopulate_Data sub sheet

Note:

The values added in the **Element IP Address** and **Public IP Address** columns in the above image must be the same as the **Element IP Address** of US in the Figure 1.

The corresponding mapping information of Setup 1 in BSM_Prepopulate_Data sub sheet is shown in Figure 6:

SP IP Address	Element IP Ad	Short H	Network Domain	IPv4 Address	Netmask	Default gate
148.147.162.100	148.147.162.103	sidtsm1	smgrdev.avaya.com	148.147.162.103	255.255.255.0	148.147.162.1

Figure 8: Figure 6. Setup 1 – BSM_Prepopulate_Data sub sheet

The values added in the **Element IP Address** and **IPv4 Address** columns in the above image must be the same as the **Element IP Address** of BSM in the Figure 1.

A sample scenario for Setup 2 (Avaya Aura® System Platform) CM Simplex Main:

	Setup-3 (Bare Metal 5.2.1) LSP				
	SP-3	Dom0	CM	US	BSM
IP	NA	NA	148.147.162.301	NA	NA

Figure 9: Figure 7. Setup 2 – (Avaya Aura® System Platform) CM Simplex Main

Note:

For CM Simplex Main, there is no mapping entry in BSM_Prepopulate_Data sub sheet.

A sample scenario for Setup 3 (Bare Metal) 5.2.1 LSP in Figure 8:

	Setup-3 (Bare Metal 5.2.1) LSP				
	SP-3	Dom0	CM	US	BSM
IP	NA	NA	148.147.162.301	NA	NA

Figure 10: Figure 8. Setup 3 – (Bare Metal) 5.2.1 LSP

Note:

1. In Element_Info sub sheet, the **SP IP Address** mentioned in column is NA for Bare Metal 5.2.1.
2. In AVP_Info sub sheet, the **Source IP** is the LSP IP Address. You need to provide a new IP Address for **AVP_Mgmt_IPv4_Address**, which is assigned to the target Appliance Virtualization Platform Host after installation.
3. In CM_Prepopulate_Data sub sheet, the **SP IP Address** mentioned in column is NA for Bare Metal 5.2.1.
4. US_Prepopulate_Data sub sheet and BSM_Prepopulate_Data sub sheet do not have any mapping entry for Bare Metal 5.2.1 LSP.

Note:

This information is applicable only if you are migrating to Release 7.1.2 and higher.

Upgrading Branch Session Manager instances in bulk by using System Manager Solution Deployment Manager

Before you begin

- On the Manage Elements page, add Branch Session Manager instances. For information about adding a new element, see *Administering Avaya Aura® System Manager*.
- Refresh the element.

- Analyze the software.
- Perform the pre-upgrade check.
- Download a copy of the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet. For information, see “Downloading the bulk import spreadsheet template”.
- Fill the required system details in the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet.

Note:

If you provide the incorrect data in the spreadsheet, the upgrade might fail.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, select Branch Session Manager instances.
4. Click **Upgrade Actions** > **Upgrade/Update**.
5. On the Upgrade Configuration page, click **Bulk Import Configuration(s)**.
6. On the Upload Xlsx File Configuration dialog box, perform the following:
   a. Click **Browse** and select the file from the local computer.
   b. To upload the spreadsheet, click **Upload**.
   c. When the spreadsheet upload is 100%, click **Submit**.

      The system displays the file size, timestamp, and percentage complete for the uploaded file. When the file upload is in-progress, do not navigate away from the page.

      On the Upgrade Management page, the system displays the message: `Please Wait - Saving Import Excel Sheet Configuration ....` You must wait until the system stops showing this message.
7. On the Upgrade Management page, click .

   The **Configuration Status** column displays .
8. To save the configuration, click **Save Configuration**.

   The update configuration is saved as a job in the Upgrade Jobs Status page.
9. On the Upgrade Configuration page, click **Upgrade**.
10. To view the upgrade status, perform the following:
    a. In the navigation pane, click **Upgrade Job Status**.
    b. In the **Job Type** field, click **Upgrade**.
    c. Click the upgrade job that you want to view.
11. On the Upgrade Management page, click .

The **Last Action** column displays **Upgrade**, and **Last Action Status** column displays ✓.

System Manager upgrade management

Upgrade Management field descriptions

Upgrade Elements

Name	Description
SMGR Name	System Manager name.
IP/FQDN	The IP address or the FQDN of System Manager virtual machine.
C-DOM IP/FQDN	The IP address or the FQDN of console domain.
Element Type	The type of the element.
Current Version	The current version of the element.
Upgrade To Version	The upgrade to version for the element.
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.
Related VM	The associated virtual machine.

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.
Commit	Saves the changes and upgrades the System Manager virtual machine.
Rollback	Reverts the upgrade of the System Manager virtual machine.

Add Element field descriptions

System Platform: Required C-DOM information

Name	Description
C-DOM IP/FQDN	The C-DOM IP/FQDN.

Table continues…

Name	Description
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.

Virtual Machine Platform (6.x): Required Host/VM Details Information

Name	Description
Hosts	The host of the virtual machine.
Virtual machines	The virtual machine.

System Platform/Virtual Machine Platform (6.x): Required Element Information

Name	Description
SMGR IP	The IP address of System Manager.
SMGR VM 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.

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 Host	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. **Note:** When upgrading from System Platform-based System Manager to AVP or ESXi, the system displays this field.
Platform FQDN	The platform FQDN to which you want to upgrade. The system displays the CPU and memory details of the platform in the Capacity Details section.
Application Name	The application name displayed on the Add Element page.

OVA/ISO Details

Name	Description
Select the OVA	The option to select a `.ova` file of the virtual machine that is available on System Manager.
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.
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 ✓.
SMGR Data migration Utility file	The absolute path to the System Manager data migration utility file. **Note:** Provide the latest data migration bin that is available for the System Manager release.

Table continues…

Name	Description
Service Pack or Feature Pack	The absolute path to the service pack or feature pack. For the latest service pack or feature pack, see Avaya Aura® Release Notes on the Avaya Support website at http://support.avaya.com/.

Configuration Parameters

The system populates the values for most of the fields from the 7.x or 8.0.x system. You must provide information, such as password, FQDN, time zone, and EASG.

Management Network Settings

Name	Description
Management IPv4 Address (or Out of Band Management IPv4 Address)	The IPv4 address of the System Manager application for Out of Band Management. This field is an 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 application.
Management Gateway	The gateway IPv4 address to assign to the System Manager application.
IP Address of DNS Server	The DNS IP addresses to assign to the primary, secondary, and other System Manager applications. Separate the IP addresses with commas (,).
Management FQDN	The FQDN to assign to the System Manager application. **Note:** System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.
IPv6 Address	The IPv6 address of the System Manager application for out of band management. This field is optional.
IPv6 Network prefix	The IPv6 subnetwork mask to assign to the System Manager application. This field is optional.
IPv6 Gateway	The gateway IPv6 address to assign to the System Manager application. This field is optional.
Default Search List	The search list of domain names. This field is optional.
NTP Server IP/FQDN	The IP address or FQDN of the NTP server. This field is optional. Separate the IP addresses with commas (,). This field is not applicable for software-only deployment. The application supports only the NTP server. It does not support the NTP pool.
Time Zone	The timezone where the System Manager application is located. A list is available where you select the name of the continent and the name of the country. This field is not applicable for the software-only deployment.

Public Network Settings

Name	Description
Public IP Address	The IPv4 address to enable public access to different interfaces. The field is optional.
Public Netmask	The IPv4 subnetwork mask to assign to System Manager application. The field is optional.
Public Gateway	The gateway IPv4 address to assign to the System Manager application. The field is optional.
Public FQDN	The FQDN to assign to the System Manager application. The field is optional.
Public IPv6 Address	The IPv6 address to enable public access to different interfaces. The field is optional.
Public IPv6 Network Prefix	The IPv6 subnetwork mask to assign to System Manager application. The field is optional.
Public IPv6 Gateway	The gateway IPv6 address to assign to the System Manager application. The field is optional.

Virtual FQDN

Name	Description
Virtual Hostname	The virtual hostname of the System Manager application. **Note:** • The VFQDN value must be unique and different from the FQDN value of System Manager and the elements. • VFQDN is a mandatory field. • By default, VFQDN entry gets added in the `/etc/hosts` file during installation. Do not remove VFQDN entry from the `/etc/hosts` file. • VFQDN entry will be below FQDN entry and mapped with IP address of system. Do not manually change the order and value. • You must keep VFQDN domain value same as of FQDN domain value. • If required, VFQDN value can be added in DNS configuration, ensure that the value can be resolved. • Secondary Server (Standby mode) IP address value is mapped with VFQDN value in hosts file of Primary server IP address. After Secondary Server is activated, then the IP address gets updated with Secondary Server IP address. • In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN. • After System Manager installation, if you require to change the System Manager VFQDN value, perform the following: 1. Log in to System Manager with administrator privilege credentials. 2. Run the **`changeVFQDN`** command. **Important:** When you run the **`changeVFQDN`** command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.
Virtual Domain	The virtual domain name of the System Manager application.

Name	Description
SNMPv3 User Name Prefix	The prefix for SNMPv3 user.

Table continues…

Name	Description
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.

SMGR CLI USER

Name	Description
SMGR command line user name	The user name of the System Manager CLI user. **Note:** Do not provide the common user names, such as admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel.
SMGR command line user password	The password for the System Manager CLI user.
Confirm Password	The password that you retype to confirm the System Manager CLI user authentication.

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.

Table continues…

Name	Description
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. If there is no successful backup in the last ‘n’ days, where ‘n’ is configurable, then System Manager raises an alarm. The default number of days is set to 7, but it can be configured to any number from 1 to 30 using the 'Alarm Threshold for number of days since last successful SMGR Backup' parameter.
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.
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 six 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.

Enhanced Access Security Gateway (EASG) - EASG User Access

Name	Description
Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG	Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks. The options are: • 1: To enable EASG. • 2: To disable EASG. Avaya recommends that you enable EASG. You can also enable EASG after deploying or upgrading the application using the command: **`EASGManage --enableEASG`**.

Customer Root Account

Note:

The **Customer Root Account** field is applicable only in case of deploying application OVA on Appliance Virtualization Platform Release 8.x or earlier, Avaya Solutions Platform 130, and VMware by using Solution Deployment Manager. The system does not display the **Customer Root Account** field, when you deploy an application:

- OVA on VMware by using vSphere Client (HTML5).
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

Name	Description
Enable Customer Root Account for this Application	Enables or disables the customer root account for the application. Displays the ROOT ACCESS ACCEPTANCE STATEMENT screen. To accept the root access, click **Accept**. When you accept the root access statement, the system displays the **Customer Root Password** and **Re-enter Customer Root Password** fields.
Customer Root Password	The root password for the application
Re-enter Customer Root Password	The root password for the application

Data Encryption

Note:

Data Encryption is supported only for Appliance Virtualization Platform Release 8.x or earlier, Avaya Solutions Platform 130, and VMware Virtualized Environment.

For more information, see the application-specific Data Privacy Guidelines on the Avaya Support website.

Name	Description
Data Encryption	Enables or disables the data encryption. The options are: • **1**: To enable the data encryption. • **2**: To disable the data encryption. **Important:** • An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa. • While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to vCenter limitation. Therefore, ensure that you enter the encryption passphrase, if data encryption is enabled. • **On Solution Deployment Manager:** When the **Data Encryption** field is set to 1, the system enables the **Encryption Pass-Phrase** and **Re-enter Encryption Pass-Phrase** fields to enter the encryption passphrase. • **On vCenter or ESXi:** When the **Data Encryption** field is set to 1, enter the encryption passphrase in the **Password** and **Confirm Password** fields.
Encryption Pass-Phrase	This field is applicable when data encryption is enabled. The passphrase for data encryption. When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules. When you deploy the application by using vCenter or ESXi, the system does not apply the passphrase complexity rules.
Re-enter Encryption Pass-Phrase	The passphrase for data encryption.

Table continues…

Name	Description
Require Encryption Pass-Phrase at Boot-Time	If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default, the **Require Encryption Pass-Phrase at Boot-Time** check box is selected. **Important:** You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA. If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure. You can also set up the remote key server by using the `encryptionRemoteKey` command after the deployment of the application.

Network Parameters

Name	Description
Out of Band Management IP Address	The IP Address 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. To accept EULA and start the upgrade process, click **Accept**.

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. Log on to the System Manager web console.
2. Click **Services** > **Solution Deployment Manager** > **Upgrade Jobs Status**.

   System Manager displays the Upgrade Jobs Status page.
3. In the **Job Type** field, select the required upgrade job type.

   System Manager displays the status of the upgrade job type that you selected.

Editing an upgrade job

Before you begin

Upgrade job status must be in pending state.

Procedure

1. Log on to the System Manager web console.
2. Click **Services** > **Solution Deployment Manager** > **Upgrade Jobs Status**.

   System Manager displays the Upgrade Jobs Status page.
3. In the **Job Type** field, select the required upgrade job type.

   System Manager displays the status of the upgrade job type that you selected.
4. Select a pending upgrade job to edit.
5. Click **Edit Configuration**.

   System Manager displays the Upgrade Configuration page.
6. Edit the required fields.

Deleting Upgrade Jobs

Procedure

1. Log on to the System Manager web console.
2. Click **Services** > **Solution Deployment Manager** > **Upgrade Jobs Status**.

   System Manager displays the Upgrade Jobs Status page.
3. In the **Job Type** field, select the required upgrade job type.

System Manager displays the status of the upgrade job type that you selected.

4. Click **Delete**.

   System Manager 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
Delete	Deletes the upgrade job.
Re-run Checks	Performs the upgrade job again.
Edit Configuration	Displays the Upgrade Configuration page where you can change the upgrade configuration details.

Upgrading media gateways and media modules

About this task

According to the compatibility matrix, you can upgrade Media Gateway/Media Module from:

- Higher Release to Lower Release

- Lower Release to Higher Release

Therefore, in Solution Deployment Manager, if Gateways/Media Modules are on latest firmware release on the Upgrade Management page and if any older firmware artifact(s) already downloaded in Software Library then the **Update Status** column displays **Ready for Upgrade** on the Upgrade Management page. You can see the compatibility matrix on Avaya Support website.

If a Avaya MP160 Media Module is added in System Manager on the **Inventory** > **Manage Elements** > page and its device type is displaying as **Other** then:

1. Upgrade to System Manager 7.1.3.5 (if the system is on the System Manager 7.1.x load) or Release 8.1.1 (if the system is on System Manager 8.1.x load)
2. Click **Refresh Elements** operation against the Media Module

By doing this, the system starts displaying the device type as **Avaya MP160** instead of **Other** on the Upgrade Management and Manage Elements pages.

Note:

System Manager Release 8.0.x does not have this change. Therefore, on the System Manager 8.0.x system the device type of Avaya MP160 Media Modules is displayed as **Other**.

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 navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the 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.

G430 Branch Gateway and G450 Branch Gateway multistep upgrade overview

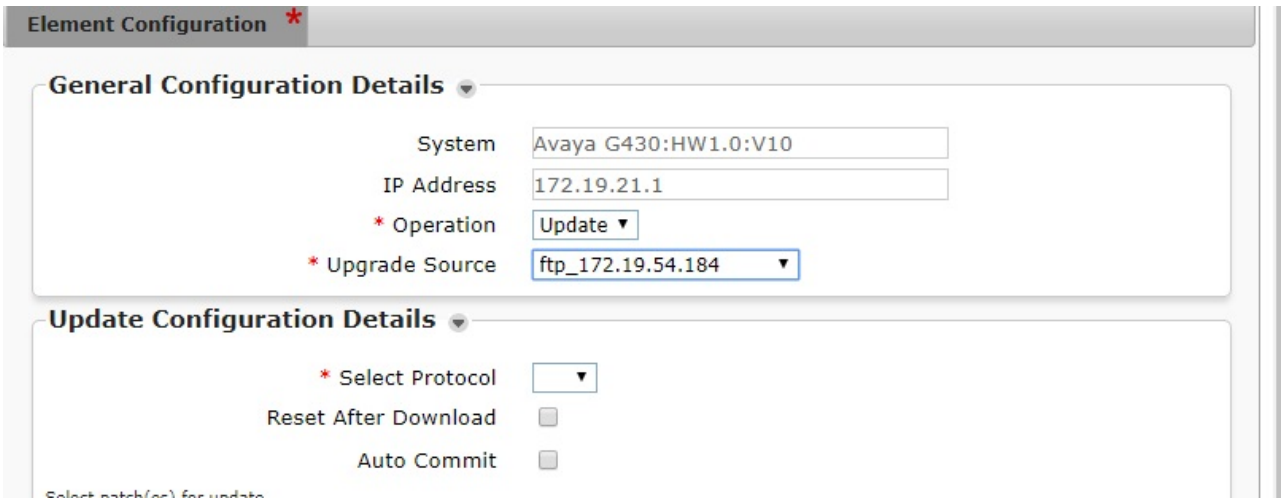
Direct upgrade of G430 Branch Gateway and G450 Branch Gateway is not supported for certain versions. You must upgrade the gateway through specific intermediate versions. The following table displays the supported upgrade path of G430 Branch Gateway and G450 Branch Gateway:

Upgrade/ Downgrade	**To version**					
From version	**<= 36.xx**	**37.xx**	**38.18 to 38.20.x**	**38.21.0**	**39.5.0 and later**	**40.xx**
<= 36.xx	Direct Upgrade	Direct Upgrade	Upgrade via 37.xx	Upgrade via 37.xx	Upgrade via 37.xx and 38.21.0	Upgrade via 37.xx and 38.21.0
<= 37. xx	Direct Downgrade	Direct Upgrade	Direct Upgrade	Direct Upgrade	Upgrade via 38.21.0	Upgrade via 38.21.0
38.18 – 38.20.x	Direct Downgrade	Direct Downgrade	Direct Upgrade	Direct Upgrade	Upgrade via 38.21.0	Upgrade via 38.21.0
39.5.0	Direct Downgrade	Direct Downgrade	Direct Downgrade	Direct Downgrade	Direct Upgrade	Direct Upgrade
40.xx	Direct Downgrade	Direct Downgrade	Direct Downgrade	Direct Downgrade	Direct Downgrade	Direct Upgrade

For example, if G430 Branch Gateway is currently on version 36.8.0 and must be upgraded to 39.5.0, then first upgrade the gateway to 37.xx of version such as 37.38.0 or 37.41.0. Then upgrade to 38.21.0, and then to 39.5.0. Therefore, the upgrade path is 36.8.0 > 37.xx > 38.21.0 > 39.5.0.

Solution Deployment Manager supports this multistep upgrade and updates it automatically based on the current version of the gateway and the selected Upgrade to version. But Solution Deployment Manager requires that you download the intermediate versions for the upgrade path in the same software library where the selected Upgrade to version is present. Solution Deployment Manager then automatically upgrades the gateway through the intermediate versions and up to the selected Upgrade to version.

If you perform a gateway upgrade through Solution Deployment Manager, the system displays an error message. This message is irrespective of the availability of the required intermediate version in the selected software library (**Upgrade Source**) on the Upgrade Configuration page.

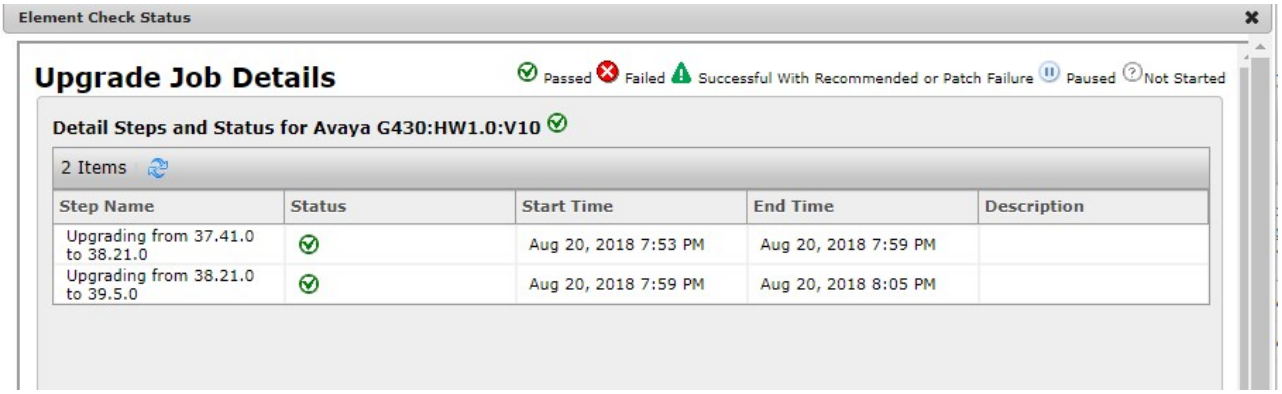


The system displays the following error message when intermediate versions are unavailable in the selected **Upgrade Source** or Software Library:

```
Page contains error(s) - Software Version(s) <Version_numbers> of
Media Gateway must also be downloaded and present in the selected
software library, <Software_Library_Name> for the selected upgrade path.
Upgrading from <Older_GatewayVersion> to <Later_GatewayVersion> is a
multi-step upgrade. Please see the Administering System Manager guide
for more details.
```

If all required intermediate versions are present in the selected **Upgrade Source** software library, you can save the upgrade configuration and schedule the upgrade on the Upgrade Configuration page.

For viewing the multistep upgrades progress, you can click the **Upgrade Status** icon on the **Upgrade Management** page. To view **Job Status** and **Upgrade Path** steps with intermediate upgrades, if any, and their progress, click the **Upgrade Status** icon.



Related links

Configuring EASG during G430 Branch Gateway and G450 Branch Gateway upgrade on page 1478

Configuring EASG during G430 Branch Gateway and G450 Branch Gateway upgrade

About this task

G430 Branch Gateway and G450 Branch Gateway support Enhanced Access Security Gateway (EASG) from version 39.5.0.

When G430 Branch Gateway or G450 Branch Gateway is upgraded to any version later than or same as 39.5.0, Solution Deployment Manager displays the **Enhanced Access Security Gateway (EASG)** field on the Edit Upgrade Configuration page.

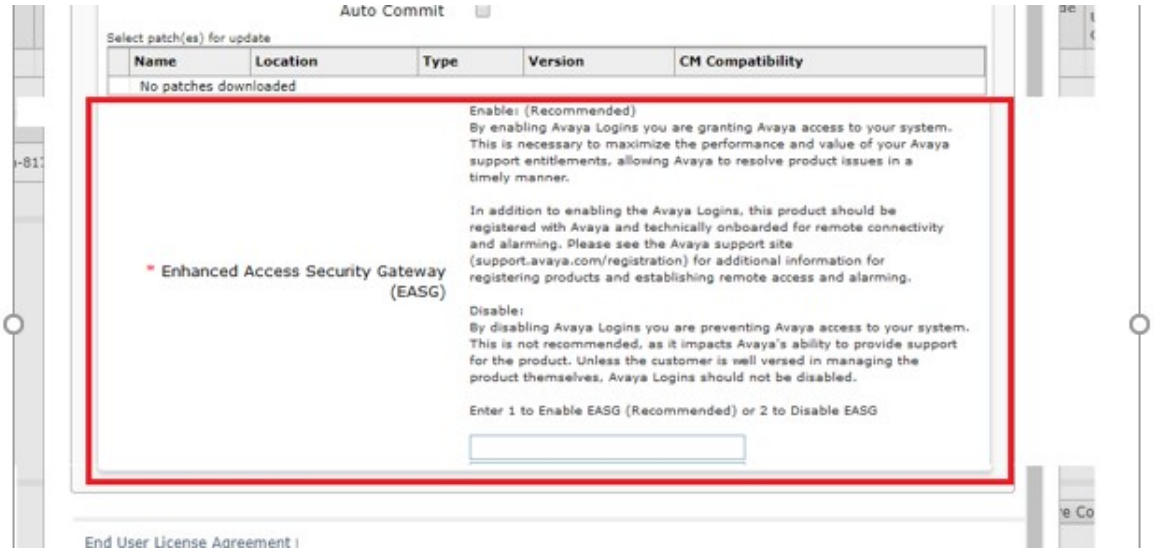
To fetch the EASG configuration information, click **Refresh Element(s)**. Based on the **Refresh Element(s)** operation and the target upgrade version, the system displays the **Enhanced Access Security Gateway (EASG)** field.

If EASG is already enabled, the system does not prompt for the EASG configuration.

Use this procedure to configure EASG during the gateway upgrade.

Procedure

1. On the **Edit Upgrade Configuration** page, do one of the following:
   - To enable EASG, type 1.
   - To disable EASG, type 2.



   This field is mandatory.

   If you leave it blank or type a value other than 1 or 2 , the page displays the following error message.

   ```
   Page contains error(s) - Please Enter 1 to Enable EASG
   (Recommended) or 2 to Disable EASG.
   ```

2. Save the upgrade configuration.

3. To refresh the gateway after successful upgrade, click **Refresh Element(s)**.

   Solution Deployment Manager does not prompt for EASG configuration in subsequent upgrades.

Related links

G430 Branch Gateway and G450 Branch Gateway multistep upgrade overview on page 1476

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.

Protocol matrix for upgrades

Table 10: 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 version of the gateway is 31.17.X or later.
G450	FTP, SCP (gateway versions later than 31.17.XX), USB	G450 supports the SCP protocol only if the current version of the gateway is 31.17.X or later.
G250	FTP, USB	Media modules associated with the gateway support the same protocols as the gateway.
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.

System Manager Solution Deployment Manager supports both FTP and SCP protocol supported remote library for Media gateway upgrade. This is strictly in accordance with the products and supported protocols in the above table.

For example, if a media gateway supports only FTP then you can only configure FTP protocol supported remote software library in System Manager Solution Deployment Manager Library management.

If a media gateway supports both SCP and FTP then you can configure either FTP or SCP protocol supported remote software library in the System Manager Solution Deployment Manager Library management.

Uploading the version.xml file

About this task

Using **Upload Version XML**, you can upload the `version.xml` file from your local system to System Manager to perform upgrades.

Note:

If you do not have the internet connectivity from System Manager to PLDS and do not want to configure alternate source, you can upload the `version.xml` file.

Before you begin

Download the `smgr-versionsxmls.zip` file from PLDS.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
2. On the **Home** > **Services** > **Solution Deployment Manager** > **User Settings** page, click **Reset to Default**.

   Solution Deployment Manager checks the `versions.xml` files that are already present on System Manager.
3. In the navigation pane, click **Upload Version XML**.
4. On the Upload Version XML page, click **Browse**.

   Note:

   Upload one `versions.xml` file at a time. Uploading the complete `smgr-versionsxmls.zip` is not supported.
5. Select a `version.xml` file from your local system and click **Open**.
6. Click **Commit** to upload the file.

   System Manager displays the following message:

   `File upload is in progress. Please do not navigate away from this page.`

Chapter 24: Data Encryption

From Release 10.1, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Avaya Solutions Platform 130 and VMware Virtualized Environment. Once you deploy the application with data encryption, you cannot disable data encryption after deployment.

By enabling Data Encryption, your Communication Product's certain Operational data and Log Files will be encrypted. You will be prompted to enter a passphrase that will be used to create or access an encryption key. You must remember the encryption passphrase, if not it can result in locking up the system. Secondly, you will be asked to configure the option for local key storage.

It is important to note that the encryption of the disk may have a performance impact. For further information, refer to the Avaya Product Administration guide(s). Before you select an encryption option, please read the Data Privacy Guideline so that you may better understand these options.

By disabling Data Encryption, your Communication Product's Operational data and Log Files will not be stored in encrypted partitions.

If encryption is enabled and the **Require Encryption Pass-Phrase at Boot-Time** check box is selected, you need to reenter the encryption passphrase whenever the application reboots.

During reboot, the application prompts you to enter the encryption passphrase on VM console at first boot and upon entering the correct encryption passphrase, the system mounts all the encrypted disks.

Note the following:

- If a common encryption passphrase is used for all the encrypted partitions, but an incorrect encryption passphrase is entered in first attempt, then you have to enter the correct encryption passphrase for every partition at least once.
- Multiple failures on encryption passphrase boots the system into the Maintenance/Emergency mode. To get the prompt again, you need to reboot the system.

If encryption is enabled and the **Require Encryption Pass-Phrase at Boot-Time** check box is not selected during OVA deployment, the application creates the Local Key Store and the system does not prompt you to type the encryption passphrase whenever the application reboots to mount the encrypted disks. You can also set up the remote key server by using the **`encryptionRemoteKey`** command after the deployment of the application.

Important:

An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa.

Encryption of System Manager partitions

When you enable data encryption for System Manager, the system encrypts the following partitions that have personal data.

- `/var/log`
- `/var/log/audit`
- `/var/lib/pgsql/data`
- `/var/opt/nortel/cnd`

Remote Key Server

When you enable data encryption for an application, you can set up remote key server. You can add multiple remote key servers. When you add a remote key server for the first time, the application disables the local key store. You can enable the local key store again after adding a remote key server. However, it is not recommended to enable local key store when the remote key server configuration exists.

If there is only one empty slot, then you cannot add a new remote key server or a new passphrase. You can use a total of 32 slots. The last empty slot is a “reserved” slot and you can use that only for changing the passphrase.

Application checks for the remote key server accessibility every 15 minutes. If any of the remote key server goes down, the application generates a Warning alarm. If all remote key servers are not accessible, then the application generates a Minor alarm.

Data Encryption password policy

The encryption passphrase must meet the following requirements:

- Must contain at least eight characters.
- Must contain at least one of each: an uppercase letter, a lowercase letter, a numerical, and a special character.

Ensure that you keep the encryption passphrase safe. You need the encryption passphrase later.

Data encryption commands

The following CLI commands are available to make changes to the data encryption settings.

encryptionPassphrase command

Using the **encryptionPassphrase** command you can manage the encryption passphrase after deploying the application.

Syntax

```
encryptionPassphrase [add | change | remove | list]
```

add	Displays the prompts to add the encryption passphrase.
change	Displays the prompts to change the encryption passphrase.
remove	Removes the encryption passphrase.
list	Displays the encryption passphrase and slot assignment.

Considerations

You must deploy the application with data encryption.

Adding encryption passphrase

About this task

Use the **encryptionPassphrase add** command to add encryption passphrase.

You can add a maximum of seven encryption passphrases, if free slots are available.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase add**.
3. When the system prompts for privileged command execution verification [sudo], type the password.
4. In **Enter existing passphrase**, type the encryption passphrase.
5. In **Enter new Passphrase**, type the new encryption passphrase.
6. In **Retype Passphrase**, retype the encryption passphrase.

Changing encryption passphrase

About this task

Use the **encryptionPassphrase change** command to change the existing encryption passphrase.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase change**.

3. When the system prompts for privileged command execution verification [sudo], type the password.
4. At the prompt, in **Current Passphrase**, type the encryption passphrase.
5. In **Enter new Passphrase**, type the new encryption passphrase.
6. In **Retype Passphrase**, retype the encryption passphrase.

   The application displays the following message.

   ```
   Passphrase successfully changed.
   ```

Removing encryption passphrase

About this task

Use the **`encryptionPassphrase remove`** command to remove the existing encryption passphrase. You cannot remove all encryption passphrases, the application retains minimum one encryption passphrase.

If you attempt to delete the last encryption passphrase, the system displays the following message:

```
The last passphrase cannot be removed!
```

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **`encryptionPassphrase remove`**.
3. When the system prompts for privileged command execution verification [sudo], type the password.
4. At the prompt, in **Passphrase to remove**, type the existing encryption passphrase.

   The application displays the following message.

   ```
   Passphrase successfully removed.
   ```

Displaying encryption passphrase and slot assignment

About this task

Use the **`encryptionPassphrase list`** command to list the slots assignment, encryption passphrase, and remote server details.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **`encryptionPassphrase list`**.
3. When the system prompts for privileged command execution verification [sudo], type the password.

The application displays the details based on the system configuration.

```
Slot        Status      Passphrase/Remote Server
-----------------------------------------------
Key Slot 0: ENABLED     Passphrase
Key Slot 1: ENABLED     Passphrase
Key Slot 2: ENABLED     Passphrase
Key Slot 3: DISABLED    empty
Key Slot 4: DISABLED    empty
Key Slot 5: DISABLED    empty
Key Slot 6: DISABLED    empty
Key Slot 7: DISABLED    empty
.......
.......
.......
Key Slot 31: Disabled    empty
```

encryptionRemoteKey command

Using the **encryptionRemoteKey** command you can manage the remote key server after deploying the application.

Syntax

```
encryptionRemoteKey [add | remove | list]
```

add	Displays the prompts to add the remote key server.
remove	Removes the remote key server.
list	Displays the remote key server and slot assignment.

Considerations

You must deploy the application with data encryption.

Adding remote key server

Before you begin

Ensure that the remote key server is configured and accessible.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionRemoteKey add** <Address> <Port>.

   Where:

   Address is the IP address or FQDN of the remote key server.

   Port is the port number of the remote key server. If you do not enter the port number the application uses the value of default port as 80.
3. When the system prompts for privileged command execution verification [sudo], type the password.
4. In **Enter existing passphrase**, type the existing encryption passphrase.

If the remote key server is not configured, the application displays the following message.

```
Remote key server not found
```

If the remote key server is configured, the application adds the remote key server. When you add a remote key server for the first time, the application disables the local key store.

Removing remote key server

About this task

Use the **encryptionRemoteKey remove** command to remove the existing remote key server.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionRemoteKey remove** <Address>.

   Where:

   Address is the IP address or FQDN of the remote key server.

   You must use the same IP address or FQDN value that you used to add the remote key server.
3. When the system prompts for privileged command execution verification [sudo], type the password.
4. In **Passphrase**, type the existing encryption passphrase.

   The application removes the remote key server and displays the following message:

   ```
   RemoteKey successfully removed.
   ```

Displaying remote key server and slot assignment

About this task

Use the **encryptionRemoteKey list** command to list the slots assignment, encryption passphrase, and remote server details.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionRemoteKey list**.
3. When the system prompts for privileged command execution verification [sudo], type the password.

   The application displays the details based on the system configuration.

   ```
   Slot        Status      Passphrase/Remote Server
   ------------------------------------------------
   Key Slot 0: ENABLED     Passphrase
   Key Slot 1: ENABLED     <IP Address of Remote Key Server>
   Key Slot 2: ENABLED     Passphrase
   Key Slot 3: DISABLED    empty
   Key Slot 4: DISABLED    empty
   ```

```
Key Slot 5: DISABLED    empty
Key Slot 6: DISABLED    empty
Key Slot 7: DISABLED    empty
.......
.......
.......
Key Slot 31: Disabled    empty
```

encryptionLocalKey command

Using the **encryptionLocalKey** command you can enable or disable the local key store after deploying the application with data encryption.

Syntax

```
encryptionLocalKey [enable | disable]
```

enable	Enables the local key store.
disable	Disables the local key store.

Considerations

You must deploy the application with data encryption.

Enabling local key store

About this task

Use the **encryptionLocalKey enable** command to enable the local key store.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionLocalKey enable**.
3. When the system prompts for privileged command execution verification [sudo], type the password.
4. At the prompt, in **Enter existing passphrase**, type the existing encryption passphrase.

   If the local key store is already enabled, the application displays the following message.

   ```
   Local key store is already enabled.
   ```

Disabling local key store

About this task

Use the **encryptionLocalKey disable** command to disable the local key store.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionLocalKey disable**.

3. When the system prompts for privileged command execution verification [sudo], type the password.

   The application displays the following message.

   ```
   Local keystore removed
   ```

   ```
   Local Key Store is now disabled.
   ```

Viewing data encryption status

About this task

The **`encryptionStatus`** command displays information about encryption on the system.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type `encryptionStatus`.
3. When the system prompts, type the password.

   For example, if the local key store is configured, the system displays the following status:

   ```
   Data Encryption: enabled
   Number of PassPhrases used: <n>
   Local Key Store: enabled
   Encryption Passphrase Required at Boot-time: no
   ```

   For example, if the remote key server is configured, the system displays the following status:

   ```
   Data Encryption: enabled
   Local Key Store: disabled
   Encryption Passphrase Required at Boot-time: yes
   remoteKeyServers: <remoteServer1: <remoteServerIPAddress> accessible>
   ```

Chapter 25: Communication Manager Notify Sync

Communication Manager notify synchronization

When you perform an administrative task from System Manager, the local database is immediately updated. If you do 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 run certain tasks against a Communication Manager object from a system other than System Manager
- Notifications whenever the tti-m, tti-s, psa-u, psa-a, or psa-d login perform 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 existing rsyslog capability of Communication Manager. rsyslog uses UDP or TCP to send event messages from the originating Communication Manager to the System Manager.

Note:

The daily default synchronization and any other scheduled synchronization operations are unaffected by the CM notify sync feature.

You need Communication Manager 6.2 or later to enable the CM notify sync feature. System Manager 6.3 supports one-way and two-way TLS.

Note:

If you log on to Communication Manager using SSH from a system with IPv6 address assigned and execute add/change/duplicate/delete commands on Communication Manager, Notify sync does not operate successfully.

You must log on to Communication Manager from a system with IPv4 address assigned for Notify sync feature to operate.

Enable the CM notify sync feature

You can enable and disable the CM notify sync feature on each Communication Manager. You can activate the CM notify sync feature on the **Services** > **Inventory** > **Manage Elements** page. You can select Communication Manager 6.2 or later, and select **Enable Notifications** in the General Attributes section.

Note:

System Manager resolves the host name or IP address of active and standby Communication Manager as configured on the Manage Elements page. You can check the logs on the Communication ManagerSAT screen in the `/var/log/commandhistory` file.

As a system administrator, you must specify the IP addresses of one or two System Manager servers to which Communication Manager sends the event data using rsyslog. If your configuration includes two System Manager servers, the standby System Manager ignores the syslog messages until the System Manager becomes active.

Configuring one-way and two-way TLS

You must configure one-way or two-way TLS for the CM notify sync feature.

To configure one-way TLS, perform the following:

- Downloading the System Manager PEM certificate on page 144
- Downloading the pem file to Communication Manager on page 1492
- Adding a trusted certificate to Communication Manager on page 1493
- Configuring notify sync between Communication Manager and System Manager on page 1494

  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, do the following:

- Downloading the System Manager PEM certificate on page 144
- Downloading the pem file to Communication Manager on page 1492
- Adding a trusted certificate to Communication Manager on page 1493
- Configuring notify sync between Communication Manager and System Manager on page 1494
- Adding the Communication Manager certificate to the System Manager trust on page 1496
- Enabling two-way TLS in System Manager on page 1497

Downloading the System Manager PEM certificate

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **CA Structure & CRLs**.
4. Click **Download PEM file**.

   The system downloads the `.pem` file on your system.

Related links

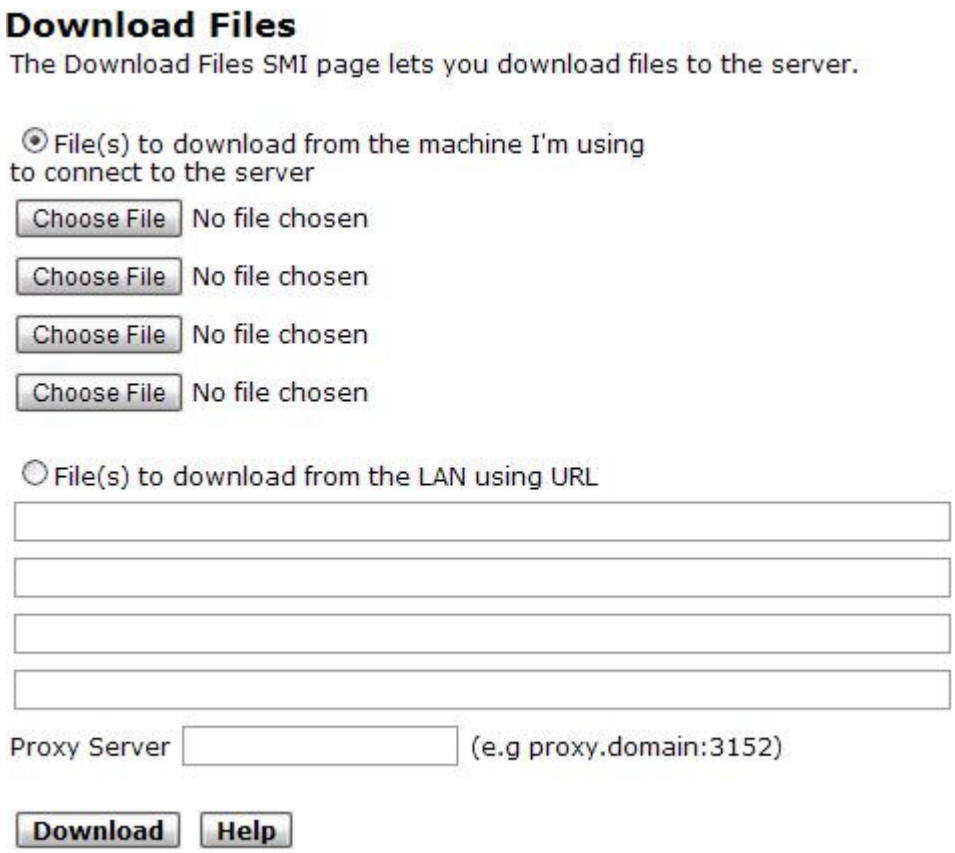
Exchanging CA certificates between System Manager and Avaya Meetings Management on page 143

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.



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.

Configuring notify sync between Communication Manager and System Manager

About this task

When Geographic Redundancy is configured, on Communication Manager, the system registers the IP address of the primary or secondary System Manager that manages Communication Manager.

Before you begin

On the Manage Elements page, register both the IP addresses of the duplex Communication Manager pair for System Manager to handle the notify sync messages.

Note:

In a duplex configuration, you cannot use the virtual address on Communication Manager.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Select a Communication Manager system.
4. In the Attributes section, select **Enable Notifications**.

   When you enable notify sync, the system sends a register command to Communication Manager for registering the IP address of System Manager as a syslog server. The system sends all administrative changes that you make on Communication Manager to System Manager.
5. To verify that the notify sync feature is successfully enabled, do the following:
   a. Using an SSH client, log in to Communication Manager as sroot.
   b. At the prompt, type `sudo /opt/ws/cmSyslogConfig --iptcmquery`.

   The system displays the details of the registration.
6. When the notify sync is nonoperational, and when Geographic Redundancy is set up on System Manager, complete the following:
   a. Ensure that you have root permissions to Communication Manager to edit the file.
   b. Using an SSH client, log in to Communication Manager as root.
   c. Open the `/etc/syslog.conf` file.
   d. Add hash (#) at the beginning of the following secondary System Manager related entries in the file:

      ```
      $ActionSendStreamDriver gtls
      $ActionSendStreamDriverMode 1
      $ActionSendStreamDriverAuthMode x509/certvalid
      #local6.*   @@[148.147.162.36]:9000
      ```
   e. To restart the rsyslog service on Communication Manager, type `service rsyslog restart`.

      Notify sync becomes operational.

7. 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 the 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 hash (#) at the beginning of the following secondary System Manager related entries in the file:

      ```
      $ActionSendStreamDriver gtls
      $ActionSendStreamDriverMode 1
      $ActionSendStreamDriverAuthMode x509/certvalid
      local6.*   @@[148.147.162.35]:9000
      ```

Configure two-way TLS

You must configure either one-way or two-way TLS to enable the Communication Manager notification service. To configure two-way TLS, do the following:

- Downloading the System Manager PEM certificate on page 144
- Downloading the pem file to Communication Manager on page 1492
- Adding a trusted certificate to Communication Manager on page 1493
- Configuring notify sync between Communication Manager and System Manager on page 1494
- Adding the Communication Manager certificate to the System Manager trust on page 1496
- Enabling two-way TLS in System Manager on page 1497

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. Log on to System Manager Web Console.
3. On the System Manager web console, click **Services** > **Inventory**.
4. In the navigation pane, click **Manage Elements**.
5. Select **System Manager** from the elements list.
6. Click **More Options** > **Manage 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 Application server 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. To restart the Application server, type `smgr restart`.

During a restart the System Manager web console will be unavailable for 10-15 minutes.

Chapter 26: System Manager Network Configuration

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 Release 10.2.x, 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 Avaya Breeze® 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 deployed on an Avaya Solutions Platform 130 host that is configured with Out of Band Management. To configure Out of Band Management on Avaya Solutions Platform 130, see *Installing the Avaya Solutions Platform 130 Series*.

Note:

Once OOBM is enabled on System Manager, public interface eth1 is no longer reachable using ping command from other systems that are present in a public network. However, System Manager can reach other systems on a public interface.

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.

Configuring Out of Band Management on System Manager

About this task

If you do not configure Out of Band Management during the deployment of System Manager OVA from Solution Deployment Manager on an Avaya-provided server, you can use the **`configureOOBM`** command to configure Out of Band Management anytime after the deployment.

Before you begin

- Configure Out of Band Management on Avaya Solutions Platform 130, see *Installing the Avaya Solutions Platform 130 Series*.
- Install System Manager on the Avaya Solutions Platform 130 host on which Out of Band Management is configured.
- Ensure that IP address or hostname of Public network and Management network are different.

  If both are in the same network, Out of Band Management configuration might not function as expected.
- Log in to System Manager by using an SSH client utility.

  When you enable Out of Band Management configuration, you might lose the connection as the system does a network restart. You can login to System Manager from the Console of VMware vSphere to connect to the Avaya Solutions Platform host server.

Procedure

1. To enable Out of Band Management, type `configureOOBM -EnableOOBM`.

   The system enables Out of Band Management on the System Manager virtual machine. With **`EnableOOBM`**, the system configures the additional Ethernet interface, updates network configuration, and sets the firewall rules.

2. To disable Out of Band Management, type `configureOOBM -DisableOOBM`.

   The system disables Out of Band Management on the System Manager virtual machine. With **`DisableOOBM`**, the system disables the additional Ethernet interface that you configured earlier and sets the firewall rules to default.

Configuring Out of Band Management on System Manager in the Geographic Redundancy setup

About this task

Note:

You cannot enable Out of Band Management on secondary System Manager server when Out of Band Management on primary System Manager server is disabled.

Before you begin

Identify one of the following:

- Enable Out of Band Management on both the primary and secondary System Manager server.
- Enable Out of Band Management on the primary System Manager server and not enable Out of Band Management on the secondary System Manager server.
- Disable Out of Band Management on secondary System Manager server.
- Disable Out of Band Management on both the primary and secondary System Manager server.

Procedure

1. To enable Out of Band Management on both primary and secondary System Manager server, perform the following:
   a. Disable Geographic Redundancy replication on primary System Manager server.
   b. Convert primary System Manager server to standalone System Manager server and activate the secondary System Manager server.
   c. Enable Out of Band Management on both primary and secondary System Manager server.
   d. Reconfigure the Geographic Redundancy on the secondary System Manager server.

   e. Enable Geographic Redundancy replication on primary System Manager server.

2. To enable Out of Band Management on the primary System Manager server and not enable Out of Band Management on secondary System Manager server, perform the following:
   a. Disable Geographic Redundancy replication on primary System Manager server.
   b. Convert primary System Manager server to standalone System Manager server.
   c. Enable Out of Band Management on primary System Manager server.
   d. Once Out of Band Management on primary System Manager server is enabled, reconfigure Geographic Redundancy on secondary System Manager server.
   e. Enable Geographic Redundancy replication on primary System Manager server.
3. To disable Out of Band Management on secondary server, perform the following:
   a. Disable Geographic Redundancy replication on primary System Manager server.
   b. Convert primary System Manager server to standalone System Manager server.
   c. Activate secondary System Manager server and disable Out of Band Management.
   d. Reconfigure primary System Manager server from the web console of the secondary System Manager server.
   e. Enable Geographic Redundancy replication on primary System Manager server.
4. To disable Out of Band Management on both servers, perform the following:
   a. Disable Geographic Redundancy replication on primary System Manager server.
   b. Convert primary System Manager server to standalone System Manager server and disable Out of Band Management.
   c. Activate secondary System Manager server and disable Out of Band Management.
   d. Reconfigure Geographic Redundancy on secondary System Manager server with old primary System Manager server which is now standalone.
   e. Enable Geographic Redundancy replication on primary System Manager server.

Changing the IP address and FQDN in System Manager

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 a 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 modes

- 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 a 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 involving remote machines such as, CS 1000 servers and solutions based on the System Manager Single Sign On (SSO) client, the SSO between System Manager and the remote machine fails.

During the data migration or IP-FQDN change, the system does not import the LDAP attribute containing the SSO cookie domain value back to the directory. Therefore, the System Manager SSO login to the remote machine fails. You must enable SSO after the data migration or the IP-FQDN change.

Related links

Reimporting the SSO cookie domain value on page 67

Changing network parameters on System Manager

Changing the IP address, FQDN, DNS, Gateway, or Netmask address of System Manager from CLI

About this task

Use this procedure to change the network configuration parameters for the Public interface and Management interface when OOBM is enabled.

Note:

To change the network parameters on a primary or secondary System Manager server in a Geographic Redundancy setup, you can use the **`changeIPFQDN`** command.

For more information about changing the IP address or FQDN in a Geographic Redundancy setup, see “Changing the IP address and FQDN on the primary System Manager when the secondary is in the standby or active mode”.

Important:

- Do not change the network settings from vSphere Client (HTML5) when the virtual machine is in a power off state.
- FQDN value must be unique and different from the virtual FQDN value of System Manager.

Before you begin

- To reach the System Manager command-line interface, use one of the following methods:
  - Open vSphere Client (HTML5) and click the **Console** tab or the icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.
- 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 the following:

   ```
   changeIPFQDN -IP <IPv4 address> -FQDN <FQDN> -GATEWAY <Gateway IPv4
   address> -NETMASK <Netmask address> -DNS <DNS address> -SEARCH
   <search list of domain names> -IPV6 <IPv6 address> -IPV6GW <IPv6
   Gateway address> -IPV6PREFIX <IPv6 prefix>
   ```

   For more information, see **`changeIPFQDN`**.

2. To configure Public network parameters, type the following:

   ```
   changePublicIPFQDN -IP <IP address> -PublicFQDN <FQDN>
   -PublicGATEWAY <Gateway IP address> -PublicNETMASK <Netmask
   address>
   ```

   For more information, see **`changePublicIPFQDN`**.

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 more information about how to install a license file, see Managing Licenses in *Administering Avaya Aura® System Manager*.
- After you change the IP address of System Manager, the SNMP Target Profiles must be available under the **Manage Profiles** > **SNMP Target Profiles** tab for the selected agent on

the **Services** > **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents** page. If the target profile is not available, create a new target profile on the **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMP Target Profiles** page.

If target profile is available with latest IP address, re-assign to the targetAddr or create a new target profile and assign to the same.

Related links

System Manager command line interface operations on page 1510
changeIPFQDN command on page 1505

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. You can also use this command to enable or configure to IPv4 or IPv6 network details.

Note:

On the System Manager Release 7.1 and later, if you change the IP Address of System Manager using the **`changeIPFQDN`** command, the system changes the host ID of System Manager and invalidates the existing installed license file. Therefore, you must reinstall the license file on System Manager after changing the IP Address of System Manager.

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 < >-IPV6 < >
-IPV6GW < >-IPV6PREFIX < >
```

#	Option	Description	Usage
1	IP	The new Management IPv4 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 IPv4 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 can 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`**

Table continues…

#	Option	Description	Usage
7	IPV6	The new Management IPv6 address of System Manager.	**changeIPFQDN -IPV6 2001:b00d:dead:1111:1111:1111:1234:8080**
8	IPV6GW	The new Management Gateway IPv6 address of System Manager.	**changeIPFQDN -IPV6GW 2001:b00d::1**
9	IPV6PREFIX	The new Management netmask prefix of System Manager. The default value is 64.	**changeIPFQDN -IPV6PREFIX 64**

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
```

```
changeIPFQDN -IPV6 2001:b00d:dead:1111:1111:1111:1234:8080 -IPV6GW 2001:b00d::1
-IPV6PREFIX 64
```

Changing IP address or FQDN of managed elements

About this task

For instructions to change the IP address or FQDN of managed elements, see the application-specific document. 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 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, type the appropriate value.
6. In the **Access Profile** section, in the **Host** field, type the appropriate 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. Log in to the CLI of the secondary System Manager server with administrator privilege CLI user credentials 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 105
Disabling the Geographic Redundancy replication on page 106

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. Log in to the CLI of the secondary System Manager server with administrator privilege CLI user credentials 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 105
Disabling the Geographic Redundancy replication on page 106

System Manager command line interface operations

#	Command	Parameters	Description	Usage
1	**changeIPFQDN**	• **-IP <new Management interface or Out of Band Management IP address for System Manager>** • **-FQDN <new Management or Out of Band Management fully qualified domain name for System Manager>** • **-GATEWAY <new Management interface or Out of Band Management Gateway address for System Manager>** • **-NETMASK <new Management interface or Out of Band 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 Band Management IP address, FQDN, Gateway, Netmask, DNS, and the search list with the new value. **Note:** On the System Manager Release 7.1 and later, if you change the IP Address of System Manager using the **changeIPFQDN** command, the system changes the host ID of System Manager and invalidates the existing installed license file. Therefore, you must reinstall the license file on System Manager after changing the IP Address of System Manager.	• **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>**

Table continues…

#	Command	Parameters	Description	Usage
2	**changePublicIPFQDN**	• **-publicIP <new IP address for System Manager>** • **-publicFQDN <new fully qualified domain name for System Manager>** • **-publicGATEWAY <new Gateway address for System Manager>** • **-publicNETMASK <new netmask address for System Manage>**	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 domain name for public interface>** • **changePublicIPFQDN -publicIP <new Public IP address> -publicGATEWAY <new Public Gateway address for System Manager>**
3	**upgradeSMGR**	**<absolute path to the dmutility.bin> -m –v**	Upgrades System Manager using the data migration utility.	**upgradeSMGR dmutility *.bin -m –v**
4	**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 SMGRservicepackName>** **Note:** Copy the System Manager service pack or patches that you must install to `/swlibrary`.
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**

Table continues…

#	Command	Parameters	Description	Usage
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. For more information, see, Creating a new Certificate Authority by using SHA2 signing algorithm and 2048 key size.	**createCA** You must provide the desired Common Name (CN)
8	**configureOOBM**		Enables or disables the Out of Band Management configuration.	• To enable Out of Band Management: **configureOOBM –EnableOOBM** • To disable Out of Band Management: **configureOOBM -DisableOOBM**
9	**enableOOBMMultiTenancy**		If Out of Band Management and MultiTenancy are enabled on system, use this command to provision tenant administrators to available on public interface.	
10	**setSecurityProfile**		Enabling the commercial and military grade hardening.	• Enabling commercial grade hardening: **setSecurityProfile --enable-commercial-grade** • Enabling military grade hardening: **setSecurityProfile --enable-military-grade**

Table continues…

#	Command	Parameters	Description	Usage
11	**`EASGManage`**		Enables or disables EASG.	• **`EASGManage --enableEASG`** • **`EASGManage --disableEASG`**
12	**`EASGStatus`**		Displays the status of EASG.	
13	**`EASGProductCert`**		Displays the EASG certificate details.	**`EASGProductCert --certInfo`**
14	**`EASGSiteCertManage`**		To manage EASG Certificates.	
15	**`editHosts`**		To add, replace, and delete the IP Address, FQDN, or hostname entries in the `/etc/hosts` file.	
16	• **`swversion`** • **`swversion -s`**		• swversion: Displays the System Manager software information. • swversion -s: Displays the System Manager software version and also displays information about the application name, profile, and deployment type. • **Note:** The output varies based on the application deployment and the virtualization environment.	

Table continues…

#	Command	Parameters	Description	Usage
17	**changeVFQDN**		To change the System Manager Virtual FQDN.	**changeVFQDN** Type the System Manager Virtual FQDN. **Note:** When you run the **changeVFQDN** command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.
18	**smgr**		Starts, stops, and checks the status of the Application server.	**smgr** `start/stop/status`
19	**smgr-db**		Starts, stops, and checks the status of postgresql.service.	**smgr-db** `start/stop/status`
20	**getUserAuthCert**		Generates a user specific certificate for System Manager to facilitate certificate-based authentication.	

Table continues…

#	Command	Parameters	Description	Usage
21	**`changeCipherSuiteList`**		Configures cipher suite mode for System Manager	• To configure strict cipher suite list, type the following command. This would disable CBC ciphers: **`changeCipherSuiteList LIST2`** • To configure relax cipher suite list, type the following command. This would enable CBC ciphers: **`changeCipherSuiteList LIST1`**
22	**`collectLogs`**		Collects the required logs.	• To collect all the logs: **`collectLogs`** • To collect all the logs along with backup: **`collectLogs -Db`** • To collect all the logs along with CND data: **`collectLogs –CND`**

Table continues…

#	Command	Parameters	Description	Usage
23	**`rebootVM`**		Reboots the System Manager virtual machine. **Important:** If you configured a NFS mount on System Manager for Session Manager Performance Data (perfdata) collection, then, if and when you reboot/boot System Manager virtual machine, you need to ensure that you manually re-mount the NFS store once the System Manager VM is up and you are able to log in to the VM through SSH. Failure to re-mount the NFS partition will result in the Session Manager perfdata to go, by default, into a folder which is in the root (/) partition of the System Manager file system. This might cause the partition to get full which in-turn might cause issues with the System Manager application.	Type `y` or `n` to reboot the System Manager virtual machine.
24	**`powerOffVM`**		Power off the System Manager virtual machine.	Type `y` or `n` to power off the System Manager virtual machine.
25	sudo /bin/systemctl (parameter) snmpd	start/stop/restart/status	To start or stop, and to check status of the SNMP service.	
26	sudo /bin/systemctl (parameter) spiritAgent	start/stop/restart/status	To start or stop, and to check status of the Spirit Agent service.	

Table continues…

#	Command	Parameters	Description	Usage
27	sudo /bin/systemctl (parameter) cnd	start/stop/restart/status	To start or stop, and to check status of the CND service.	
28	encryptionPassphrase	[add | change | remove | list]	To add, change, remove, and display the encryption passphrase.	• **`encryptionPassphrase add`**: To add encryption passphrase. • **`encryptionPassphrase change`**: To change existing encryption passphrase. • **`encryptionPassphrase remove`**: To remove encryption passphrase. • **`encryptionPassphrase list`**: To display the encryption passphrase and slot assignment.
29	encryptionRemoteKey	[add | remove | list]	To add, remove, and display the remote key server.	• **`encryptionRemoteKey add`**: To add remote key server. • **`encryptionRemoteKey remove`**: To remove remote key server. • **`encryptionRemoteKey list`**: To display the remote key server and slot assignment.
30	encryptionLocalKey	[enable | disable]	To enable and disable the local key store.	• **`encryptionLocalKey enable`**: To enable local key store. • **`encryptionLocalKey disable`**: To disable local key store.

Table continues…

#	Command	Parameters	Description	Usage
31	encryptionStatus		Displays information about encryption on the system.	**`encryptionStatus`** displays information about encryption on the system.
32	**`updateLogRetention.sh`**	[-p] [-v] [maxRetentionTime]	Manages the log retention time.	
33	**`pruneAllLogs.sh`**	[-b] [-t] [-v] [-h] [maxRetentionTime]	Manages the deletion of log files.	
34	**`manageEntityClassWhitelist`**	[-h] [addAll *-e* <ENTITY_CLASS_NAME> *-f* <INPUT_FILE> *-u* <USERNAME> *-p* <PASSWORD>] [add *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-u* <USERNAME> *-p* <PASSWORD>] [list *-e* <ENTITY_CLASS_NAME> *-f* <OUTPUT_FILE> *-u* <USERNAME> *-p* <PASSWORD> *-pn* <PAGENUMBER> *-ps* <PAGESIZE>] [view *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-f* <OUTPUT_FILE> *-u* <USERNAME> *-p* <PASSWORD>] [subjectCheck *-e* <ENTITY_CLASS_NAME> *-u* <USERNAME> *-p* <PASSWORD>] [deleteAll *-e* <ENTITY_CLASS_NAME> *-u* <USERNAME> *-p* <PASSWORD>] [delete *-e* <ENTITY_CLASS_NAME> *-s* <SUBJECT_NAME> *-u* <USERNAME> *-p* <PASSWORD>]	You can add, list, view, and delete the subject names for the provided entity class. You can add and delete the bulk entries of subject names and check the status of the subject name validation for the entity class.	
35	**`outboundConnectionLogging`**	[enable] [disable]	If you enable this, you can capture the logs in the `/var/log/Avaya/connections` file for every new outgoing connections initiated from System Manager.	

Table continues…

#	Command	Parameters	Description	Usage
36	**`configureOutboundFirewall`**	[add {*-s*} {*-f*}] [list] [status] [remove {*-e*} {*-f*}] [disable] [overwrite {*-s*} {*-f*}] [enable-logging] [disable-logging] [logging-status]	If you enable this, you can configure System Manager outbound firewall.	
37	**`setSecurityPolicy`**	[--status] [--display-only] [--restore-standard] [--refresh-custom]	You can modify the default password policy settings of System Manager by using the **`setSecurityPolicy`** command. This command is only applicable for changing or setting up the password for the CLI user or root user that gets created at the time of deployment.	
38	**`configureSyslog`**	-h [-e] [-s <*syslog server destination*> ""]	You can configure, list, and delete the remote syslog server by using the **`configureSyslog`** command.	
39	**`ASP_SSH`**	[enable] [status]	If System Manager is deployed on the Avaya Solutions Platform 130 Release 5.1 host, you can enable SSH and check the SSH status of the Avaya Solutions Platform 130 host.	

Table continues…

#	Command	Parameters	Description	Usage

40	**`toggleOldWebLMClientCommunication`**	Run this utility as the following:
		• Type `1` to check the old WebLM client communication status
		• Type `2` to enable the old WebLM client communication status
		• Type `3` to disable the old WebLM client communication status
		Note:
		The user can enter the values specified above based on their usage.
			This utility is used to check, enable, and disable the old WebLM client communication status with releases 10.1.3.1 and later. For the older WebLM client communication, the default status is ENABLED.	• Type `1` to check the old WebLM client communication status.
				• Type `2` to enable the old WebLM client communication status.
				• Type `3` to disable the old WebLM client communication status.
				If your input is 1 and the current status is enabled, the message
				`Old WebLM client communication status is ENABLED`
				is displayed.
				If the current status is disabled, the message
				`Old WebLM client communication status is DISABLED`
				is displayed.
				If your input is 2, the message
				`Old WebLM client communication is now ENABLED`
				is displayed.
				If your input is 3, the message
				`Old WebLM client communication is now DISABLED`
				is displayed.

editHosts

You can add, replace, and delete the IP Address, FQDN, or hostname entries in the `/etc/hosts` file.

Syntax

```
editHosts [-A <ip> <FQDN> <hostname>] [-R <ip> <FQDN> <hostname>] [-D <ip> <FQDN>
<hostname>] [-f </path/filename>] [--restoreDefault] [--verify]
```

-A <ip> <FQDN> <hostname>	Adds the entries.
-R <ip> <FQDN> <hostname>	Replaces the entries.
-D <ip> <FQDN> <hostname>	Deletes the entries.
-f </path/filename>	Adds the entries using a file. You can find a sample file on System Manager at: `/opt/vsp/editHostSampleInput`
--restoreDefault	Restores the default values.
--verify	Verifies the entries in the `/etc/hosts` file.

Example

To add the 10.13.60.21 entry:

```
editHosts "-A 10.13.60.21 datasmgr.smgrdev.avaya.com datasmgr"
number of argument 1==== 1 "-A 10.13.60.21 datasmgr.smgrtest.avaya.com datasmgr"========
Adding IP 10.13.60.21
Valid IPv4 address 10.13.60.21
SUCCESS: Added Entry 10.13.60.21
```

Chapter 27: 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`.

Changing date and time on System Manager running on VMware

Configuring the NTP server

About this task

This is not applicable for the Software-Only deployment.

Before you begin

- To reach the System Manager command-line interface, use one of the following methods:
  - Open vSphere Client (HTML5) and click the **Console** tab or the icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.

Procedure

Type `configureNTP <IP address of NTP server>`.

The application supports only the NTP server. It does not support the NTP pool.

Related links

System Manager command line interface operations on page 1510

Configuring the time zone

About this task

When you run the **`configureTimeZone`** command, it restarts the database connection.

Before you begin

- To reach the System Manager command-line interface, use one of the following methods:
  - Open vSphere Client (HTML5) and click the **Console** tab or the icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.

Procedure

1. Type `configureTimeZone` on the System Manager command line interface.
2. Select the time zone from the list.

   For example, America/Denver.
3. Reboot the system to reflect the time zone changes.

Related links

System Manager command line interface operations on page 1510

Chapter 28: System Manager localization

When you install the language pack on System Manager, the following user interface screens support the Canadian French localization:

- Authentication page.

  Localization changes are not available for System Manager Dashboard.

- On User Management, in **Communication Profile**, localized pages are available for **Session Manager**, **Communication Manager**, and **Messaging** profiles.

  Note:

  Localized pages are not available for following:

  - Password change/management pages
  - In **Communication Profile**, profiles for Collaboration Environment, CS 1000, Callpilot, IP Office, Presence, and Work Assignment.
  - Membership and Contact pages

- Communication Manager management
  - Edit Endpoint Extension on the Manage Endpoints page.
  - On the Maintenance page, **Release Endpoint**, **Busyout Endpoint**, **Test Endpoint**, **List Trace Station** and **Status Station** pages.
  - On the Edit Endpoint page, **General Options**, **Group Membership**, **Feature Options**, **Site Data**, **Abbreviated Call Dialing**, **Enhanced Call Fwd**, **Button Assignment** and **Profile Settings**.

- Messaging Management

  On **Messaging** > **Subscriber** > **Edit Subscriber**, **Basic Information**, **Subscriber Directory**, **Subscriber Security**, **Mailbox Features**, **Secondary Extensions** and **Miscellaneous**.

Related links

Installing language pack on System Manager on page 1525

Installing language pack on System Manager

About this task

After you install, upgrade, or apply a service or a feature pack, run the language pack to get the localization support for the French language.

Note:

After installing the language pack, you cannot uninstall the language pack.

Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Type `locate LocalizationScript.sh`, and press `Enter`.

   System Manager displays the path of the localization script.

   For example: `/opt/Avaya/Mgmt/10.2.x/CommonConsole/script/LocalizationScript.sh`
3. Type `locate FrenchResourceBundle.zip`, and press `Enter`.

   The System Manager displays the path of the `FrenchResourceBundle.zip` script.

   For example: `/opt/Avaya/Mgmt/10.2.x/CommonConsole/localization/common_console/FrenchResourceBundle.zip`

   This is just an example of the path; the path might vary based on actual path that you get.
4. Type `cd $MGMT_HOME/CommonConsole/script/` to go to the localization script folder.
5. To run the localization script, type `sudo ./LocalizationScript.sh $MGMT_HOME/CommonConsole/localization/common_console/FrenchResourceBundle.zip`.
6. If you are installing the language pack through SSH connection, then do not close the SSH session or terminate the connection.

   If you close the SSH session or terminate the connection, System Manager kills the process and the installation fails.

   Note:

   During this activity, System Manager restarts the Application server. Therefore, the System Manager web console will not be accessible. If System Manager is in the Geographic Redundancy mode, then apply these steps on the secondary System Manager server also after secondary server is active.
7. Change the browser language setting to French.

Related links

System Manager localization on page 1524

Chapter 29: Resources

System Manager 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
Administering Avaya Aura® System Manager	Administering System Manager applications and install patches on System Manager applications.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Certificate Management	Understand certificate management.	Customers and sales, services, and support personnel
Avaya Aura® System Manager Data Privacy Guidelines	Describes how to administer System Manager to fulfill Data Privacy requirements.	System administrators and IT personnel
Using		
Using the Solution Deployment Manager client	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Avaya Aura® System Manager Solution Deployment Manager Job-Aid	Deploy System Manager applications and install patches on System Manager applications.	System administrators
Implementation		
Upgrading Avaya Aura® System Manager	Upgrade Avaya Aura® System Manager.	Implementation personnel
Deploying Avaya Aura® System Manager in Virtualized Environment	Deploy System Manager applications in Virtualized Environment.	Implementation personnel

Table continues…

Title	Description	Audience
Deploying Avaya Aura® System Manager in Software-Only and Infrastructure as a Service Environments	Deploy System Manager applications in Software-Only and Infrastructure as a Service environments.	Implementation personnel
Maintenance and Troubleshooting		
Avaya Aura® System Manager SNMP Whitepaper	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

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click 🔍 to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Select Release**, select the appropriate release number.

This field is not available if there is only one release for the product.

5. From the **Select Content Type** list. select one or both of the following options:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** ( ) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

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

Course code	Course title
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

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.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://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.

Related links

Using the Avaya InSite Knowledge Base on page 1530

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.

- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Related links

Support on page 1530

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

System Manager supports the following list reports:

A

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			

B

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			

C

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	

D

data-module	directory board	disabled-mos	do-not-disturb group
do-not-disturb station			

E

eda-external-device-alrm	emergency	extended-pickup-group	extension-type

G

group-page	groups-of-extension

H

history	holiday-table	hunt-group

I

internal-data loginID	integrated-annc-boards	intercom-group	intra-switch-cdr
ip-codec-set	ip-interface	ip-network-map	ip-network-region direct-wan
ip-network-region igar-dpt	ip-network-region monitor	ip-network-region qos	ip-route
ipserver-interface	isdnpri-testcall		

L

logins

M

marked-ports	mct-history
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

Table continues…

measurements cell-traffic summary last-hour	measurements cell-traffic summary today-peak
measurements cell-traffic summary yesterday-peak	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 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

Table continues…

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 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
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	

N

node-routing	node-names

O

off-pbx-telephone station-mapping	

P

partition-route-table	partitioned-group	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	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

R

registered-ip-stations	remote-office	report-scheduler	route-pattern

S

service-hours-table	set-data	signaling-group	sip-station
skill-status	station	stn-firmware	survivable-processor
suspend-alm-orig	synchronization	sys-link	

T

term-ext-group	toll all	toll restricted-call	toll toll-list
toll unrestricted-call	trace	trunk-group	tti-ip-stations

U

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	

V

vdn	vector	video-bridge	vrt
vustats-display-format			

W

wakeup incomplete	wakeup requests	wakeup station

X

xmobile mapping

System Manager does not support the CSV report format for the following list reports:

C

configuration radio-controller	configuration software-versions
configuration wt-stations	

M

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 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 summary	measurements tone-receiver summary last-hour
measurements tone-receiver summary today-peak	measurements tone-receiver summary yesterday-peak
mmi	mct-history
measurements ds1-facility log	measurements ds1-facility summary
measurements principal last-hour	measurements principal today-peak
measurements principal yesterday-peak	

Display reports

System Manager supports the following display reports:

Note:

System Manager does not support the CSV report format for display reports.

A

aar analysis	aar digit-conversion	abbreviated-dialing 7103A-buttons	abbreviated-dialing enhanced

Table continues…

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		

B

bcms-vustats loginIDs	best-service-routing	bp	bri-trunk-board
bulletin-board	button-labels	button-location-aca	

C

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	

D

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		

E

eda-external-device-alrm	enp-number-plan	errors	ethernet-options
events	extended-pickup-group		

F

failed-ip-network-region	feature-access-codes	firmware download	firmware station-download

G

group-page	

H

holiday-table	hunt-group

I

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			

L

listed-directory-numbers	location-parameters	locations	login
lsp			

M

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		

N

node-names audix	node-names ip	node-routing

O

off-pbx-telephone configuration-set	off-pbx-telephone feature-name-extensions
off-pbx-telephone station-mapping	

P

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

R

radio-controller	reason-code-names	remote-access	remote-office
rhnpa	route-pattern		

S

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		

T

telecommuting-access	tenant	term-ext-group	terminal-parameters
tftp-server	time	time-of-day	toll
tone-generation	trunk-group		

U

uniform-dialplan

V

variables	vdn	vector	video-bridge
vrt	vustats-display-format		

X

xmobile configuration-set

Status reports

System Manager supports the following status reports.

A

access-endpoint	administered-connection	aesvcs cti-link	aesvcs interface
aesvcs link	attendant	audits cumulative	audits peak-hour

B

bri-port

C

cabinet	cdr-link

D

data-module

E

environment	esm	ess clusters	ess port-networks

F

firmware station-download	firmware download

H

hardware-group	health

I

ip-board	ip-network-region	ip-synchronization master	ip-synchronization oos-members
ip-synchronization system-information	ip-synchronization member media-gateway	ip-synchronization source media-gateway	isdnpri-testcall

J

journal-link

L

link	logins

M

media-gateways	media-processor all	media-processor board	mg-announcements
meet-me-vdn	mst		

N

nr-registration all-regions	nr-registration network-region	nr-registration survivable-processor

O

off-pbx-telephone mapping-subscriptions	off-pbx-telephone station

P

packet-interface	periodic-scheduled	pms-link	pnc
port-network	pri-endpoint	processor-channels	psa

Q

qos-parameters ipserver-interface

R

remote-access	remote-office

S

signaling-group	sp-link	socket-usage	station
switch-node	synchronization	sys-link	

T

trace-analyzer	trunk	tsc-administered	tti

V

val-ip	video-bridge

System Manager supports the CSV report format for the following status reports.

A

aesvcs cti-link	aesvcs interface	aesvcs link

E

ess clusters	ess port-networks

I

ip-synchronization master	ip-synchronization oos-members	ip-synchronization member media-gateway	ip-synchronization source media-gateway
isdnpri-testcall			

M

media-processor all	mg-announcements

O

off-pbx-telephone mapping-subscriptions

Q

qos-parameters ipserver-interface

S

switch-node	synchronization

T

trunk	tsc-administered

Appendix C: Remote Access

Remote access of System Manager

To provide remote and online support, Avaya services personnel can remotely access the System Manager application by using Enhanced Access Security Gateway (EASG)

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

The product must be registered using the Avaya Global Registration Tool for enabling the system for Avaya Remote Connectivity.

You can also enable EASG after deploying or upgrading the application using the command: **`EASGManage --enableEASG`**.

For more information about EASG, see *Deploying Avaya Aura® System Manager in Virtualized Environment*.

EASG login for System Manager

From System Manager Release 7.1.2 and later, Avaya Technician can use the EASG user accounts to access the System Manager web console and Command Line Interface. Following are the EASG user accounts:

- **init:** Provides the System Administrator role.
- **craft:** Provides the Avaya Services and Maintenance support.

The init and craft accounts are built-in user accounts. Therefore, you cannot modify these user accounts. If EASG is disabled, the system removes the user accounts from System Manager.

Logging on to the System Manager web console by using EASG login

About this task

Avaya Technician and Avaya Services can use the following procedure to login to the System Manager web console by using EASG login.

Before you begin

EASG must be enabled.

Procedure

1. On the web browser, do one of the following:
   - If you are in a customer network, type `https://<System Manager_Fully Qualified Domain Name>/services`.
   - If you are not in the customer network and using the Secure Access Link (SAL) https connection, type `https://localhost/services` or `https://127.0.0.1/services`.

     If you are neither in the customer network nor using the Secure Access Link (SAL) https connection then you cannot access the System Manager web console.

   If EASG is disabled, the system displays the message: `EASG is disabled`.

   If EASG is enabled, proceed with the following steps.
2. In the **Username** field, type `init` or `craft`.
3. Click **Next**.

   The system displays the **Challenge**, **Product ID**, and **Response** fields. The **Challenge** and **Product ID** fields are read only.
4. In **Response**, paste the response for the EASG challenge.

   The response is up to ove512 characters long.
5. Click **Login**.

   The system validates the challenge and response. If authentication is successful, the system displays the System Manager web console.

Glossary

Application Server From Release 8.x onwards, the Application server used in System Manager is WilDFly. Operating System level service name is jboss.

Index

Special Characters

.CADF xml file to MIB and trapd file 962, 963

Numerics

2048 key size 1240

A

AAR/ARS Digit Conversion field descriptions
    AAR/ARS Digit Conversion; field description 802, 805
Abbreviated Dialing
    Enhanced List 762
Abbreviated Dialing List 1, List 2, List 3 762
abbreviated dialing lists 762
abort
    global user settings import job on first error 402
abort a user import job 394
abort global user settings import job on first error 402
aborting
    virtual machine report generation 1417
about audio files 1168
about CM aduit 992
about reports 1098
Access Control 171
access log harvesting 1017
access profile 944
    create 927
    delete 928
    modify 928
    new 927
    remove 928
access Solution Deployment Manager client 1322
Access to Administrative Users 209
access to PLDS 1327
Accessing Element Cut-Through 714
accessing log harvest 1017
accessing port matrix 1527
accessing resources 165
accessing scheduler 1118
accessing the Backup and Restore service 851
accessing the Data Retention Rules service
    data retention rules service; access 869
accessing the Log Settings service 1030
accessing WebLM 1048
account operations
    CS1000 998
account synchronization 994
Act Time 713
activate SSH from AVP Utilities 1380
activating
    secondary server 108
activating agent 975
activating serviceability agent 975
Active
    Coverage Path 707
Active Directory Federation Service(ADFS) 1283
Active Station Ringing 747
actual license usage 1051
add
    custom role 177
    custom tenant administrator role 178
    endpoints 718
    G430 Branch Gateway 936
    G450 Branch Gateway 936
    hunt group 786
    new role 177
    new tenant administrator role 178
    role 177
add a contact address of a private contact 275
add a contact address of a public contact 601
add a postal address to public contact 600
add a public contact 598
Add Address page 246, 281, 611
add element access profile 917
add element instances 1060
Add elements
    bulk 906
    manual 906
Add elements in bulk 906
Add End Entity 1235
add endpoint templates
    field descriptions 743
add endpoints
    field descriptions 743
add endpoints in bulk 776
Add Entity Class
    field descriptions 1225
Add IP Office
    field description 960
Add local WebLM page 1074
Add Mapping 186, 187
Add new Administrative Users
    field descriptions 71
Add new Administrative Users field descriptions 71
Add New Role 185
Add Platform 1364
add resources; selected groups 166
Add service to user 620
add SNMP Access profile 912
Add Station Template 744
add subscribers
    Messaging field descriptions 648
add System Platform 930
Add To New Group 165

adding
Appliance Virtualization Platform host 1356
AVP host 1356
Communication Manager 932
communication profile for user 248
encryption passphrase 1484
ESXi host 1356
location 1354
remote key server 1486
software-only platform 1362
subject names for an entity class 1228
syslog server 1424
trunk group 790
vCenter to SDM 1419
Adding
administrative user 68
listen-only 782
Service Observe 782
so-coach 782
adding a CM Endpoint profile 253
adding a contact in contact list 265
adding a CS 1000 profile 259
Adding a data module
data modules; adding 810
adding a local WebLM server 1065
adding a messaging profile 256
adding a postal address of a private contact 273
adding a private contact 271
adding a shared address 610
adding a trunk group 790
adding a trusted certificate to Communication Manager . 1493
adding a user address 244
adding a vector routing table 697
Adding a VMPro Call Flow template 1177
Adding a VMPro System Configuration template 1174
Adding AD FS as Remote Identity Provider in System Manager 1286
adding additional certificate 1211
adding agent 663
adding agents in bulk
agents; bulk add 665
adding an announcement 677
Adding an Application Server Configuration template 1171
adding an audio group 688
adding an element access profile 917
adding an entity class 1222
adding an IP Office endpoint profile 261
adding an SNMP Access profile 912
adding an SNMP target profile 967
adding announcements 677
adding audio groups 688
adding certificates
available hosts 1395
existing hosts 1395
migrated hosts 1395
adding CM Agent template 1137
adding CM Endpoint template 1139
Adding Communication Manager certificate to the System Manager 1496
adding communication profile for user 248
adding communication profiles
IP Office endpoint 261
Adding corporate logo 66
adding coverage path
coverage path; add 702
adding coverage time-of-day
coverage time-of-day; add 711
adding custom role 177
adding dependencies to endpoints 838
adding endpoints 718
adding ESXi host 1356
adding hunt group 786
adding IP Office endpoint template 1161
adding IP Office system configuration templates 1165
adding location 1354
adding location to host 1421
adding new instance of element 906
Adding off PBX endpoint mapping 795
adding Officelinx to System Manager 937
adding Remote Servers 1111
adding resources to a selected group 166
adding subnetworks 916
adding subscriber templates
field descriptions 1153
adding subscriber templates MM; field description 1158
adding subscriber templates; field description 1156
adding synchronization datasources 75
adding templates
subscriber 1142
adding trusted certificate
primary to secondary server 103
secondary to primary server 121
adding trusted certificates 1205
WebLM 1064
adding UDP entries 833
adding udp group 828
adding uniform dial plan group 828
adding Utility Services to System Manager 932
adding vCenter to SDM 1419
adding vector directory number
vector directory number; add 694
additional certificate
adding 1211
additional identity certificate
removing 1213
Additional Post Login Banner Message 65
address, deleting 245
administration
Session Manager communication profile 250
administrative user
adding 68
editing details 68
enabling 69
Administrative user

Administrative user *(continued)*
deleting ... 70
editing roles ... 69
viewing details ... 68
administrative user details
editing ... 68
Administrative user sessions
terminating ... 70
Administrative Users ... 209
field descriptions ... 70
Administrative Users field descriptions ... 70
administrator privilege
logon information ... 45
adopter application
cannot communicate with WebLM ... 1062
Advance Options Presence Integration ... 767
advanced search
searching announcements ... 683
searching endpoints ... 724
AES
user management ... 148
agent
adding dependencies ... 838
Agent editor
permissions ... 191
Agent Management page ... 872
agent template
field description ... 1147
agent template field description ... 1147
agents ... 663
download excel template ... 668
exporting all agents ... 667
exporting selected agent ... 666
field description ... 668
importing agents ... 667
agents field descriptions ... 668
agents list ... 663
agents; bulk delete ... 666
Alarm List page ... 1012
alarm status
changing ... 1004
alarm threshold
edit alarm backup ... 1008
alarm threshold; view alarm backup ... 1008
alarm throttling; change ... 1006
Alarming ... 1003
Alarming UI ... 886
alarms
CS 1000 ... 134
delete ... 1005
exclude ... 969
exporting ... 1005
forward from secondary to primary System Manager ... 1010
include ... 969
remote key server ... 1004
standby mode ... 1010
alarms *(continued)*
viewing ... 1004
Alarms for IP Office ... 147
alarms; search ... 1006
alert message at login ... 41
all announcements; backup ... 679
all coverage paths ... 704
all endpoints ... 731
all hunt groups ... 788
all vector directory numbers ... 696
Allocations by Local WebLM ... 1081
Allow access to Administrative Users Web UI ... 209
alternate source ... 1326
upgrades ... 1328
Always Use
Station ... 756
analyze inventory
SDM ... 1349, 1399
analyze job status ... 1472
announcement ... 675
add ... 677
new ... 677
Announcements
field descriptions ... 684
announcements list ... 676
announcements; backup ... 679
announcements; broadcast ... 681
announcements; delete ... 678
announcements; download ... 679
announcements; edit ... 677
announcements; filter ... 683
announcements; move ... 680
announcements; restore ... 680
announcements; save ... 678
announcements; view ... 678
anonymous communication profiles ... 997
anonymous profiles ... 995
assign ... 995
delete ... 996
answer ... 778
appender; modify ... 1032
Appliance Virtualization Host
configure login banner ... 1386
push login banner ... 1386
Appliance Virtualization Platform ... 1373, 1376, 1381
change password ... 1379
generating kickstart file ... 1369
license file ... 1383
restarting ... 1391
shutting down ... 1391
update ... 1391
WebLM Configuration ... 1383
Appliance Virtualization Platform host Gateway
change ... 1371
edit ... 1371
Appliance Virtualization Platform host IP address
change ... 1371

Appliance Virtualization Platform host IP address *(continued)*
edit ... 1371
Appliance Virtualization Platform host password
changing ... 1379
Appliance Virtualization Platform network parameters ... 1371
application
deleting ... 1403
edit ... 1402
monitoring ... 1418
re-establishing trust ... 1400
restart ... 1405
start ... 1405
stop ... 1405
Application Deployment
field descriptions ... 1408
application instance
create ... 906
new ... 906
application instances ... 904
Application management ... 1353
application management page ... 70, 71, 941
Application Server System Configuration template
field descriptions ... 1173
applications
preupgrade check ... 1351
Applications ... 1427
applying
third-party certificates to Appliance Virtualization Platform ... 1232, 1386
Applying a VMPro call flow template on a device ... 1179
Applying a VMPro System Configuration template on a device ... 1176
Applying an Application Server Configuration template ... 1173
Applying an IP Office system configuration template on an IP Office device ... 1167
Argument ... 763
ASP_SSH
enable ... 1367
Assertions ... 1278
assign
tenant administrator ... 1297
assign groups
multiple users ... 239, 240
single user ... 239
Assign Groups ... 364
assign groups to user ... 364
assign permissions in Scheduler ... 1118
assign permissions in Solution Deployment Manager ... 180
Assign Role page ... 363
Assign Roles page ... 363
assign roles to
single user ... 238
assign users ... 181, 243
Assign Users ... 186, 366
assign users to role ... 181
assign users to roles ... 243
assigned elements
remove ... 927
assigned resources
remove ... 157
assigning
shared address to user ... 245, 609
assigning an appender to a logger ... 1031
assigning anonymous profiles ... 995
assigning applications ... 927
assigning filter profile to serviceability agent ... 972
assigning permission to access UDP groups ... 835
Assigning permissions
CM templates ... 1141
assigning permissions in user management ... 191
assigning permissions through User Management ... 191
assigning range for endpoints ... 198
assigning resources ... 165
assigning resources to group ... 154
assigning roles to
multiple users ... 239
assigning users to role ... 181
association between IP Office endpoint profile and user
remove ... 264
asymmetric keys
regenerating ... 1289, 1290
Attach Appender page ... 1034
attach contacts page ... 266
attaching target profiles
CLI ... 982
Attendant
New Endpoint ... 746
attribute details defined in Delete user XSD ... 532
attribute details defined in Import User XSD ... 521
attribute details defined in the CM Endpoint profile XSD ... 533
attribute details defined in the Conferencing communication profile XSD ... 580
attribute details defined in the Messaging communication profile XSD ... 563
attribute details defined in the Session Manager communication profile XSD ... 572
Audible Message Waiting ... 756
audio groups ... 688
audio groups field description ... 690
audio groups; add ... 688
audio groups; delete ... 689
audio groups; edit ... 688
audio groups; more actions ... 689
audio groups; view ... 688
audit logging
configuring ... 1041
audit logging configuration
field descriptions ... 1041
audit logging configuration field descriptions ... 1041
audit reports ... 992
Audix Name ... 753
authentication
Kerberos server ... 1274

authentication scheme
edit ... 1272
authentication servers
field descriptions ... 1275
provisioning ... 1273
authentication servers field descriptions ... 1275
authorization code ... 822
authorization code field description
authorization code; field description ... 824
authorization code list ... 823
auto ... 778
Auto activation of serviceability agents ... 974
Auto answer ... 778
field descriptions ... 779
Auto Answer
Station ... 747
Auto Select Any Idle Appearance ... 756
auto-refresh log list page ... 1040
automatic alternate routing digit conversion ,
aar digit conversion ... 801, 804
ars digit conversion ... 801, 804
automatic route selection digit conversion ... 801, 804
automatic call routes
using ... 254
automatic route selection toll field descriptions ... 807
automatic route selection toll list ... 806
automatic route selection toll,
ars toll ... 806
AutoRefresh Alarm List page ... 1011
Avaya Aura application
Services Port static routing update ... 1404
Avaya Aura application upgrade ... 1434, 1442
Avaya Equinox Management
SSO configuration ... 144
Avaya InSite Knowledge Base ... 1530
Avaya Multimedia Messaging ... 149
Avaya SIP AST endpoints ... 1301
Avaya Solutions Platform 130 Release 5.1 host
adding ... 1360
Avaya Solutions Platform S8300
generating kickstart file ... 1365
Avaya support website ... 1530
AVP license status ... 1385
AVP_Bulk_Import
bulk_import ... 1458
sample scenario ... 1458

B

B5800 endpoint templates
duplicate ... 1163
backing up all anouncements ... 679
backing up audio groups ... 689
backing up audio groups; field description ... 690
backup ... 848, 850
remote server ... 853
backup alarm
backup alarm *(continued)*
edit system manager backup ... 1008
backup alarm; system manager backup ... 1008
backup and restore ... 848, 850
Backup and Restore page ... 862
backup and restore service; access ... 851
backup and restore time ... 860
backup encryption
enabling ... 852
Backup field descriptions ... 863
backup file size ... 860
backup files; view ... 851
backup of announcements ... 679
bidirectional synchronization ... 72
Bindings ... 1278
Bridged Appearance Origination Restriction ... 761
Bridged Call Alerting ... 747
Bridged Idle Line Preference ... 756
broadcasting an announcement ... 681
broadcasting announcements ... 681
browser requirements ... 34
Building
Station ... 762
built-in roles ... 171
Built-in roles ... 171
bulk add endpoint; field descriptions ... 776
bulk delete endpoints ... 723
bulk deleting agents ... 666
bulk deleting endpoints ... 723
bulk edit
users ... 222, 224
bulk export ... 368, 374
key features ... 374
bulk export of global user settings ... 399
bulk export of users ... 381
bulk export of users partially ... 391
bulk export users ... 380
bulk export utility ... 925
bulk import ... 368, 374
global settings options ... 397
global user settings ... 398
key features ... 374
bulk import and export ... 368, 374
bulk import and export of user by using Excel file ... 370
bulk import and export with Excel ... 368
Bulk import of elements ... 906
bulk import of global user settings ... 397, 398
bulk import of partial user attributes ... 390
bulk import of users ... 377
bulk import users ... 375
bulk import XML for users with SIP phone ... 590
bulk user
delete ... 223
bulk user edit job
view ... 222
Bulk User Editor ... 224
Busy

Busy *(continued)*
Coverage Path 707
Button Assignment 763
Button Feature 763
Button Label 763

C

CA certificate 1283
CA certificate exchange
Avaya Equinox Management and System Manager ...143
Cable 761
Call Appearance Display Format 754
Call Forwarding 763
cancel
global user settings import job 403
cancel a global user settings import job 403
cancel a user import job 395
cancelling
endpoint migration job 739
capabilities
Solution Deployment Manager client 1317, 1322
System Manager Solution Deployment Manager 1317
capability comparison
System Manager Solution Deployment Manager and client capabilities 1317
CDR Privacy 757
centralized licensing 1056
adding elements 1058
disable 1061
enable 1057
overview 1056
certificate
authentication 45
generation capabilities 1199
management capabilities 1199
view 1238
Certificate authorities 1232
Certificate Authority 1247
Certificate Enrollment 1238
certificate generation 1234
certificate keystore
generate 1236
certificate renewal 1218
certificate response 1249
certificate revocation list 1260
certificate signing request 1247
Certificate Signing Request
create 1235
certificate update
ESXi host 1394
vCenter 1394
VMware documentation 1394
certificate using CSR
create 1238
certificate-based authentication
overview 45
certificates
accepting 1393
generating 1393
revoking 1221
unrevoking 1221
viewing 1220
Certification
validation 1392
Certification validation 1392
change
Appliance Virtualization Platform host IP address 1371
Host/ IP Settings 1373
network settings 1376
Network Settings 1373
change abbreviated-dialing enhanced 762
change communication profile password 212
change FQDN
primary System Manager 1508
change FQDN in the primary System Manager 1508
change FQDN on primary System Manager 1508
Change Gateway 1376
change H323 and SIP passwords 210
change IP address
primary System Manager 1508
change IP address and FQDN on primary and secondary System Manager 1507
change IP address for AVP host 1371
change IP address on primary System Manager 1508
Change IP address on primary System Manager 1508
Change IP FQDN 1402
change Netmask for Appliance Virtualization Platform host 1371
Change Network Params 1371
Change Password page 43
changeIPFQDN command, ...1505
changing
alarm status 1004
DNS 1503
encryption passphrase 1484
FQDN 1503
Gateway 1503
IP address 1503
IP address and default gateway 1382
Netmask 1503
password policy through CLI 57
search list 1503
System Manager TLS version 1189
changing a managed element's FQDN 1506
changing a managed element's IP address in System Manager 1506
changing allocations of a licensed feature 1070
changing System Manager IP address in managed elements 1506
changing the Appliance Virtualization Platform host password 1379
changing the TLS version of primary and secondary System Manager 1190

changing to classic view 662
checking
backup failure 849
checklist
Branch Session Manager upgrade 1435
Session Manager upgrade 1435
choose a shared address for a private contact 601
Choose Address page 247
Choose Group page 169
choose parent group 170
choosing
shared address 245, 609
choosing a shared address for a private contact 274
cipher suite list 1189
class of service 819
messaging 645
Class of Service
COS List 646
class of service data; edit 819
class of service data; view 819
class of service field description 820
class of service group field descriptions
class of service group; field description 826
class of service group list 824
class of service group,
cos group 824
system; class of service group 824
class of service list; field description 820
class of service list; filter 819
clean up communication profiles 996
CleanUp 996
Clearing the Delete on Unassign from User or on Delete User check box 845
Clearing the Delete on Unassign from User or on Delete User check box for users in bulk 845
CLI 979–985
SSH 48
CLI access
certificate-based 48
client audit 1087
Client node locking 1050
client Solution Deployment Manager 1315
cluster level alarming 1003
Cluster Session Manager 808
CM Agent template
upgrade 1136
view 1138
CM Agent template;
add 1137
copy 1138
delete 1138
edit 1137
CM audit 992
CM audit field description 993
CM audit report field descriptions 993
CM audit report; field description 993
CM Endpoint profile
CM Endpoint profile *(continued)*
delete 255
CM Endpoint template
upgrade 1136
CM Endpoint templates
add 1139
copy 1141
delete 1140
edit 1139
view 1140
CM notify
configure two-way TLS 1496
CM notify sync feature 1490
CM objetcs 657
CM station data
export 368
import 368
CM templates
permissions 1141
collection
delete 1528
edit 1528
generating PDF 1528
sharing content 1528
command 1218
changeIPFQDN 1505
configureOutboundFirewall 1192
ConfigureSyslog 1042
configureTimeZone 1523
editHosts 1521
exportUpmGlobalsettings 399
logRetention 871
manageEntityClassWhitelist 1226
outboundConnectionLogging 1191
pruneAllLogs.sh 872
runRTSCli.sh 925
setSecurityPolicy 55
updateLogRetention.sh 871
command runRTSCli.sh 925
common causes
application deployment failure 1408
communication address
modifying 249
Communication Manager
adding 932
Multi Tenancy 1302
Communication Manager audit 993
Communication Manager capabilities 653
Communication Manager data 985
Communication Manager notify sync 1490
Communication Manager objects 657
Communication Manager objects; add
adding Communication Manager objects 660
Communication Manager objects; changing to classic view 662
Communication Manager objects; delete
deleting Communication Manager objects 661

Communication Manager objects; edit
Communication Manager objects; edit 661
Communication Manager Session Manager correlation 842
Communication Manager templates
permissions 1141
Communication Manager update 1401, 1437, 1439
Communication Manager upgrade from Software Management 1433
Communication Manager upgrade from System Manager 1433
Communication Manager; adding a trusted certificate 1493
communication profile
adding 248
CM Endpoint profile for a user 252
Messaging profile for a user 256
Presence 252
Communication profile 285
communication profile for a user
deleting 248
communication profile password history policy 614
communication profile password policy
edit 615
Communication Profile Password Policy field descriptions 616
communication profile password strength policy 614
communication profile worksheets
communication profile hierarchy 372
hierarchy 372
parent-child communication profile 372
relationship 372
worksheets 372
communication profiles 247
clean up 996
delete 996
communication profiles synchronization 994
communication profiles; synchronize 994
Company ID 1327
completed jobs 1121
view 1120
Completed Jobs Page 1125
Conf/Trans On Primary Appearance 757
configuration 377, 389
IP Phone Group ID 754
Meeting Exchange element 137
Messaging 139
syslog server 1424
Configuration and Network Parameters
Communication Manager 1408
configuration management 872
configuration options for bulk import of users 389
configuration options for bulk import through Excel 377
configure
Geographical Redundancy 112
health monitoring timeout interval 115
Hosted Service Provider on System Manager 1280
login banner on host 1386
Remote Identity Provider 1280
configure alarm throttling 1006
configure an expired sub CA 1259
configure backup alarm; threshold 1007
configure centralized licensing 1057
field description 1057
field descriptions 1057
configure CS 1000 SNMP alarms 134
configure customized interface
field descriptions 67
configure enterprise licensing 1062
configure FTP server as remote server 1336
Configure options 1001
Configure Presence Server 138
configure remote server
protocol support 1334
configure revocation information in SubCA 1250
configureNTP 1522
configureTimeZone 1523
configuring
audit logging 1041
Avaya Services registration 939
cipher suite list on System Manager 1189
CRL download 1265
email properties 1108
Geographical Redundancy 103
IP Phone Group ID 755
Multimedia Messaging 149
outbound firewall rule 1194
periodic report cleanup 1110
remote syslog server from CLI 1043
report properties 1110
SAL Gateway 939
single-user mode credentials 44
System Manager as local software library 1333
WebLM Server on Appliance Virtualization Platform 1384
Configuring
external admin connect properties 1109
GR-unaware elements 127
configuring audit logging 1041
Configuring Communication Manager during GR failback . 132
Configuring Communication Manager during GR failover . 131
Configuring Communication Manager during GR failover when only the primary is reachable 132
configuring communication manager user profile settings . 654
Configuring CS 1000 134
Configuring DTLS for CS 1000 1259
configuring EASG
during G430 and G450 Branch Gateway upgrade ... 1478
gateway 1478
configuring endpoints 836
configuring IP Office 874
field description 874
configuring IP Office in Active-Active scenario 147
Configuring IP Office in normal operation with SCEP disabled 146
Configuring IP Office in normal operation with SCEP enabled 145

Configuring IP Office when primary is active 145, 146
configuring IP Office when primary nonfunctional 147
Configuring Linux-based CS1000 servers 135
Configuring Messaging during GR failback 141
Configuring Messaging during split network 142
Configuring Messaging in normal operational mode 139
Configuring Messaging when primary server is
nonoperational 140
configuring notify sync 1494
configuring NTP server 1522
configuring Out of Band Management on System
Manager 1500, 1501
configuring periodic 1110
configuring periodic cleanup 1110
configuring periodic cleanup for reports 1110
Configuring Presence Server 138
configuring Remote Servers 1111
Configuring Remote Servers 1111
configuring report 1110
configuring report properties 1110
Configuring Session Manager Release 6.2 and earlier
during failback 129
configuring Session Manager Release 6.2 and earlier
during GR failover 129
Configuring SIP TLS for CS1000 1260
configuring time zone 1523
configuring trap listener 897
configuring trust management 898
configuring two-way TLS 1496
Configuring user settings 1327
Configuring VxWorks-based CS1000 servers 135
configuringfor GR
IP Office 145
confirming identity certificate updates 1258
Connection Pooling 998
configure 998
create 998
edit 998
field descriptions 1000
connectivity status of the local WebLM servers 1067
console
Tenant Management 49
contact
add in default contact list 265
modify 265
Contact Center
reconfiguring 148
contact list member
edit 268
contacts
attach 266
content
publishing PDF output 1528
searching 1528
sharing 1528
sort by last updated 1528
watching for updates 1528
Continue on Error 745
convert
to stand-alone 114
convert .CADF xml file to MIB and trapd 963
converting .CADF xml file to MIB and trapd 962
converting .wav audio files 1169
converting .wav to .c11 audio file format 1169
converting primary System Manager server to a
standalone server 1243
converting to .c11 audio files 1169
cookie domain value
SSO 1503
copy
permission 187
Copy All From 187
Copy from Role 187
copy group 152
copying
CRL 100
copying CM Agent template 1138
copying CM Endpoint templates 1141
copying permission mapping for a role 182
COR 744
Cord Length 762
corporate logo
add 66
Corporate logo 35
Corporate Logo 66
correcting ESXi host certificate 1394
correlation 842
COS 645
Station 744
courses 1529
Coverage After Forwarding 748
Coverage Msg Retrieval 757
Coverage Path 705
Coverage Path 1 or Coverage Path 2 744
Coverage Path Description 706
coverage path list
coverage; coverage path list 702
Coverage Path Number 706
coverage path,
coverage; coverage path 702
coverage path, exporting 704
coverage time-of-day list 710
coverage time-of-day,
coverage; coverage time-of-day 710
create
new user profile 213
profiles 907
site 1294
team 1294
tenant 1294
tenant organization 1294
user account 213
virtual machine 1396
create certificate signing request 1234

Create Discovery Profile
field descriptions ... 910
create discovery profiles ... 907
create duplicate groups ... 152
create filter profiles ... 973
create new Certificate Authority with SHA2 and 2048 ... 1240
create new Certificate Authority with SHA256withRSA and 2048 ... 1240
Create New Profile if it doesn't exist for the user ... 223
create synchronization job ... 84
Create Tenant page ... 1305
create user
user provisioning rule ... 214, 215
create using user provisioning rule
user profile ... 214
createCA ... 1240
creating
browser certificate ... 46
duplicate user provisioning rule ... 622
generic CSR ... 1234, 1388
new CRL ... 1260
user provisioning rule ... 621
creating a browser certificate ... 46
Creating a Certificate Signing Request ... 1235
creating a new communication address for a profile ... 249
creating a new port ... 929
creating a new root CA
command CreateNewCA ... 1241
using option 1 ... 1241
creating a new root CA and making it the default CA
command All ... 1244
using option 3 ... 1244
creating a role in vCenter ... 1418
creating access profile ... 927
creating an end entity ... 1235
creating an SNMP target profile ... 967
creating an SNMPv3 user profile ... 964
creating basic reports ... 1101
Creating certificate using certificate signing request ... 1238
creating data backup on remote server ... 853
creating detailed reports ... 1100
creating discovery profiles ... 907
creating duplicate groups ... 152
creating duplicate user provisioning rule ... 622
creating duplicate users ... 220
creating groups ... 151
creating log harvesting profile ... 1017
creating new instance ... 906
creating new user account ... 213
creating notification filter profile ... 970
Creating NRP ... 840, 841
Creating NRP groups ... 840, 841
creating SCS profiles ... 919
creating software library ... 1341
creating SRS profiles ... 919
creating system data backup on a local server ... 852
creating target profiles
creating target profiles *(continued)*
CLI ... 981
creating use profile ... 643, 645
creating user profile using user provisioning rule ... 214
creating user profiles
CLI ... 980
creating user provisioning rule ... 621
creating user synchronization job ... 84
creation
new CRL ... 1260
Criteria for migrating 96x1 SIP set type to J1xx set type ... 732
CRL
configuring download ... 1265
configuring download job ... 1265
creating new ... 1260
deleting download job ... 1267
download ... 1265
overview ... 1260
scheduling download ... 1265
scheduling download job ... 1265
viewing download job ... 1267
CRL download
configuring ... 1265
scheduling ... 1265
CRL download configuration
field descriptions ... 1267
CRL download configuration field descriptions ... 1267
CRL download job
deleting ... 1267
viewing ... 1267
CRL download job details
field descriptions ... 1268
CRL download job details field descriptions ... 1268
CS 1000
functionality limitations ... 136
CS 1000 account operations ... 998
CS 1000 alarms
configure ... 134
CS 1000 configuration ... 134
CS 1000 profile administration ... 259
CS1000 Presence users ... 261
CS1000 server
configuration ... 135
CSR
create ... 1235
create field description ... 1389
edit field description ... 1389
CSR create ... 1234
custom patch
upload ... 1452
custom reports ... 1098
custom role
add ... 177
delete ... 184
edit ... 183
custom roles ... 176
Custom roles ... 171

custom templates 1135
custom tenant administrator role
add 178
Customized
interface 66
logo 66
Customized interface 66
Customized Interface field descriptions 67
customizing 1106
customizing reports 1106
Cvg Enabled for VDN Route-To Party 706
CVG Path 713

D

dashboard
login 39
Dashboard
System Manager 35
data backup
remote server 853
data backup from local server 857
data backup; schedule 854, 855
data encryption 1483
overview 1482
password policy 1483
remote key server 1483
Data entry warning in Excel 374
Data entry warning in Microsoft Excel 374
Data link error in Excel 373
Data link error in Microsoft Excel 373
data module list 809
Data Modules 809
data modules field descriptions
data modules; field descriptions 811
data replication 1086, 1087
data replication service 1086
Data Restriction 757
data retention
applying data retention rule 870
editing data retention rule 870
field descriptions 870
modifying data retention rule 870
data retention rules 868
excluded log files from log purging 868
Data Transport Config field descriptions 880
Data Transport Static Config page 883
database replication 95
Database size 860
date and time configuration; verify 1522
deactivate
secondary server 109
Decommissioning Communication Manager from System Manager 847
Default ACL 613
default contact
add contact list 265
default end entities
use new CA 1253
Default Policy rule 613
default templates 1135
Defining claim rules 1285
delete
element 951
global user settings import job on first error 403
hunt group 787
remote syslog servers 1045
role 184
subscriber templates 1144
subscribers 647
tenant 1299
trunk group 791
unused port 1378
delete a global user settings import Job 403
delete a user import job 395
Delete agents associated with CM users 844
delete alarms 1005
Delete ALL 1005
delete ca 1256
Delete Confirmation Page 1133
delete contact addresses of a public contact 602
delete custom role 184
delete element 925
delete element access profile 918
Delete Element Confirmation page 951
delete element instance mapping 1060
delete element instances 1060
delete filter profiles 973
Delete Group Confirmation page 163
delete IP Office endpoint profile of a user 263
Delete IP Office field description 961
Delete local WebLM page 1077
delete Local WebLM server 1077
delete mapping 1060
delete postal addresses of a public contact 601
delete public contact of a user 599
Delete Selected 1005
delete SNMP Access profile 912
delete SNMPv3 user profiles 965
delete subca 1256
delete users in bulk 223
Deleted Trusted Certificate Confirmation page 1210
deleted user
restoring 243
Deleted Users page 365
deleting
application 1403
communication profile 248
CRL download job 1267
endpoint migration job 740
expired certificates 1270
location 1355
metering collector configuration 1084
subject names for the entity class 1231

deleting *(continued)*
syslog servers 1426
upgrade jobs 1473
user provisioning rule 623
Deleting
administrative user 70
deleting a communication address 250
deleting a communication profile 248
deleting a location 1355
deleting a port 929
deleting a profile 1019
Deleting a Remote Server 1112
deleting a shared address 610
deleting a station profile 258
Deleting a VMPro Call Flow template 1179
Deleting a VMPro System Configuration template 1175
deleting access profile 928
deleting agent
agents; delete 664
deleting agents in bulk 666
deleting an address 245
deleting an announcement 678
Deleting an Application Server System Configuration
template 1172
deleting an audio file in IP Office system configuration
template 1169
deleting an audio group 689
deleting an CM Endpoint profile 255
deleting an element access profile 918
deleting an element instance 1060
deleting an SNMP target profile 969
deleting an SNMPv3 user profile 965
deleting announcements 678
deleting anonymous profiles 996
deleting audio groups 689
deleting bulk user edit jobs 223
deleting CM Agent template 1138
Deleting CM configuration from inventory 846
deleting CM Endpoint templates 1140
Deleting CM from the Manage Endpoints page 846
Deleting CM users permanently from SMGR 844
Deleting communication profile from users in bulk 845
deleting completed jobs 1121
deleting contact addresses of a private contact 276
deleting contacts from the contact list 266
deleting coverage path
coverage path; delete 703
deleting coverage time-of-day
coverage time-of-day; delete 712
deleting data modules
data modules; delete 811
deleting element instances 1060
deleting endpoints
removing endpoints 721
deleting entity class 1223
deleting files from software library 1346
deleting groups 152
deleting hunt group 787
deleting instances 1060
deleting IP Office endpoint templates 1163
deleting IP Office system configuration templates 1166
deleting jobs 1121
deleting notification filter profile 971
deleting pending jobs 1121
deleting postal addresses of a private contact 274
deleting private contact of a user 273
deleting reports 1110
deleting scheduled backup job 856
deleting SNMP Access profile 912
deleting SNMP target profiles 969
deleting software library 1342
deleting subnetworks 916
deleting subscriber templates 1144
deleting synchronization datasource, ... 77
deleting templates
subscriber 1144
deleting trunk group 791
deleting udp group 830
deleting uniform dial plan group 830
deleting user provisioning rule 623
deleting user synchronization job history 88
deleting user synchronization jobs 86
deleting vCenter 1421
deleting vector directory number
vector directory number; delete 694
deleting vector routing tables
vector routing table; delete 698
department
create 1294
editing 1299
viewing 1298
deploy
Branch Session Manager 1396
Communication Manager 1396
Session Manager 1396
System Manager 1396
Utility Services 1396
deploy application 1353
deploy Avaya Aura application 1396
deploy OVA 1396
Desktop Video Conferencing 751
detaching target profiles
CLI 982
determine System Manager that manages GR-aware
element 923
device list 908
Direct IP-IP Audio Connections
Attendant Console 757
directory synchronization 72
Disable Confirmation page 1131
disable self provisioning 211
disabling
completed jobs 1122
Geo Redundancy replication 106

disabling *(continued)*
local key store 1488
outbound connection logging 1192
outbound firewall rule 1196
pending jobs 1122
SSH on Appliance Virtualization Platform 1380
SSH on 1366
Disabling
administrative user 70
disabling centralized licensing 1061
disabling security hardening 1187
disabling SSH 1381
disabling the Geographic Redundancy replication for System Manager 1243
disabling the outbound firewall rule 1196
disaster recovery 124
disaster recovery on primary server
add trusted certificate 121
configure CRL download 120
disaster recovery primary server
prerequisites 119
discover
device 908
discover 96x1 SIP set type 733
discover elements 907
Discover Now 909
Discover SCS server
field descriptions 921
discover SCS servers 919
Discover SRS server
field descriptions 921
discover SRS servers 919
discovering elements 907
discovering endpoints for migration 734
discovering SCS servers 919
discovering SRS servers 919
discovery
profiles 907
Discovery Job Status 909
discovery profiles
create 907
Discovery Profiles 909
field descriptions 909
disk space for
System Manager backup 850
display 1213
Display Client Redirection 757
Display Language 749
displaying
password policies 60
slots assignment and remote key server 1487
subject names for an entity class 1229
Displaying the password policies 60
distributing new root CA with Communication Manager 1242
distributing the new root CA with 96x1 series phones 1243
DND/SAC/Go to Cover
All 708
DND/SAC/Go to Cover *(continued)*
Coverage Path 708
Don't Answer 708
documentation
System Manager 1526
documentation center 1528
finding content 1528
navigation 1528
documentation portal 1528
domain control 784
domain control SIP endpoints
enable reachability 784
download
harvested log files 1022
download manager
downloading software releases 1479
uploading custom patch 1453
download software 1344, 1349
download version.xml
smgr-versionsxmls.zip 1330
downloading
System Manager PEM certificate 144, 1492
downloading an announcement 679
downloading announcements 679
downloading audio groups 689
downloading bulk import spreadsheet 1455
downloading excel template
coverage paths 705
download excel template 697
download excel template hunt groups 789
Downloading Excel template 379
downloading excel template endpoints 732
downloading harvested log files 1022
downloading new root CA 1241
downloading reports 1107
downloading smgr-versionsxmls.zip 1330
downloading the .pem file 1492
downloading the .pem file to Communication Manager 1492
downloading upgrade files 1479
DRS 1086, 1087
DRS client audit 1087
DRS clients 1087
duplicate
subscriber templates 1144
Duplicate Group page 164
duplicate groups; create 152
duplicate user provisioning rule
creating 622
Duplicate User Provisioning Rule
field descriptions 624
Duplicating a VMPro call flow template 1180
Duplicating a VMPro System Configuration template 1176
duplicating an endpoint 720
duplicating CM Agent template 1138
duplicating CM Endpoint templates 1141
duplicating IP Office endpoint templates 1163
duplicating subscriber templates 1144

duplicating templates
subscribers 1144
duration
backup and restore 860
CS 1000 account operations 998
DVC 751

E

EASG login overview
System Manager 1546
edit
application 1402
communication profile password policy 615
custom role 183
grace period 889
hunt group 786
scheduled job 1129
site 1299
subscriber templates 1143
Edit Address page 282, 611
edit agent data in bulk,
agents; bulk edit 665
Edit Appender page 1033
edit application 1402
edit assignment of a license file 1059
edit authentication scheme 1272
Edit Common Console Profile page 888
edit Communication Profile Password Policy
field descriptions 616
edit contact in a contact list 265
edit contact list member page 268
Edit Discovery Profile
field descriptions 910
edit element access profile 917
edit element instances 1060
Edit Element page 944
edit endpoint
field descriptions 743
edit endpoint extension
field descriptions 776
edit endpoint templates
field descriptions 743
edit filter profiles 973
Edit Group page 162
edit IPOffice.properties file 264
Edit Location 1355
edit logger 1031
Edit Logger page 1033
edit password policies
field description 52
Edit Platform 1364
Edit Private Contact List page 278
Edit profile Messaging field descriptions 879
Edit Profile SMGR Element Manager
field descriptions 894
Edit Profile SMGR Element Manager field descriptions 894
Edit Profile System Manager page 883
Edit Profile: Configuration page
Inventory 879
Edit Profile: Inventory page 879
Edit Profile: Trust Management field description 899
Edit Profile:Alarming UI page 886
Edit Profile:Communication System Management
Configuration page 876
Edit Profile:GracefulShutdown 889
Edit Profile:HealthMonitor UI page 889
Edit Profile:Licenses page 890
Edit Profile:Logging page 891
Edit Profile:Logging Service page 893
Edit Public Contact List page 604
Edit Scheduler Profile page 897
edit SNMP access profile 912
edit synchronization datasources 77
Edit Upgrade Configuration
AVP Configuration 1445
Element Configuration 1445
edit user
user provisioning rule 215
Edit User Provisioning Rule
field descriptions 624
edit users in bulk 222, 224
Edit vCenter 1422
editing
clusters 809
department 1299
generic CSR 1234, 1388
location 1355
team 1299
tenant 1299
trunk group 790
vCenter 1421
Editing
administrative user details 68
administrative user roles 69
completed jobs 856
pending jobs 856, 1121
editing a coverage path
coverage path; edit 703
editing a platform 1363
Editing a Remote Server details 1111
editing a trunk group 790
Editing a VMPro call flow template 1178
Editing a VMPro System Configuration template 1175
editing agent data
agents; edit data 664
editing an announcement 677
Editing an Application Server Configuration template 1172
editing an audio group 688
editing an element access profile 917
editing an IP Office endpoint profile 263
editing an SNMP target profile 968
editing an SNMPv3 user profile 964
editing announcements 677

editing audio groups 688
editing authorization code
authorization code; edit 823
Editing Automatic Alternate Routing Digit Conversion data
Automatic Alternate Routing Digit Conversion; editing data 802
editing automatic route selection digit conversion data
automatic route selection digit conversion; edit data .. 804
editing automatic route selection toll data
automatic route selection toll; edit data 807
editing class of service data 819
editing class of service group
class of service group; edit 825
editing CM Agent template 1137
editing CM Endpoint templates 1139
editing coverage time-of-day
coverage time-of-day; edit 711
editing data modules
data modules; edit 811
editing element instances 1059
editing entity class 1223
editing hunt group 786
editing inactive account deactivation policy
field descriptions 64
editing IP Office endpoint templates 1162
editing IP Office system configuration templates 1166
editing log harvesting profile 1018
editing notification filter profile 971
Editing Off PBX Configuration Set 792
Editing Off PBX Endpoint Mapping 795
editing password policies 51
editing Remote Servers 1111
Editing report 1105
Editing report parameters 1105
editing session properties 63
field descriptions 63
editing SNMP Access profile 912
editing SNMPv3 user profiles 964
editing software library 1341
editing subsciber templates CMM; field description 1156
editing subscriber templates 1143
editing subscriber templates Messaging
field descriptions 1153
editing subscriber templates MM; field description 1158
editing templates
subscriber 1143
editing tenant 1299
editing the location 1355
editing the login failure message 65
editing the login warning banner 64
editing the properties of an element instance 1059
editing the select all attribute 655
editing UDP entries 833
editing UDP Group 829
editing Uniform Dial Plan Group 829
editing upgrade configuration 1473
editing vCenter 1421
editing vector directory number;
vector directory number; edit 694
editing vector routing table 698
editing xmobile configuration
xmobile configuration; edit 797
editing, user address 244
EJBCA 1198, 1247
EJBCA to Sub CA 1247
element
add 906, 1462
create 906
create Communication Manager 922
create Messaging 922
delete 925, 951
edit 924
import 906
new 906
view 924
Element
Cut Through 784
element access profile
add 917
delete 918
edit 917
Element Access Profile Management 918
Element Cut-Through 657, 714
Element Cut-Through; access 714
element data export 925
element export from System Manager CLI 925
element instance
delete 1060
edit 1059
edit properties 1059
remove 1060
element instance field description 1060
element management 904
Element Manager
redirect CS 1000 user 259
element upgrade 1442
elements
discover 907
import 952
refresh 1348, 1398
Elements Geographic Redundancy manageability status matrix 127
elements upgrade
target release 1436, 1437
Emergency Location Ext 744
EMU Login Allowed 760
enable
commercial grade hardening 1183
military grade hardening 1184
Multi Tenancy 883
password strength policy 50
enable self provisioning 210
enabling 1057

enabling *(continued)*
backup encryption ... 852
certificate based authentication ... 46
Extended Hostname Validation ... 1271
FTP ... 1333
Geographic Redundancy replication ... 105
local key store ... 1488
Multi Tenancy ... 1293
outbound connection logging ... 1191
Setup.sh ... 1333
Setup.sh stop ... 1333
SSH on Appliance Virtualization Platform ... 1380
SSH on ... 1366
System Manager ... 1333
Enabling
administrative user ... 69
completed jobs ... 1122
pending jobs ... 1122
enabling backup encryption ... 852
enabling security hardening
security hardening ... 1186
enabling SSH ... 1381
Avaya Solutions Platform 130 ... 1367
checking SSH status ... 1367
enabling the Discover Endpoint eligible for migration job ... 734
enabling two-way TLS ... 1497
encryptionLocalKey ... 1488
encryptionPassphrase ... 1484
encryptionRemoteKey ... 1486
end entry
create ... 1235
end user change communication profile password ... 212
end user self provisioning ... 210, 212
endpoint ... 241, 242
adding dependencies ... 838
administration ... 716
change parameters globally ... 725
duplicate ... 720
management ... 716
save as template ... 721
endpoint display mode ... 766
Endpoint editor
permissions ... 191
endpoint extension ... 776
edit ... 722
editing endpoint extension ... 722
endpoint list ... 730
Endpoint options ... 836
endpoint template list ... 1145
endpoint template versions ... 1135
endpoints ... 716
add ... 718
assign range ... 198
change set type of endpoints ... 780
field-level RBAC ... 200
list trace station ... 728
range ... 197, 198
endpoints *(continued)*
releasing ... 726
remove dependencies ... 838
swap ... 777
Endpoints
Element Cut Through ... 784
endpoints, exporting ... 730
endpoints; bulk add
bulk add endpoints ... 722
Endpoints; bulk delete ... 723
endpoints; busy out
busy out endpoint ... 727
endpoints; delete ... 721
endpoints; edit
editing endpoints ... 719
endpoints; status
endpoint status ... 729
endpoints; testing
testing endpoints ... 727
endpoints; view
viewing endpoints ... 720
Enhanced Call Fwd ... 763
enrollment password ... 1202
generate ... 1202
Enrollment Password page ... 1203
ensuring certificate response ... 1249
Enterprise Configuration page ... 1072
Enterprise Java Beans Certificate Authority ... 1198
enterprise licensing
configure ... 1062
entity class
filter ... 1224
Equinox Conferencing
configuration ... 143
error codes ... 777
error codes for failout results ... 777
esxcfg-route ... 1382
esxcli network ip interface ipv4 set -i vmk0 -I ... 1382
ESXi host
adding ... 1356
restarting ... 1391
ESXi host certificate addition ... 1395
ESXi host certificate update ... 1394
ESXi host map to unknown location ... 1368
Event processor page ... 877
Example
bulk import and export of user by using Excel file ... 370
Excel
bulk import ... 377
Data entry warning ... 374
Data link error ... 373
export ... 368
import ... 368
import user ... 377
Excel file
bulk import and export of user ... 370
import users ... 581

excel template 697, 705
Excel template
download 379
excel template endpoints 732
excel template hunt group 789
exchanging CA certificate
System Manager and Avaya Equinox Management ...143
existing hosts
managing certificates 1395
existing vCenter
managing certificates 1395
export
communication profile 381
contacts 381
element 925
global user settings 399
user data 368, 374
user data to Excel 368
export CM Agent profile 368
export CM station data 368
export elements from System Manager CLI 925
export logs 1035
export users 380
System Manager web console 381
Export Users 384
exporting
alarms 1005
Exporting ADFS metadata 1285
exporting all coverage paths 704
exporting all endpoints 731
exporting all hunt groups 788
exporting all vector directory numbers 696
exporting coverage paths 704
exporting CS 1000 user data 643, 645
exporting endpoints 731
exporting hunt groups 788
exporting selected coverage path 704
exporting selected endpoints 730
exporting selected hunt group 788
exporting selected hunt group; hunt group 788
exporting selected vector directory number 695
exporting the user data 640
exporting vector directory number; vector directory
number 695
exporting vector directory numbers 696
exportUpmGlobalsettings command, ...399
extended hostname validation
overview 1271
extension
add 241
remove 242
Extension
Station 743
external authentication 1271
external server for upgrade 1332
external server; system requirements 1347

F

Favorite 763
feature options
voice mail number 761
Feature Options 747
field description
anonymous communication profiles 997
edit elements 1463
password policies 52
SNMP Access Profile 914
TrapListener service 898
User Settings 1331
field descriptions
Add Communication Manager 955
Add Entity Class 1225
Add Mapping 186
Add new Administrative Users 71
Add Platform 1364
Add Server 1112
Add Trusted Certificate 1207
Adding AES instance to System Manager 959
Administrative Users 70
Agent List 977
Allocations by Feature 1080
Application Server System Configuration template ...1173
Applications 1427
ars toll 807
Assigned Users 186
audit logging configuration 1041
authentication servers 1275
Auto answer 779
automatic route selection toll 807
Change Allocations 1082
change password 1380
Choose Address 247
Choose Group 169
corporate logo 67
Create ASP S8300 Kickstart 1365
Create AVP Kickstart 1369
create CSR 1389
Create Discovery Profile 910
Create New Profile 1024
Create Tenant 1305
CRL download configuration 1267
CRL download job details 1268
customized interface 67
data retention 870
Data Transport Config 880
Delete Group Confirmation 163
Deleted Users page 365
Discovery Profiles 909
Duplicate User Provisioning Rule 624
edit CSR 1389
Edit Discovery Profile 910
edit endpoint extension 776
Edit Group 162

field descriptions *(continued)*
Edit Location 1355
Edit Platform 1364
Edit Profile SMGR 883
Edit Profile SMGR Element Manager 894
Edit Public Contacts 604
Edit Remote Server 1112
Edit User Provisioning Rule 624
Element Access Profile Management 918
Element Cut-Through 714
Endpoint Migration 740
Endpoint Migration Job History 742
Enterprise Usage 1079
Export Users 384
Filter Profiles 973
Group Management 157
Harvest Archives 1026
Host Network / IP Settings 1376
Import Global Settings page 585
inactive account deactivation policy 64
IP Office System Configuration template 1168
Job History 1432
load AVP host certificate 1388
Locations 1427
login failure message 66
manage certificate revocation 1221
Manage Elements 941
Manage Entity Classes 1224
Manage Trusted Certificates 1204
Map vCenter 1421
Metering Collector Configuration 1084
Modify Access Profile Entry 919
Move Group 164
New Group 159
New Location 1355
New Public Contact List page 606
New Report 1102
New User Provisioning Rule 624
Notification Filter Profiles 973
Periodic cleanup of reports 877
Platforms 1427
Preupgrade configuration 1352
provision first LDAP server 1275
provision Kerberos server 1275
provision LDAP server 1275
provision RADIUS server 1275
provision SAML remote identity provider 1275
provision second LDAP server 1275
provision user certificate authentication 1275
Remote Server configuration 1112
Remote Server Configuration 1112
replace identity certificates 1216
Replica Nodes 1092
Replication Node Details 1095
Reports Definition List 1098
Reports Generation 1098
Reports History 1108

field descriptions *(continued)*
Resource Synchronization 165
revoke certificate 1222
Roles 184
schedule CRL download 1265
security configuration 1269
security settings 65
server properties 1062
Serviceability Agents 977
session properties 63
Shutdown System Manager 1313
SNMP Access Profiles 913
Subnet Configurations 917
synchronization job history 87
Synchronize CM Data and Configure Options 714
syslog receiver configuration 1425
System Manager Dashboard 37
Tenant Management 1305
UnAssign Roles 367
Update Entity Class 1225
Upgrade Configuration 1444
Upgrade Management 1442
User Bulk Editor 224
User Profile | Add 285
User Profile | Duplicate | <User Name> page 344
User Profile | Edit | <User Name> 307
User Profile | View | <User Name> page 328
User Provisioning Rules 224, 623
User Restore Confirmation Page 366
user synchronization datasource 78
user synchronization jobs 86
view by feature 1071
view certificate detail 1220
View Group 160
View License Capacity 1054
View Peak Usage 1055
View Profile SMGR 883
View Profile SMGR Element Manager 894
View Remote Server 1112
View Trust Certificate 1209
View User Provisioning Rule 624
Viewing job summary 89
WebLM Configuration 1385
WebLM Home 1053
field descriptions, Snapshot Manager 1390
field level RBAC 193
Communication Manager objects 193
field-level RBAC in endpoints 200
field-level RBAC in hunt group 204
field-level RBAC in trunk group 206
file download manager 1350
file replication 95
file size
bulk export user 388
file transfer settings; announcements 682
filling
bulk import spreadsheet 1455

filling *(continued)*
bulk instances 1455
filter
alarm 969
informs 969
notification 969
traps 969
filter profile
assign to serviceability agent 972
create 970
unassign from serviceability agent 972
filter profiles
CLI 983–985
Filter Profiles
field descriptions 973
filter users 236
filtering alarms 1005
filtering announcements 683
filtering class of service list 819
filtering Communication Manager objects
using filters; Communication Manager objects 662
filtering entity class 1224
filtering groups 156
filtering jobs 1120
filtering log harvesting profiles 1022
Filtering log harvesting requests 1023
filtering logs 1035
filtering resources 156, 167
filtering SNMPv3 user profiles 965
filtering subscribers
using filters; subscribers 648
filtering target profiles 967
filtering templates
filtering endpoint templates 1135
filtering subscriber templates 1135
using filters; templates 1135
finding content on documentation center 1528
finding port matrix 1527
FIPS mode 1254
firewall basics 1532
firewall implementation in System Manager 1532
Floor
Station 761
Form based authentication 1285
forward the secondary alarms to primary System
Manager 1010
Forwarded Destination 763
FQDN 1503
changeIPFQDN 1505
FQDN and IP address change on Geographic
Redundancy 1502
FTP Configuration (F) 1342
FTP server
configure as remote 1336
install 1336
functions
User Management scheduled job 1118

G

G430 and G450 Media Gateway multistep upgrade 1476
G430 Branch Gateway
add 936
G450 Branch Gateway
add 936
gateway protocol matrix 1480
gateway upgrade
multistep upgrade 1476
General Configuration Details 1445
general guidelines and capabilities
user provisioning rules 619
General Options 744
generate
end user communication profile password 211
generate certificate signing request 1247
generate communication profile password 211
generate identity certificates 1257
generate test alarm 1009
generate test alarms 1008
generate_report.sh 1416
generateTrapdAndMibUnix 963
generateTrapdAndMibUnix.sh 962
generating
certificate using CLI 47
certificates 1393
virtual machine report 1416
generating basic reports 1101
generating certificate
for cert-based authentication 47
generating certificate keystore 1236
generating detailed reports 1100
generating kickstart file
Appliance Virtualization Platform 1369
Avaya Solutions Platform S8300 1365
generating test alarms 1009
generic CSR
creating 1234, 1388
editing 1234, 1388
Geo Health 114
Geographic Redundancy
..... 108, 109, 114, 116, 117, 923, 930, 1087, 1502
auto-disable 107
backup and restore 850
disable 106
enabling 105
hardware resource or parameter 96
overview 91
prerequisite — Step 2 103
prerequisite Step 1 102
prerequisites 95
Geographic Redundancy field descriptions 116
Geographic Redundancy key tasks 97
Geographic Redundancy licenses 92
geographic redundancy prerequisites
overview 99

Geographic Redundancy replication 95
Geographic Redundancy terminology 92
geographical redundancy 121
Geographical redundancy 95
Geographical Redundancy 103, 112, 121–123
configuring 103
Get
Company ID 1327
Global Endpoint Change 725
global endpoint parameter change 725
global user settings import job
abort 402
GLS 150
GR failover 129
GR Health field descriptions 117
GR-aware element
manage 923
GR-unaware elements 127
graceful shutdown 888, 889
granular RBAC 188
group 840, 841
copy 164
duplicate 164
Group and Lookup Service 150
Group List 763
Group management 150
Group Management page 157
group membership 155
Group Membership 774
Group Name 186
group types 241
groups
copy 152
create 151
defined 774
delete 152
duplicate 152
filter 156
modify 151
move 153
view 151
guidelines
upgrading and updating elements 1435
guidelines for signing the certificate
certificate signing request 1248

H

H.320 Conversion
Attendant Console 758
H.320 Desktop Video Conferencing 751
H323 and SIP passwords 210
hardware and software prerequisites on primary and secondary servers 95
Harvest Archives page 1028
Harvest Criteria Edit page 1025
harvested log files; download 1022
Headset 762
health monitor 889
Health Monitor service 114
health monitoring
timeout interval 115
Hierarchy in communication profile worksheets 372
history
synchronization job 87
Holiday After Coverage 707
Holiday Coverage 706
Holiday Table 707
downloading excel template 693
exporting all holiday table 691
exporting selected holiday table 692
importing holiday table 692
Holiday Table List 691
host 1373, 1376
adding 1358
Host
update 1391
HTTP proxy 1264
adding 1262
checklist 1261
deleting 1263
editing 1262
field descriptions 1264
introduction 1260
overview 1260
HTTP/HTTPS Configuration (H) 1342
hunt group
add 786
assign range 202
delete 787
edit 786
field-level RBAC 204
view 786
Hunt Group List
field descriptions 785
Hunt Groups 785
Hunt-to Station 750

I

identity certificate 1210, 1247
identity certificate updates
confirm 1258
identity certificates 1213
making default 1213
renew 1215
replacing 1214
Identity Certificates page 1211
Idle Appearance Preference 758
impact of change in FQDN and IP address on Geographic Redundancy 1502
implicit permissions for Communication Manager objects .189
implicit permissions for range 189
import

import *(continued)*
elements ... 952
user data ... 368, 374
user data from Excel ... 368
Import as PEM certificate ... 1205
import CM station data ... 368
import CS1000 user data to User Management ... 642
import element; ... 906
Import Elements ... 952
Import from existing trusted certificates ... 1205
import from file ... 1205
Import Global Settings page ... 585
import job on the Scheduler page
view ... 396
import of users ... 377, 389
Import Status page ... 954
import the Subscriber Manager data ... 636, 637
import user
Excel ... 377
XML ... 377
import user considerations ... 392
import user data to User Management ... 635
import users ... 375
Import Users ... 581
Import using TLS ... 1205
Importing ADFS CA Certificate into System Manager ... 1283
importing coverage paths ... 705
importing CS 1000 Subscriber Manager data ... 643, 644
importing CS 1000 user data ... 643, 645
importing CS1000 Subscriber Manager data ... 642
importing endpoints ... 731
importing hunt groups ... 788
importing the Subscriber Manager data ... 643
importing the user data ... 640
importing trusted certificates from file ... 1205
importing vector directory numbers ... 696
inactive account deactivation policy field descriptions ... 64
Inactive session termination policy ... 63
Increase Paging Group Members ... 759
incremental synchronization
synchronizing Communication Manager data ... 989
information
to create Communication Manager ... 922
to create Messaging ... 922
initializing synchronization
force it ... 989
synchronizing Communication Manager data ... 988
install
Application Enablement Services ... 1319
Avaya Aura applications ... 1319
Avaya Aura Media Server ... 1319
Avaya Breeze ... 1319
Branch Session Manager ... 1319
Communication Manager ... 1319
SAL ... 1319
SDM ... 1319
Session Manager ... 1319
install *(continued)*
Solution Deployment Manager client ... 1319
System Manager ... 1319
WebLM ... 1319
install custom patches ... 1439
install custom software patches ... 1439
install FTP server ... 1336
install license file ... 1049
Install License page ... 1053
install on same ESXi ... 1464
install patches ... 1401, 1437
install services packs ... 1401, 1437, 1439
install software patches ... 1401, 1437
Install System Manager patch ... 1414
Install System Manager patches ... 1462
Installed Patches ... 1441
Installing and configuring an HTTP server as a remote
server ... 1335
Installing and configuring an SCP or SFTP server as a
remote server ... 1338
installing language pack
Canadian French ... 1525
Integrated Management transition ... 1098
Introduction ... 128
inventory
refresh elements ... 1348, 1398
IP address ... 1503
IP address and default gateway
changing ... 1382
IP address and FQDN change on Geographic
Redundancy servers ... 1507
IP Audio Hairpinning
Signaling Group ... 758
IP Hoteling ... 759
IP Office
add device ... 960
delete ... 961
reconfigure ... 148
synchronization ... 985
synchronizing system configuration ... 990
user management ... 148
IP Office Application Server
synchronize ... 990
IP Office configuration ... 145, 146
IP Office configuring for GR ... 147
IP Office endpoint profile ... 261
delete ... 263
edit ... 263
view ... 262
IP Office endpoint template
view ... 1162
IP Office endpoint template field description ... 1164
IP Office endpoint templates
add ... 1161
delete ... 1163
edit ... 1162
field description ... 1164

IP Office endpoint templates *(continued)*
remove ... 1163
upgrade ... 1164
IP Office GR configuration ... 145
IP Office GR configuration in Active-Active scenario ... 147
IP Office GR configuration when primary nonfunctional ... 147
IP Office profile field description ... 874
IP Office System Configuration
manage audio files ... 1168
IP Office system configuration template
upload audio files ... 1168
IP Office System Configuration template
field descriptions ... 1168
IP Office System Configuration template field
descriptions ... 1168
IP Office system configuration templates
add ... 1165
convert .wav to .c11 ... 1169
convert to .c11 ... 1169
delete ... 1166
delete audio files ... 1169
edit ... 1166
view ... 1166
IP Office; configure ... 874
IP Phone Group ID ... 754
IP Softphone ... 759
IP Video ... 757
IPOffice.properties file
remove association between IP Office endpoint
profile and user ... 264

J

Jack ... 761
Job Details page ... 584, 588
Job History ... 1427, 1432
Job Scheduling -Edit Job page ... 1129
Job Scheduling -On Demand Job page ... 1130
Job Scheduling -View Job page ... 1127
job summary
synchronization job history ... 89
Job summary ... 89

K

KB
Support site ... 1530
KERBEROS ... 1271
Kerberos server
provisioning ... 1274
Kerberos server provisioning ... 1274
key features
bulk export ... 374
bulk import ... 374
key size 2048 ... 1240
key tasks
Geographic Redundancy ... 97

L

LAC ... 1048
LDAP ... 1271
LDAP directory server ... 72–74, 215
LDAP replication ... 95
LDAP server
provisioning ... 45, 1273
LDAP server provisioning ... 45, 1273
LDAP server; provision ... 45, 1273
Library Server Details (L) ... 1342
License Activation Code ... 1048
license file ... 1047
add mapping ... 1059
install ... 1049
license file installation ... 1053
license files and elements ... 1058
License management ... 137
License management for Contact Center ... 148
Licensing
Geographic Redundancy ... 92
Life cycle management ... 1353
limitations
directory synchronization ... 74
Limitations of CS 1000 ... 136
Linkage ... 707
Linux-based CS1000 servers
configuration ... 135
list of XML Schema Definitions and Sample XMLs for
bulk import ... 403
list usage extension
hunt group ... 787
list usage extension in vector directory number
vector directory number; list usage extension ... 695
list usage extension; announcements ... 683
listing
slots assignment and encryption passphrase ... 1485
slots assignment and remote key server ... 1487
slots assignment and remote server ... 1485
listing agents
CLI ... 983
listing filter profiles
CLI ... 984
listing target profiles
CLI ... 982, 983
listing user profiles
CLI ... 981
load AVP host certificate
field descriptions ... 1388
local data backup
create ... 852
local software library
configure ... 1333
Local Survivable Processor(LSP) ... 1342
local WebLM ... 1074
local WebLM server
remove ... 1067

Localized Display Name 719
location
adding 1354
deleting 1355
editing 1355
view 1354
Location 747
Locations 1427
Lock Messages 745
lockout policy
password 51
log details; view 1035
log file; search for text 1020
log harvest requests; filter 1023
log harvest; access 1017
log harvester overview 1016
Log Harvester page 1024
log harvesting 1016
log harvesting profiles; filter 1022
log into System Manager 39
log on to System Manager
using EASG login 1547
Log Settings 1029
log types 1016
log viewer 1015
Log Viewer 1035
Log; log settings 1029
Logged off/PSA/TTI
Coverage Path 708
logger
edit 1031
logging 1015
Logging Configuration page 1030
logging on to System Manager
administrator privilege 45
Logging page 1036
logging service 1015
login details 40
login failure message
edit 65
field descriptions 66
Login Failure Message 65
login password
reset 921
login profiles
overwrite 920
overwriting profiles on devices 920
login warning banner 64, 65
edit 64
logo
add 66
Logo 66
logon banner 64
logon information
administrator privilege 45
Logs Settings service; access 1030
logs; export 1035
logs; log viewer 1035
logs; search 1036
Loss Group 752
LWC Activation 759
LWC Log External Calls 759
LWC Reception
Agent Login ID 752

M

MAC address of server 1062
mailbox administration
subscriber management 646
Mailing reports 1110
main, feature, expansion/module, and softkeys buttons ..1099
maintenance
clear amw all 728
making default certificate 1213
making the new CA as default System Manager CA
command MakeNewCADefault 1243
using option 2 1243
manage
applications 904
elements 904
GR-aware element 923
identity certificate 1210
tenant 1297, 1298
trusted certificate 1204
Manage
System Manager upgrades 1462
manage applications 904
manage audio field description 1170
manage certificate revocation field descriptions 1221
manage certificates 1198
manage elements 904, 930
Geographic Redundancy 923
Manage Elements field descriptions 941
manage entity classes 1222
Manage Entity Classes
field descriptions 1224
manage Presence access control lists 613
manage public contact list 598
manage resources 165
manage shared address 609
Manage Software 1433
manage software library files field description 1347
manage users 208
managed elements
changing System Manager IP address 1506
Management interface 1499
managing
command line password policy 56
Managing
outbound firewall rule logging 1198
managing certificates migrated hosts 1395
managing certification authorities 1245
Managing NRP 841

Managing NRP groups ... 841
Managing outbound firewall rule logging ... 1198
managing resources ... 165
managing SNMPv3 user profiles ... 975, 976
managing target profiles ... 975
managing tasks after running createCA utility ... 1245
managing user profiles ... 976
Manual addition of elements ... 906
map
  permission ... 187
  permission from template ... 187
map ESXi host to unknown location ... 1368
map permission ... 182
map permissions
  using templates ... 181
Map vCenter ... 1419, 1421, 1422
Map-to Station ... 749
mapping
  add ... 186
mapping elements and license files ... 1058
Media Complex Ext ... 753
media server ... 684
Meeting Exchange configuration ... 137
Meeting Exchange element configuration ... 137
Message Lamp Ext ... 744
messaging class of service ... 645
Messaging configuration ... 139
Messaging configuration in GR failback ... 141
Messaging configuration in operational mode ... 139
Messaging configuration in split network ... 142
Messaging configuration when primary is nonoperational ... 140
messaging COS ... 645
messaging data
  synchronize ... 992
Messaging data ... 985
Messaging field description ... 1153
Messaging field descriptions
  add subscriber ... 648
Messaging profile
  edit ... 879
  view ... 879
Metering Collector configuration
  overview ... 1083
MIB tool ... 962, 963
MIB.properties ... 963
MIBTOOL.jar ... 963
MIBXMLTAGS.properties ... 963
Microsoft Active Directory Federation Server (ADFS) ... 1282
migrated hosts
  managing certificates ... 1395
migrating
  96x1 SIP set type to J1xx endpoint ... 735
  all 96x1 SIP to J1xx set type ... 737
Migration of J-Series endpoints configured as 96x1 SIP set type ... 732
modify
  element access profile ... 919
modify *(continued)*
  port ... 929
Modify Access Profile Entry ... 919
modify appender ... 1032
modify details of a private contact ... 272
modify details of a public contact ... 599
modify element ... 924
modify FQDN
  primary System Manager ... 1508
modify IP address
  primary System Manager ... 1508
Modify local WebLM page ... 1075
modifying
  communication address ... 249
  user provisioning rule ... 621
modifying a CM Endpoint profile ... 254
modifying a contact address of a private contact ... 276
modifying a CS 1000 profile ... 261
modifying a local WebLM server configuration ... 1066
modifying a managed element's IP address and FQDN ... 1506
modifying a messaging profile ... 257
modifying a port ... 929
modifying a postal address of a public contact ... 600
modifying a shared address ... 610
modifying an access profile ... 928
modifying an appender ... 1032
modifying an IP Office endpoint profile ... 263
modifying contact in a contact list ... 265
modifying default end entities ... 1253
modifying groups ... 151
modifying postal address of a private contact ... 274
modifying SNMPv3 user profiles ... 964
modifying the communication address ... 249
modifying the details of a public contact ... 602
modifying user account ... 219
modifying user provisioning rule ... 621
modifying, user address ... 244
monitoring
  application ... 1418
  platform ... 1417
Mounting ... 762
Move Group page ... 164
move primary System Manager server ... 121, 122
moving an announcement ... 680
moving announcements ... 680
moving groups ... 153
Multi Device Access ... 251
Multi Tenancy ... 1292, 1294, 1297–1299
  Avaya SIP AST endpoints ... 1301
  Communication Manager ... 1301, 1302
  enable ... 883
  enabling ... 1293
  RBAC ... 1302
  scheduler ... 1302
  user management ... 1302
  user provisioning rule ... 1302
Multi Tenancy for Communication Manager ... 1302

Multi Tenancy for Communication Manager objects 1301
multibyte language 745
Multimedia Early Answer 759
Multimedia Messaging 149
multiple SIP endpoints
register 251
multiple users
assign groups 240
Music Source 761
Mute Button Enabled 760
MWI Served User Type 748

N

native name 719
network parameters
change 1376
new
role 185
new CRL
creation 1260
New Element page 944
New Group page 159
new identity certificates
System Manager 1257
New Location 1355
New Private Contact List page 277
new profile
create 223
New Public Contact List page 606
new reports 1101
new root CA
downloading 1241
new subscriber
templates 1142
New User Provisioning Rule
field descriptions 624
New vCenter 1422
Next Path Number 707
non sip endpoints 783
non-station objects; view
Communication Manager objects; view 661
notification filter profile
create 970
delete 971
edit 971
view 971
Notification Filter Profiles
field descriptions 973
Notification filtering 969
notification ID 971
notification IDs 973
notify sync feature 1490
notify sync on Communication Manager 1494
NRP groups 841
NRP sync 840
NRP sync feature 840
NTP server
configure 1522
Number of Rings 709

O

obtain the license file 1047
Off PBX Configuration Set
Edit 792
field description 792
View 792
Off PBX Configuration Set field descriptions 792
Off PBX endpoint mapping
add 795
Off PBX Endpoint Mapping
edit 795
field description 796
view 795
Off PBX Endpoint Mapping field description 796
Officelinx
adding to System Manager 937
on-demand job 1114
optional settings
security hardening 1185
Out of Band Management 1499
disable 1500
enable 1500
Geographic Redundancy 1501
overview
extended hostname validation 1271
geographical redundancy 99
Overview 127
overview of System Manager root certificate authority
using SHA256withRSA signing algorithm and 2048
key size 1239
Overwrite the existing outbound firewall rules 1197
overwriting
existing outbound firewall rules 1197
overwriting login profiles 920

P

parameters 1105
parent group 170
password
change 1380
Password aging policy enforcement 50
password change
Appliance Virtualization Platform host 1379
password history enforcement policy 51
password lockout policy enforcement 51
password policies
edit 51
password policies field description 52
password policy 615, 1379
communication profile 614
password rules 1379

password strength policy enforcement 50
peak usage for a licensed product 1051
peak usage; view 1051
pending jobs
    view 1120
Pending Jobs page 1123
pending jobs; stop 1123
pending jobs; view 1119
Per Button Ring Control 760
Per Station CPN - Send Calling Number 748
Performing a CM Audit 993
Periodic cleanup of reports 877
Periodic Status 1083
periodic status of master and local WebLM servers 1069
permission
    copy 187
    map 187
permission mapping 181, 187
permissions
    Scheduler 1118
    Solution Deployment Manager 180
Personal List 762
Personalized Ringing Pattern 749
phone view layout
    read only phone view 765
platform
    editing 1363
    monitoring 1417
Platforms 1427
PLDS
    finding LAC 1048
PLDS access 1326
PLDS access to Avaya 1327
Point1, Point2, … 709
port
    modify 929
Port 944
    Station 744
port matrix 1527
post login banner message 65
post operations after running CreateCA utility 1245
Pre-requisites in SMGR before decommissioning CM 843
Precedence Call Waiting 760
preferred languages 83
preparing CS 1000 Subscriber Manager data for import
        to System Manager 643
prerequisite
    Geographic Redundancy — Step 2 103
    Geographic Redundancy Step 1 102
prerequisites 95, 97
prerequisites before making the new root CA as default . 1242
Presence access control lists (ACLs) 613
Presence ACL 613
Presence communication profile administration 252
Presence Server
    configuration 138
preupgrade check
preupgrade check *(continued)*
    applications 1351
Preupgrade Configuration 1351
preupgrade job status 1472
primary server
    CRL addition 120
primary System Manager
    change FQDN 1508
    change IP address 1508
private contact
    add a contact address 275
    modify details 272
Private Contact 277
Problems in managing Session Manager 6.1 or 6.2 using
        System Manager 6.2 130
Profile 767
Profile Criteria View page 1026
Profile Settings 767
profiles
    discovery 907
Profiles 1278
Protocol consideration 1279
protocol matrix for upgrades 1480
protocol requirements to configure remote server 1334
protocol support
    software library 1334
provision
    users 618
provision Remote Identity Provider 1281
provisioning
    authentication servers 1273
    Kerberos server 1274
    LDAP server 45, 1273
    RADIUS server 1274
    user certificate authentication 1275
provisioning authentication servers 1273
provisioning Kerberos server 1274
provisioning LDAP server 45, 1273
provisioning RADIUS server 1274
provisioning user certificate authentication 1275
public contact
    add 598
    add contact address 601
    add postal address 600
    choose a shared address 601
    delete 599
    delete contact address 602
    delete the postal address 601
    modify details 599
    view details 600
public contacts 208, 608
Public Contacts
    field descriptions 602
Public interface 1499
push
    login banner on host 1386
push syslog 1425

pushing
syslog ... 1425

Q

Query Usage page ... 1079
querying usage of feature licenses for master and local WebLM servers ... 1069
Quick Navigator ... 35
quick start to importing users ... 588

R

RADIUS ... 1271
RADIUS server
provisioning ... 1274
raise alarm; notification ... 1007
range ... 188
endpoints ... 198
Range in endpoints ... 197
RBAC ... 171
built-in roles ... 171
custom roles ... 176
Re run
reports ... 1106
Re running reports ... 1106
Re-Calculate route pattern ... 837
re-establishing trust
application ... 1400
SDM elements ... 1400
Solution Deployment Manager elements ... 1400
re-establishing trust application ... 1400
reboot System Manager
from web console ... 1312
through command-line interface ... 1313
receiving certificate response ... 1249
reconfiguring AES ... 148
reconfiguring Contact Center ... 148
reconfiguring IP Office ... 147, 148
reconfiguring Visualization, Performance, and Fault Manager ... 148
recover primary server from disaster ... 124
redirect
CS 1000 user to Element Manager ... 259
Redirect Notification ... 760
redirecting CS 1000 to Element Manager ... 259
reestablish
connection ... 1415
Reestablish Connection ... 1427
refresh elements in inventory ... 1348, 1398
refresh elements job status ... 1472
refresh host ... 1363
refreshing
default password policy settings ... 62
refreshing the default password policy settings ... 62
regenerate certificate using FQDN ... 1395
regenerating
regenerating *(continued)*
asymmetric keys ... 1289, 1290
symmetric keys ... 1288
regenerating asymmetric keys
geographic redundancy disabled ... 1289
geographic redundancy enabled ... 1290
regenerating symmetric keys ... 1288
register
multiple SIP endpoints ... 251
Reimporting SSO cookie domain value ... 67
releasing endpoint ... 726
Relying party(RP) ... 1284
remote access
System Manager CLI ... 1546
System Manager web console ... 1546
remote backup server supported
ciphers ... 861
key exchange algorithms ... 861
mac algorithms ... 861
Remote Identity Provider ... 1280
Remote Identity Provider; provision ... 1281
remote library ... 1342
Remote Off-hook Attempt ... 779
Remote Server
add ... 1111
delete ... 1112
edit ... 1111
view details ... 1111
Remote Soft Phone Emergency Calls ... 750
remove a user from groups ... 240
remove assigned elements ... 927
remove association between IP Office endpoint profile and user ... 264
remove endpoint dependencies
field description ... 839
remove endpoint reference field description ... 839
remove replica node from queue ... 1090
remove roles ... 239
remove user account ... 221
removing
Appliance Virtualization Platform host ... 1364
Avaya Solutions Platform 130 host ... 1364
encryption passphrase ... 1485
ESXi host ... 1364
outbound firewall rules ... 1196
remote key server ... 1487
removing a node ... 1090
removing additional identity certificates ... 1213
removing an appender from a logger ... 1032
removing an association between a subscriber and a user ... 258
removing assigned resources from group ... 157
removing association between an endpoint and a user ... 255
Removing Communication profile for a user ... 844
removing deleted users from database ... 221
removing dependencies of endpoints ... 838
removing local WebLM server ... 1067

removing location from host 1421
removing outbound firewall rules 1196
removing references to endpoints 838
Removing Stations and agents from CM users on System Manager 843
Removing the CM configuration from tenants 846
removing trusted certificates 1209
removing users from role 182, 244
removing vCenter 1421
renewCertificates 1218
renewing identity certificates 1215
repairing a replica node 1089
replace
primary System Manager server 121
secondary System Manager server 123
replace identity certificates
field descriptions 1216
replace primary System Manager server using secondary System Manager 123
replace System Manager servers 121
replacing identity certificates 1214
replica group
remove nodes 1090
Replica Groups page 1091
replica groups; view 1088
replication
database 95
file 95
LDAP 95
report 1105
Report alarm properties 877
reports 1098, 1106
delete 1110
download 1107
email 1110
generate 1106
generating 1101
new 1106
rerun 1106
Reports Generation field descriptions 1098
Reports output directory 877
resetting the password 921
resolving anonymous profiles 995
Resource Synchronization page 165
resources
assign to group 165
filter 156
group 154
manage 165
remove 157
search 154
search group 155
Resources page 168
resources; filter 167
resources; search 167
resources; synchronize 153
restart
restart *(continued)*
application 1405
restart application from SDM 1405
restarting
Appliance Virtualization Platform 1391
ESXi host 1391
restore 848
primary System Manager 109
primary System Manager server 122–124
Restore
field descriptions 866
restore backup
remote server 858
restore backup from remote server 858
Restore Confirmation Page 366
restore data backup 857
restore on System Manager Geographic Redundancy 850
restore system backup from local server 857
restoring
default password policy settings 61
restoring all announcements 680
restoring announcements 680
restoring announcements; all 680
restoring audio groups 689
restoring audio groups; field description 690
Restoring the default password policy settings 61
restoring, deleted user 243
Restrict Last Appearance 760
retrieve harvested log file 1016
retrieving
local WebLM certificate 1064
retrieving the System Manager CA certificate 1232
retrying
Utility Services to AVP Utilities upgrade 1454
revocation in SubCA 1250
revocation information 1250
revocation list
overview 1260
revoke certificate field descriptions 1222
revoking certificates 1221
Rng 710
role
add 185
assign users 181
copy permission mapping 182
delete 184
details 185
edit 183
new 185
unassign users 182, 244
role based access control 171
Role Details 185
Role page 184
roles
built-in 171
RBAC 176
remove 239

roles *(continued)*
Service Provider Administrator 171
System Administrator 171
Tenant Administrator 171
Roles 171
rolling back
Utility Services 1454
Room
Station 761
root CA 1255
root CA created using SHA256withRSA signing algorithm and 2048 key size 1239
route pattern
calculate 837
route selection 837
rules 618
Running a full synchronization on SMGR 847
runRTSCli.sh 925

S

SAC/CF Override 763
Salient features of SAML implementation in System Manager 1279
SAML 1278
SAML authentication 1277
SAML implementation 1278, 1279
SAML protocol 1277
SAML Service Provider 1284
SAML Service Provider metadata 1284
sample scenario
range feature 191
sample XML file for a user with SIP Communication Profile 597
sample XML with a single user profile 589
Save as template 721
saving an announcement 678
saving an endpoint template 721
saving announcements 678
saving CM translations 992
saving Communication Manager trnaslations 992
schedule
on-demand job 1114
schedule a user import job 392
Schedule Backup page 865
schedule CRL download
field descriptions 1265
schedule CRL download field descriptions 1265
schedule data backup; remote server 855
Schedule Discovery 909
scheduled backup job
deleting 856
scheduled job
edit 1129
scheduled jobs
completed 1125
scheduler 1114
Scheduler
permissions 1118
scheduler service 1114
scheduler; access 1118
scheduling
CRL download 1265
scheduling a data backup on a local server 854
scheduling a data backup on a remote server 855
scheduling a global user settings import job 400
scheduling a user synchronization job 85
SCP Configuration (S) 1342
SDM
installation 1319
SDM Client 1316
SDM elements
re-establishing trust 1400
search
Communication Manager objects 655
Search Archives page 1028
search resource 168
search users 237
searching
96x1 SIP set type for J1xx endpoint migration by using advanced search 734
search component 237
users 237
searching Communication Manager objects 655
searching contacts on Avaya SIP AST endpoints 1301
searching for a text in a log file 1020
searching for alarms 1006
searching for content 1528
searching for logs 1036
searching for resources 154, 155, 167
searching logs 1036
secondary alarms
forward to primary System Manager 1010
secondary server 108
CRL addition 102
secondary server alarms
view 1010
secondary System Manager failure 123
Security Code 745
security configuration
field descriptions 1269
security configuration field descriptions 1269
security hardening 1186
commercial grade 1183
military grade 1184
System Manager 1182
security settings 64
field descriptions 65
select all attribute; edit 655
Select Flexi Footprint 1402
Select Last Used Appearance 758
select upgrade target release 1437
Select Users 367
selected groups; adding resources 166

Selected Roles 363, 367
self provisioning
disable 211
enable 210
end user 210, 212
Sending reports through email 1110
Server Host ID 1062
Server Properties 1062
server properties; view 1052
service
Health Monitor 114
Service Hours Table
downloading excel template 702
exporting all service hours table 700
exporting selected service hours table 701
importing service hours table 701
Service Hours Table List 700
Service Link Mode
Attendant Console 751
service observe
coach 782
listen-only 782
Service Profile Management 872
Service Provider Initiated SSO 1286
serviceability agent
activate 975
assign filter profile 972
unassign filter profile 972
serviceability agents 961, 982
activate 974
Serviceability agents
Manage Profile Job Status 977
repair 975
Services Port static route update 1404
Session Manager
configure during GR failover 129
primary, secondary, third, fourth 746
Session Manager communication profile administration ... 250
Session Manager Communication profile administration ...251
Session Manager configuration 128
Session Manager correlation 842
Session Manager update 1401, 1437, 1439
session properties field descriptions 63
session properties; edit 63
Session termination policy 63
Set Color 762
set enrollment password 1202
set type 780
H323 783
set type of endpoints 780
set up alternate source 1328
setting 763
setting the default CA 1253
setting the new CA as default CA 1253
Settings icon 35
SFTP Configuration (T) 1342
SHA2 signing algorithm and 2048 key size 1240
SHA256withRSA signing algorithm and 2048 key size ... 1240
shared address 609, 612
assigning 245, 609
shared addresses 208
sharing content 1528
shut down from web console 1311
shut down System Manager 1311
shutdown 1310
shutting down
AVP 1391
signing the certificate 1247
simultaneous logins 1001
Single administration
Dual Registration 783
Single Sign On to remote machine fails 1503
Single Sign-On 1277–1279
single sign-on cookie domain 67
SIP endpoint
feature button 780
SIP endpoints 784
site
create 1294
editing 1299
viewing 1298
Site Data 761
building 761
cable 761
floor 761
jack 761
room 761
SMGR_DEFAULT_LOCAL 1333
Snapshot Manager
virtual machine snapshot 1390
Snapshot Manager field descriptions 1390
SNMP
attaching 982
attaching and detaching filters 984
CLI 980–985
creating notification 983
creating target profiles 981
creating user profiles 980
listing agents 983
listing filter profiles 984, 985
listing target profiles 982, 983
listing user profiles 981
SNMP 979
SNMP access profile
edit 912
SNMP Access profile
add 912
delete 912
SNMP Access Profile 914
SNMP Access Profiles 913
SNMP alarms
CS 1000 134
SNMP attributes 944
SNMP discovery

SNMP discovery *(continued)*
device list ... 908
SNMP target profile
add ... 967
edit ... 968
SNMP target profile list ... 967
SNMP target profile; view ... 968
SNMP target profiles field descriptions ... 969
SNMP target profiles; delete ... 969
SNMP traps ... 1045
SNMP V1 ... 914
SNMP V1 protocol ... 913
SNMP V3 ... 914
SNMP V3 protocol ... 913
SNMPv3 user profile; add ... 964
SNMPv3 user profile; create ... 964
SNMPv3 user profile; delete ... 965
SNMPv3 user profile; edit ... 964
SNMPv3 user profile; filter ... 965
SNMPv3 user profile; view ... 964
SNMPv3 user profiles
assign ... 976
manage ... 976
SNMPv3 user profiles field description ... 965
software
download ... 1344, 1349
software library
delete ... 1342, 1346
protocol support ... 1334
software library management ... 1345
sync files ... 1347
upload files ... 1347
viewing a file ... 1345
Software library ... 1332
software library files ... 1347
software library files field descriptions ... 1347
software library; add ... 1341
software library; create ... 1341
software library; edit ... 1341
software library; view ... 1341
software library; viewing files ... 1344
Software Management ... 1433
Solution Deployment Manager 1315, 1349, 1379, 1399, 1433
permissions ... 180
restart application ... 1405
start application ... 1405
stop application ... 1405
supported applications ... 1324
Solution Deployment Manager client ... 1315
Solution Deployment Manager Client ... 1316
prerequisites ... 1318
Solution Deployment Manager client dashboard ... 1322
Solution Deployment Manager elements
re-establishing trust ... 1400
Solutions Platform S8300
regenerate certificate ... 1395
sort documents ... 1528
Speaker ... 762
Speakerphone ... 752
specifying range for endpoints ... 198
specifying range for hunt group ... 202
SSH from AVP Utilities ... 1380
SSO configuration
Avaya Equinox Management ... 144
SSO cookie domain value ... 1503
reimport ... 67
SSO login ... 1503
SSO setup between System Manager and Active Directory Federation Server ... 1282
stand-alone ... 114
start
application ... 1405
start application from SDM ... 1405
static routing
changing ... 1404
updating ... 1404
station ... 241, 242
status
Analyze ... 1474
analyze job ... 1472
element records import ... 954
Preupgrade check ... 1474
preupgrade check job ... 1472
Refresh elements job ... 1472
upgrade job ... 1472
upgrade jobs ... 1474
stop
application ... 1405
stop application from SDM ... 1405
Stop Confirmation page ... 1132
stop crl ... 1256
stop crl creation ... 1256
stopping pending jobs ... 1123
stopping user synchronization jobs ... 88
subca ... 1256
submitting a request for harvesting log files ... 1020
Subnet Configurations field descriptions ... 917
subnets ... 917
subnets list ... 917
subnetwork
add ... 916
delete ... 916
edit ... 916
subordinate CA ... 1250, 1255
subscriber
adding templates ... 1142
subscriber class of service ... 645
subscriber COS ... 645
subscriber list ... 648
Subscriber Manager
datasource attributes ... 639
datasource parameters ... 639
Subscriber Manager data
import ... 637

Subscriber Manager user data
importing 642
subscriber template list 1145
subscriber template versions 1135
subscriber templates
delete 1144
duplicate 1144
edit 1143
view 1144
subscriber; view
viewing subscribers 647
subscribers
delete 647
deleting 647
removing 647
subscribers; add
adding subscribers 646
subscribers; new 646
subscribers; edit
editing a subscriber 646
editing subscribers 646
support 1530
support of common parameters across endpoint template 772
supported browsers 34
Survivable COR 752
Survivable GK Node Name 753
Survivable Trunk Dest 758
svars
file size 849
swap endpoints field descriptions 777
symmetric keys
regenerating 1288
sync 840
Sync files 1347
synchronization 72, 1087
DRS clients 1087
incremental 985
initialization 985
limitations 74
synchronization datasource
add 75
deleting 77
edit 77
view 76
synchronization from LDAP directory server 73, 74
synchronization job history 87
synchronization job history field description 87
synchronization job summary
view 89
synchronization notification 1490
synchronization to LDAP directory server 73
synchronize
CM data 988
configuring options 988
CS 1000 profile 997
synchronize Application Server system configuration 990
synchronize CM data 988
synchronize communication profiles field description 997
synchronizing
Communication Manager data 985
IP Office 985
Messaging data 985
synchronizing communication profiles 995
synchronizing CS 1000 profiles 995
synchronizing messaging data 992
synchronizing resources 153
synchronizing System Manager master database and replica computer database 1089
Synchronizing the VMPro system configuration 991
syslog receiver configuration
field descriptions 1425
syslog server
adding 1424
configuration 1424
system
scheduled job 1114
System ID 746
System Manager 1255
7.0 1473
commands 1510
disabling FTP 1333
enabling FTP 1333
local software library 1333
upgrade 1473
System Manager Application Management
Installed Patches field descriptions 1414
system manager backup; alarm 1007
System Manager CA as subordinate CA 1247
System Manager CA certificate; retrieve 1232
System Manager capabilities
certificate generation 1199
certificate management 1199
System Manager certificate authority 1247
System Manager dashboard 35, 39
System Manager localization 1524
System Manager login 39
System Manager logon messages 41
System Manager messages 40
System Manager restore 109
System Manager server for upgrade 1332
System Manager shutdown 1310
System Manager training 1529
System Manager trust store; Communication Manager certificate 1496
System Manager upgrade 1464
System Manager VM update 1414
System Manager web console 35
System Manager; Communication Manager capabilities ...653
System Manager; firewall 1532
System Manager; firewall implementation 1532
System Platform
add 930
system recovery process 124
system requirements for the external server 1347

system template
manage audio field description 1170

T

target profile; manage 975
target profiles 961
attaching 982
detaching 982
edit 968
target profiles field descriptions 969
target profiles; delete 969
target profiles; filter 967
target release 1436
select 1437
team
create 1294
editing 1299
viewing 1298
template
map permissions 181
Template for permission set 181, 187
template list 1145
template versioning 1135
template versions 1135
templates 1135
new subsriber 1142
upgrade 1136
templates for mapping permission 181
tenant
create 1294
delete 1299
editing 1299
viewing 1298
tenant administrator
assign 1297
unassign 1298
tenant administrator role
add 178
tenant management 1297, 1298
Tenant Management 1292
console 49
field descriptions 1305
Tenant Management page 1305
tenant organization
create 1294
tenant partitioning
Avaya SIP AST endpoints 1301
Communication Manager 1301
Terminate to Coverage Pts. with Bridged Appearances 710
Terminating
administrative user sessions 70
terminating single sign-on sessions 1288
test alarm from CLI
generate 1009
test alarms from web console
generate 1009
third-party AVP certificates
creating generic CSR 1234, 1388
editing generic CSR 1234, 1388
third-party certificates
applying to Appliance Virtualization Platform .. 1232, 1386
third-party identity certificate 1247
threshold value
disk space 850
throttling period 1006
Through 784
Time of Day Coverage Table 712, 713
Time of Day Lock Table 753
time zone
configure 1523
timeout interval
configure 115
TrapListener 1045
TrapListener service 1045
Traplistener service; alarming UI 897
TrapListener service; configure 897
Triple Ringer Type
Call Pickup button 781
configuration 781
trunk group
adding 790
delete 791
editing 790
field-level RBAC 206
viewing 791
Trunk Group List
field descriptions 789
Trust Management 1198
trusted certificate 1204
trusted certificate; add 1493
trusted certificates
add 1205
view 1208
trusted certificates; remove 1209
truststore 1255
Turn On Mute 779
Turn On Mute for Remote Off-hook Attempt 779
two-way TLS 1497
Two-way TLS 1496
two-way TLS in System Manager 1497
two-way TLS; configure notify sync 1494

U

UDP 833
field description 832
UDP entries
add 833
edit 833
update 834
view 833
UDP field descriptions 832
UDP Group

UDP Group *(continued)*
deleting ... 830
udp groups ... 828
UDP groups
access ... 835
assign permission ... 835
udp groups field description ... 830
unassign
tenant administrator ... 1298
UnAssign Roles page ... 367
unassign users
roles ... 182, 244
unassigning filter profile from serviceability agent ... 972
unconfigure
Geographic Redundancy ... 114
understanding
groups ... 774
uniform dial plan ... 833
Uniform dial plan
UDP ... 1001
Uniform Dial Plan field descriptions ... 832
Uniform Dial Plan Group
deleting ... 830
uniform dial plan group; add ... 828
Uniform Dial Plan Group; edit ... 829
Uniform Dial Plan Group; view ... 829
uniform dial plan groups ... 828
Uninstall License page ... 1061
uninstalling a license file ... 1052
Unknown location host mapping ... 1368
unmanage elements ... 930
unrevoking certificates ... 1221
update
Appliance Virtualization Platform ... 1391
Branch Session Manager ... 1439
Communication Manager ... 1401, 1437, 1439
Session Manager ... 1401, 1437, 1439
Utility Services ... 1439
WebLM ... 1439
Update Entity Class
field descriptions ... 1225
update software ... 1401, 1437, 1439
update static routing ... 1413
Update Static Routing ... 1427
update System Manager VM ... 1414
Update UDP entries ... 834
field description ... 834
updating ESXi host or vCenter certificate ... 1394
updating Services Port static routing ... 1404
Updating UDP entries ... 834
Updating UDP entries field description ... 834
upgrade
Branch Session Manager ... 1434, 1435, 1445
checklist ... 1435
Communication Manager ... 1434, 1435, 1445
elements ... 1441
Session Manager ... 1434, 1435, 1445
upgrade *(continued)*
target release ... 1436, 1437
Upgrade Configuration
field descriptions ... 1444
Upgrade Configuration Details ... 1445
upgrade job status ... 1472
Upgrade job status
Viewing ... 1473
upgrade jobs
deleting ... 1473
editing ... 1473
status ... 1474
Upgrade Management ... 1433, 1464
User Settings ... 1331
upgrade media gateways ... 1474
upgrade media modules ... 1474
Upgrade Release Selection ... 1436, 1437
Upgrade System Manager ... 1462
Upgrade to release ... 1437
upgrades
supported protocols ... 1480
upgrading
Branch Session Manager instances in bulk ... 1460
upgrading CM Agent template ... 1136
upgrading CM Endpoint template ... 1136
upgrading devices
protocol matrix ... 1480
upgrading IP Office endpoint templates ... 1164
upload
custom patch ... 1452
upload file to software library ... 1347
uploading a custom patch ... 1452
uploading an audio file in IP Office system configuration template ... 1168
uploading custom patch ... 1453
uploading custom patch field description ... 1453
uploading version.xml ... 1481
UPM ... 247
Usage by local WebLM page ... 1078
usage options ... 836
Usage Summary page ... 1077
user
assign groups ... 364
user account
create ... 213
remove ... 221
user addressing
add ... 244
User Attribute Options ... 384
User Bulk Editor ... 224
User Bulk Editor field descriptions ... 224
User Bulk Import Profile ... 900
user certificate authentication
provisioning ... 1275
User Delete Confirmation page ... 362
user details; view ... 213
user import job

user import job *(continued)*
cancel ... 395
delete ... 395
schedule ... 392
User Management
assigning permissions ... 191
roles ... 191
User Management field descriptions ... 282
User management for Application Enablement Services .. 148
User management for IP Office ... 148
User Preference ... 35
user profile
create ... 213, 214
user profile management ... 208
user profiles ... 961
user provisioning rule ... 215, 618
add service to user ... 620
create user ... 214
creating ... 621
deleting ... 623
modifying ... 621
viewing ... 622
User Provisioning Rule ... 285
User Provisioning Rules ... 224
field descriptions ... 623
User Restore Confirmation Page ... 366
user roles
view ... 177
user search
searchable fields ... 237
User settings
configure ... 1327
User Settings
field description ... 1331
user settings for upgrades ... 1326
user synchronization datasource
field descriptions ... 78
user synchronization job
create ... 84
schedule ... 85
user synchronization job history
delete ... 88
user synchronization jobs
delete ... 86
stop ... 88
user synchronization jobs field description ... 86
user-defined templates ... 1135
users
assign ... 186
assign groups ... 239, 240
bulk edit ... 222, 224
bulk export ... 381
filtering ... 236
manage ... 208
search ... 237
using clear amw all ... 728
using filters
using filters *(continued)*
filtering endpoints ... 724
using native name ... 719
using swap endpoints
endpoints; swap endpoints ... 729
Utility Services
adding ... 932
rolling back ... 1454

V

validating connectivity to local WebLM servers for a product ... 1068
Validation
certificate ... 1392
vCenter
add ... 1422
add location ... 1421
adding ... 1419
deleting ... 1421
edit ... 1422
editing ... 1421
field descriptions ... 1421
manage ... 1421
remove location ... 1421
removing ... 1421
unmanage ... 1421
vCenter certificate update ... 1394
VDN
adding dependencies ... 838
vector directory number list ... 693
vector directory number,
vdn ... 693
vector routing table
call center; vector routing table ... 697
vector routing table field description ... 699
vector routing table list ... 697
vector routing table; add ... 697
vector routing table; edit ... 698
vector routing table; field description ... 699
vector routing table; view ... 698
verifying changes to date and time configuration ... 1522
videos ... 1529
view ... 1213
global user settings import job details ... 401
grace period ... 888
import global user settings job ... 402
location ... 1354
remote syslog profiles ... 1044
secondary server alarms ... 1010
subscriber templates ... 1144
user import job details ... 396
view an import global user settings job ... 402
view an import global user settings job on the Scheduler page ... 402
view backup files ... 851
View by local WebLM page ... 1071

view certificate detail field descriptions 1220
view completed jobs 1119
view contact list member page 269
view contents; log harvested files 1021
view details of a global user settings importing job 401
view details of element 924
view details of import job 401
view details; log harvesting request 1020
View Element page 944
view endpoint
    field descriptions 743
view endpoint template
    field descriptions 743
view filter profiles 973
View Group page 160
view last contacted status of the local WebLM servers ... 1067
view license capacity 1051
View Local WebLMs page 1074
view location 1354
view log details 1035
view loggers 1030
view logs
    completed jobs 1120
    pending jobs 1120
view periodic status of master and local WebLM servers 1069
View Private Contact List page 280
View Profile Inventory page 878
View profile Messaging field descriptions 879
View Profile SMGR Element Manager
    field descriptions 894
View Profile SMGR Element Manager field descriptions ... 894
View Profile System Manager page 883
View Profile: Trust Management field description 899
View Profile: User Bulk Import Profile page 900, 901
View Profile:Alarming UI page 886
View Profile:Communication System Management
        Configuration page 875
View Profile:Configuration page 878
View Profile:GracefulShutdown 888
View Profile:HealthMonitor UI page 889
View Profile:Logging page 891
View Profile:Logging Service page 892
View Public Contact List page 602
view replica groups 1088
View Scheduler Profile page 896
view secondary server alarms 1010
view shutdown history 1313
view shutdown history from web console 1313
View SNMP Profile page 896
view the details of a public contact 600
view the details of a user import job 396
View Trust Certificate page 1209
view trusted certificates 1208
view UDP Groups 829
view user import job on the Scheduler page 396
View User Provisioning Rule
    field descriptions 624
View WebLM page 890
viewing
    alarms 1004
    certificate add status 941
    certificates 1220
    clusters 808
    CRL download job 1267
    data encryption status 1489
    department 1298
    endpoint migration job detail 738
    endpoint migration job history 738
    groups 151
    list of outbound firewall rules 1195
    notification status 940
    outbound firewall rule status 1195
    password policy status 60
    resources for a group 151
    roles 177
    site 1298
    subject name validation status for an entity class 1231
    subject names for an entity class 1230
    syslog servers 1426
    team 1298
    tenant 1298
    trunk group 791
    user provisioning rule 622
    user roles 177
    virtual machine report status 1417
Viewing
    administrative user details 68
viewing a messaging profile of a user 257
Viewing a VMPro call flow template 1178
Viewing a VMPro System Configuration template 1174
viewing active sessions 1288
viewing agent data
    agents; view data 664
viewing allocations by features 1070
viewing allocations by local WebLM 1070
viewing an announcement 678
Viewing an Application Server Configuration template 1171
viewing an audio group 688
viewing an IP Office endpoint template 1162
Viewing an Off PBX Endpoint Mapping 795
viewing an SNMP target profile 968
viewing an SNMPv3 user profile 964
viewing announcements 678
viewing associated subscribers
    viewing subscribers 1145
viewing audio groups 688
viewing authorization code
    authorization code; view 823
Viewing Automatic Alternate Routing Digit Conversion
        data
    Automatic Alternate Routing Digit Conversion;
        viewing data 801
Viewing Automatic Route Selection Digit Conversion

Viewing Automatic Route Selection Digit Conversion *(continued)*
Automatic Route Selection Digit Conversion; viewing data ... 804
viewing automatic route selection toll data ... 807
viewing AVP host
firewall rules ... 1386
Viewing AVP host
license status ... 1385
viewing bulk user edit jobs ... 222
viewing certificates ... 1220
viewing class of service data ... 819
viewing class of service group
class of service group; view ... 825
viewing CM Agent template ... 1138
viewing CM Endpoint templates ... 1140
Viewing contents of the certificate ... 1238
viewing coverage path
coverage path; view ... 703
viewing coverage time-of-day
coverage time-of-day; view data ... 711
viewing data modules
data modules; view ... 810
viewing deleted users ... 242
viewing details of a log harvesting profile ... 1019
viewing details of a log harvesting request ... 1020
viewing details of a user ... 213
viewing enterprise usage of a license feature ... 1068
viewing files in the software library ... 1344
viewing groups ... 151
viewing harvested log files in an archive ... 1019
viewing hunt group
hunt group ... 786
viewing identity certificates ... 1213
viewing IP Office endpoint profiles ... 262
viewing IP Office system configuration templates ... 1166
viewing job history ... 1427
viewing job summary ... 89
Viewing job summary field descriptions ... 89
viewing license capacity ... 1051
viewing license capacity of a feature ... 1067
viewing list of backup files ... 851
viewing log details ... 1035
viewing loggers for a log file ... 1030
viewing notification filter profile ... 971
Viewing Off PBX Configuration Set ... 792
viewing peak usage ... 1051
viewing pending jobs ... 1119
Viewing Remote Servers ... 1111
viewing replica groups ... 1088
viewing replica node details ... 1090
viewing replica nodes in a replica group ... 1088
viewing replication details for a replica node ... 1090
viewing reports ... 1107
viewing resources for a group ... 151
viewing server properties ... 1052
viewing software library ... 1341
viewing subscriber templates ... 1144
viewing subscriber templates CMM; field description
CMM field description ... 1156
viewing subscriber templates Messaging
field descriptions ... 1153
viewing subscriber templates MM; field description
MM field description ... 1158
viewing synchronization datasources ... 76
viewing templates
subscriber ... 1144
viewing the contents of harvested log files ... 1021
viewing the details of a contact in the contact list ... 266
viewing the details of a private contact ... 272
viewing the list of outbound firewall rules ... 1195
viewing the outbound firewall rule status ... 1195
viewing the password policy status ... 60
viewing the station profile of a user ... 254
viewing the status of security hardening ... 1188
Viewing UDP entries ... 833
viewing Uniform Dial Plan Group ... 829
viewing usage by WebLM ... 1068
viewing usage summary ... 1071
viewing user provisioning rule ... 622
viewing user roles ... 177
viewing vector directory number
vector directory number; view ... 694
viewing vector routing table data ... 698
Viewing Xmobile Configuration data
Xmobile Configuration; view data ... 797
virtual machine
create ... 1396
snapshot on Appliance Virtualization Platform ... 1389
virtual machine operations
job history ... 1427
virtual machine report
aborting ... 1417
overview ... 1416
virtual machine snapshot using SDM
deleting ... 1390
Visualization, Performance, and Fault Manager ... 148
VM connection reestablish ... 1415
VM console
opening ... 1406
VM Console
overview ... 1406
VM Console field descriptions ... 1407
VMPro Call Flow Templates field descriptions ... 1180
VMPro system configuration Templates
field descriptions ... 1177
voice mail number ... 761
Voice Terminal ... 747
VPFM ... 148
VxWorks-based CS 1000 server
configuration ... 135

W

warning
data entry in Excel 374
watchlist 1528
WebLM access 1048
WebLM overview 1047
WebLM server
deleting 1067
removing 1067
WebLM Server on AVP host 1384
WebLM servers
periodic status 1069
What is an audio group 688

X

XML 241, 242
import user 377
XML file
import users 581
XML for user with core attributes 588
Xmobile Configuration field description
Xmobile Configuration; field description 798
xmobile configuration list 796
xmobile configuration,
endpoints; xmobile configuration 796