Administering Avaya Aura® Session Manager

Release 6.3
Issue 7
September 2014

© 2014 Avaya Inc.
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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

Concurrent User License

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Copyright

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

Third Party Components

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

Virtualization

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United

States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya® and Avaya Aura® are registered trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction 19
Purpose 19
Intended audience 19
Document changes since last issue 19
Related resources 20
Documentation 20
Training 21
Viewing Avaya Mentor videos 22
Support 22
Warranty 23
Chapter 2: Getting started 24
Overview of System Manager 24
Log on to System Manager 26
Turning off the compatibility mode 26
Logging on to System Manager web console 27
Logon information for users with user name *admin* 27
Password and security policies for all administrators 28
Password aging policy enforcement 28
Password strength policy enforcement 28
Password history policy enforcement 29
Password lockout policy enforcement 29
Inactive session termination policy 29
Logon warning banner 29
Editing password policies 29
Editing Session Properties 30
Security settings 30
Editing the logon warning banner 30
Password policies field descriptions 31
Session Properties field descriptions 32
Chapter 3: Managing Session Manager using geographic redundant System Manager instances 34
Terminology 35
Geographic Redundancy scenarios 35
Managing Session Manager in a Geographic Redundancy solution 39
Managing data center failures 46
Case 1: The primary System Manager or the primary data center fails 47
Case 2: Primary System Manager fails and needs a hardware replacement 49
Case 3: Replacing the secondary System Manager due to hardware failures 50
Case 4: Shutting down the primary System Manager for maintenance 50

Case 5: The primary System Manager cannot communicate with the secondary System Manager. The system elements can communicate with the primary System Manager and the secondary System Manager..... 50
Case 6: The primary System Manager cannot communicate with the system elements, but the elements can communicate with the secondary System Manager..... 51
Case 7: System elements can communicate only with the primary System Manager..... 52
Case 8: The primary System Manager cannot communicate with the secondary System Manager. Some system elements can communicate only with the primary System Manager while some system elements can communicate only with the secondary System Manager..... 52
Setting up a Geographic Redundancy enabled system..... 54
Upgrading to a Geographic Redundancy-enabled system..... 55
Simultaneous element upgrade method..... 55
Selected element upgrade method..... 56
Performing system verification tests..... 56
Chapter 4: Synchronizing Communication Manager data with the System Manager database..... 58
Creating a Communication Manager instance in the system..... 58
Creating a new element..... 58
Add Communication Manager field descriptions..... 59
Creating a Messaging instance..... 62
Synchronizing the Communication Manager data and configuring options..... 63
Synchronizing the messaging data..... 64
Manage Elements field descriptions..... 64
Element details field descriptions..... 66
Chapter 5: Managing security..... 74
Certificate management..... 74
Using the System Manager CA..... 75
Exporting the System Manager CA..... 75
Adding System Manager CA to Communication Manager..... 76
Adding System Manager's Root Certificate to 96xx Phones..... 77
Installing Enhanced Validation Certificates for Session Manager..... 77
Using a third party CA..... 78
Adding a third party CA to Communication Manager..... 79
Adding a third party Root Certificate to 96xx Phones..... 80
Installing third party certificates on Session Manager..... 80
Adding trusted certificates..... 81
Demo certificates..... 83
Viewing the TLS version..... 83
Installing demo certificates..... 83
Trusted Certificates..... 84
Viewing trusted certificates..... 84
Adding trusted certificates..... 85

Removing trusted certificates ... 87
Exporting a Session Manager Certificate ... 88
Trusted Certificates field descriptions ... 88
Identity Certificates ... 89
SIP Identity Certificate ... 89
HTTPS Identity Certificate ... 90
Identity Certificates field descriptions ... 91
Viewing Identity Certificates ... 92
Replacing a Session Manager Identity Certificate ... 92
Adding Root CA to the System Manager Trusted List ... 94
Adding Root CA to the Session Manager Trusted List ... 94
Administering a SIP Identity Certificate ... 95
Restoring the default SIP Identity Certificate ... 96
Activating a new Identity Certificate ... 96
Chapter 6: Managing users ... 97
Before administering a Session Manager profile ... 97
Adding users ... 99
Managing communication profiles ... 102
Session Manager communication profile administration ... 102
Multi Device Access ... 103
Communication profiles ... 103
Adding a communication profile for the user ... 104
Deleting the communication profile of a user ... 104
Creating a new communication address for a communication profile ... 105
Modifying the communication address ... 105
Deleting a communication address from a communication profile ... 106
Presence communication profile administration ... 106
CM Endpoint profile administration ... 107
Messaging profile administration ... 110
CS 1000 and CallPilot profile administration ... 113
IP Office profile administration ... 116
Viewing details of a user ... 119
Modifying user accounts ... 119
Removing user accounts ... 120
Removing the deleted users from the database ... 121
Viewing the deleted users ... 121
Restoring a deleted user ... 122
Creating duplicate users ... 122
Managing default contact list of the user ... 123
Adding a contact in the Default Contact list ... 123
Modifying membership details of a contact in a contact list ... 123
Viewing membership details of a contact in the contact list ... 124
Deleting contacts from the default contact list ... 124

Attach Contacts field descriptions 125
Edit Contact List Member field descriptions 126
View Contact List Member field descriptions 128
Filtering users 130
Searching for users 131
Multi Tenancy for Avaya SIP AST endpoints 131
Managing user provisioning rules 131
User Provisioning Rule 131
Capabilities and guidelines of User Provisioning Rules 132
Adding User Provisioning Rules 133
Creating the user provisioning rule 134
Modifying the user provisioning rule 134
Viewing the user provisioning rule 135
Creating a duplicate user provisioning rule 135
Deleting the user provisioning rule 135
User Provisioning Rules Management field descriptions 136
User Provisioning Rule field descriptions 136
Role Based Access Control 144
RBAC permissions for Routing Import/Export operations 145
RBAC permissions for Local Host Name Resolution imports 146
RBAC permissions for Bulk Communication Profile edits 146
Creating a Scheduler operation role 146
Creating an RBAC role with read-only permissions 147
Creating an RBAC role with read and write permissions 148
Assigning an RBAC role to a user 149
Configuring a user to have access permissions for System Manager web pages 150
Copying permission mapping for a role 151
Removing access permissions for Session Manager and Routing pages 152
Removing the assigned RBAC role from a user 152
Managing bulk import and export 153
Bulk import and export 153
Bulk import and export using the Excel file 153
XML Schema definitions and sample XMLs for bulk import 155
Examples of bulk import and export of user by using the Excel file 155
Hierarchy in communication profile worksheets 157
Microsoft Excel data link error 158
Data entry warning in Microsoft Excel 159
Key features of bulk import and bulk export 159
About bulk import of users 160
Configuration options for bulk import using Excel 162
Downloading the Excel template file 162
About bulk export of users 163
Exporting users in bulk from web console 164

exportUpmUser.sh command ... 165
Configuration options for bulk import of users ... 165
Bulk importing of partial user attributes for a user ... 166
Making exported user data compatible for partial user import ... 167
About Bulk Import Encryption utility ... 168
Encrypting passwords in user import file using BulkImportEncryptionUtil running on Windows ... 169
Encrypting passwords in user import file using BulkImportEncryptionUtil running on Linux ... 170
Import user considerations ... 171
Scheduling a user import job ... 171
Aborting a user import job on first error ... 173
Canceling a user import job ... 174
Deleting a user import job ... 174
Viewing a user import job on the Scheduler page ... 175
Viewing the details of a user import job ... 175
Bulk import of global user settings ... 176
Bulk export of global user settings ... 177
Bulk exporting of global user settings ... 178
exportUpmGlobalsettings.sh command ... 178
Scheduling a global user settings import job ... 179
Viewing details of a global user settings import job ... 180
Viewing a global user settings import job on the Scheduler page ... 181
Aborting a global user settings import job on first error ... 181
Deleting a global user settings import job ... 182
Canceling a global user settings import job ... 182
List of XML Schema definitions and sample XMLs for bulk import ... 183
Import Users field descriptions ... 183
Import Users – Job Details field descriptions ... 186
Export Users field descriptions ... 188
Job Details field descriptions ... 190
Import Global Settings field descriptions ... 190
Quick start to importing users ... 193
New User Profile field descriptions ... 198
User Profile Edit field descriptions ... 216
User Profile View field descriptions ... 232
User Delete Confirmation field descriptions ... 245
Chapter 7: Session Manager routing ... 246
Prerequisites for routing setup ... 246
Routing ... 246
Call routing using routing policy data ... 247
Handling SIP responses ... 247
Administering initial setup of the Session Manager ... 248
Routing import and export Overview ... 249

Saving configuration changes..... 254
Duplicating Routing entity data..... 254
Domains..... 254
About Domains..... 254
Creating domains..... 255
Modifying domains..... 255
Deleting Domains..... 255
Delete Confirmation field descriptions..... 256
Domain Management field descriptions..... 256
Domain Details field descriptions..... 257
Bulk import for Domains..... 257
Locations..... 258
About Locations..... 258
Dial Plan Transparency..... 259
Creating Locations..... 260
Modifying Locations..... 260
Deleting Locations..... 261
Delete Confirmation field descriptions..... 261
Location field descriptions..... 262
Location Details field descriptions..... 262
Bulk import for Locations..... 266
Call Admission Control..... 267
Adaptations..... 269
About Adaptations..... 269
Adaptation module administration..... 271
Creating Adaptations..... 275
Adaptation example..... 277
Modifying Adaptations..... 280
Deleting Adaptations..... 282
Delete Confirmation field descriptions..... 282
Installed vendor adapters..... 283
Adaptations field descriptions..... 288
Adaptation Details field descriptions..... 289
Bulk import for Adaptations..... 294
SIP Entities..... 295
About SIP Entities..... 295
Authentication of trusted SIP entities..... 296
IP and transport layer validation..... 296
TLS layer validation..... 296
SIP Responses to an OPTIONS Request..... 297
Deny new service for entity links..... 297
SIP Call Loop elimination..... 298
Creating SIP Entities..... 298

Modifying SIP entities ... 301
Deleting SIP Entities ... 303
Delete Confirmation field descriptions ... 303
Accept new service for all entity links ... 304
Accept New Service Confirmation field descriptions ... 304
Deny new service for all Entity Links ... 304
Deny New Service Confirmation field descriptions ... 304
SIP Entities field descriptions ... 305
SIP Entity Details — Session Manager type field descriptions ... 306
SIP Entity Details field descriptions for other SIP Entity types ... 310
Bulk import for SIP Entities ... 315
SIP Entity References ... 317
About SIP Entity References ... 317
Displaying SIP Entity References ... 318
Overview of References to SIP Entities field descriptions ... 318
Entity Links ... 319
Entity Links ... 319
Deny new service for entity links ... 319
Creating Entity Links ... 319
Modifying Entity Links ... 320
Deleting Entity Links ... 320
Delete Confirmation field descriptions ... 321
Accept new service for the selected Entity Links ... 321
Accept New Service Confirmation field descriptions ... 321
Deny new service for selected Entity Links ... 322
Deny New Service Confirmation field descriptions ... 322
Entity Links field descriptions ... 322
Bulk import for Entity Links ... 324
Time Ranges ... 324
About Time Ranges ... 324
Creating Time Ranges ... 325
Modifying Time Ranges ... 325
Deleting Time Ranges ... 326
Delete Confirmation field descriptions ... 326
Time Ranges field descriptions ... 326
Time Range List field descriptions ... 327
Bulk import for Time Ranges ... 328
Routing Policies ... 329
About Routing Policies ... 329
Creating Routing Policies ... 330
Modifying Routing Policies ... 331
Deleting Routing Policies ... 332
Delete Confirmation field descriptions ... 332

Routing Policies field descriptions..... 333
Routing Policy Details field descriptions..... 334
SIP Entity List field descriptions..... 336
Time Range List field descriptions..... 336
Pattern List field descriptions..... 337
Regular Expression List field descriptions..... 338
Bulk import for Routing Policies..... 338
Dial Patterns..... 339
About Dial Patterns..... 339
Emergency Numbers..... 341
Dial Plan Ranges..... 342
Multilocation Dial Plan..... 343
Creating Dial Patterns..... 343
Modifying Dial Patterns..... 344
Deleting Dial Patterns..... 345
Delete Confirmation field descriptions..... 345
Dial Patterns field descriptions..... 346
Dial Pattern Details field descriptions..... 347
Denied Originating Location List field descriptions..... 349
Bulk Import for Dial Patterns..... 349
Regular Expressions..... 350
About Regular Expressions..... 350
Creating Regular Expressions..... 352
Modifying Regular Expressions..... 353
Deleting Regular Expressions..... 354
Delete Confirmation field descriptions..... 354
Regular Expressions field descriptions..... 354
Regular Expression Details field descriptions..... 355
Routing Policy List field descriptions..... 356
Bulk import for Regular Expressions..... 357
Defaults..... 357
Modifying the default settings..... 357
Default Settings field descriptions..... 359
Chapter 8: Configuring and monitoring Session Manager instances..... 361
Session Manager Dashboard..... 361
Session Manager Dashboard field descriptions..... 361
Session Manager Administration..... 363
About Session Manager Administration..... 363
About E911 Services..... 363
NIC bonding..... 364
Adding a SIP entity as Session Manager Instance..... 364
Viewing Session Manager administration settings..... 370
Modifying the Session Manager administration settings..... 370

Deleting a Session Manager instance 377
Administering ELIN Server 377
Saving Global Session Manager Settings 378
Delete Confirmation page field descriptions 379
Session Manager Administration page field descriptions 379
Session Manager page field descriptions 382
Branch Session Manager Administration 387
Branch Session Manager 387
Survivable Branch Configuration 388
Administering Branch Session Manager 393
Adding a SIP entity as a Branch Session Manager instance 394
Viewing the Branch Session Manager administration settings 400
Modifying the Branch Session Manager administration settings 401
Deleting a Branch Session Manager instance 406
Delete Confirmation page field descriptions 407
Branch Session Manager page field descriptions 407
Communication Profile Editor 410
Communication Profile Editor 410
Viewing Communication Profiles 411
Customizing column display 411
Modifying Communication Profiles 412
Viewing background edit job status 412
Viewing Communication Profile edit failures 413
Stopping Communication Profile editing jobs 413
Communication Profile Editor field descriptions 414
Communication Profile Edit Confirmation page field descriptions 417
Network Configuration 417
Failover Groups 417
Local Host Name Resolution 428
Remote Access 436
SIP Firewall 441
Device and Location Configuration 459
Device Settings Groups 459
Location Settings 473
Application Configuration 474
Applications 474
Application Sequences 480
Conference Factory URI 484
Implicit Users 495
Session Manager Network Connect Service 498
System Status 502
Session Manager SIP Entity Monitoring 502
Managed Bandwidth 506

Security Module Status 508
SIP Firewall Status 513
Registration Summary 515
User Registrations 519
Session Counts 530
User Data Storage status and Call History management 532
System Tools 540
Session Manager maintenance tests 540
SIP Tracer Configuration 543
SIP Trace Viewer 547
Call Routing Test 549
SNMP MIB 550
Performance 552
Call Counts 552
Location Performance 554
SIP Performance 557
System Performance 562
Performance Data Collection 566
Chapter 9: System Tools 572
Session Manager maintenance tests 572
Maintenance Tests page field descriptions 572
Running maintenance tests 573
Maintenance Test descriptions 573
SIP Tracer Configuration 575
About Tracer Configuration 575
Tracer Configuration page field descriptions 575
SIP Trace Viewer 578
About SIP Tracing 578
Trace Viewer page field descriptions 579
Call Routing Test 581
About Call Routing Testing 581
Call Routing Test page field descriptions 581
SNMP MIB 582
SNMP MIB Download 582
Downloading SNMP MIBs 583
SNMP MIB Download page field descriptions 584
Chapter 10: System Status 585
Session Manager SIP Entity Monitoring 585
Viewing the SIP Monitoring Status Summary page 586
SIP Entity Link Monitoring Status Summary page field descriptions 586
Managed Bandwidth 589
Viewing Managed Bandwidth Usage 589
Managed Bandwidth Usage page field descriptions 589

Security Module Status 591
About Security Module Status 591
Security Module Status actions 591
Investigating Security Module status 591
Security Module Status page field descriptions 592
Confirm Security Module Reset page field descriptions 594
About Connection Status 594
SIP Firewall Status 596
Viewing SIP Firewall status 596
Auditing Firewall configuration 597
SIP Firewall Status page field descriptions 597
Registration Summary 599
Registration Summary 599
Viewing Registration Summary 599
Rebooting of selected AST devices 599
Reloading of selected AST devices 600
Failback of selected AST devices 600
Advanced Searching 601
Registration Summary field descriptions 601
User Registrations 602
User Registrations 602
Viewing User Registrations 603
Customizing column display 604
Forcing unregistration of device registration 604
Rebooting of selected AST devices 605
Reloading of selected AST devices 605
Failback of selected AST devices 606
Advanced Searching 606
User Registrations field descriptions 607
Session Counts 614
SIP sessions count 614
Viewing Session Count data 615
Exporting analyzed Session Count data 615
Session Counts field descriptions 616
User Data Storage status and Call History management 617
Viewing the User Data Storage Status screen 617
Data Server Status field descriptions 617
User Data Storage backup 618
Call History 622
Chapter 11: Managing system events 625
Managing alarms 625
Alarming 625
Viewing alarms 626

Changing the alarm status 626
Exporting alarms 626
Filtering alarms 627
Searching for alarms 627
Managing Geographic Redundancy related alarms 628
Alarming field descriptions 629
Alarming field descriptions 630
Managing log viewer 633
Log Viewer 633
Viewing log details 633
Exporting logs 634
Filtering logs 634
Searching for logs 635
Logging field descriptions 635
Logging field descriptions 639
Managing log settings 640
Log Settings 640
Accessing the Log Settings service 640
Viewing loggers for a log file 641
Logging Settings field descriptions 641
Editing a logger in a log file 642
Managing log harvester 646
Log Harvester 646
Accessing the Log Harvester service 646
Creating a new log harvesting profile 647
Editing a log harvesting profile 648
Viewing the harvested log files in an archive 648
Deleting a profile 649
Submitting a request for harvesting log files 649
Viewing details of a log harvesting request 650
Searching for text in a log file 650
Viewing the contents of harvested log files 651
Downloading the harvested log files 651
Filtering log harvesting profiles 652
Filtering log harvesting requests 653
Viewing details of a log harvesting profile 653
Log Harvester field descriptions 654
Create New Profile field descriptions 655
Harvest Criteria Edit field descriptions 656
Profile Criteria View field descriptions 656
Harvest Archives field descriptions 657
Search Archives field descriptions 659
Harvest - View Harvest detail field descriptions 659

Chapter 12: Managing system data 662
Managing backup and restore 662
Backup and restore 662
Disk space management for System Manager backup 663
Disk space required for backup 663
Time duration for backup and restore 664
Backup and restore on System Manager that is configured for Geographic Redundancy 664
System Manager data backup options 665
Accessing the Backup and Restore service 665
Viewing list of backup files 665
Creating a data backup on a local server 666
Creating a data backup on a remote server 666
Scheduling a data backup on a local server 667
Scheduling a data backup on a remote server 667
Editing a scheduled backup job 668
Deleting the scheduled backup job 669
Restoring data backup from a local server 669
Restoring a backup from a remote server 670
Restoring the backup through the command line interface 672
Backup and Restore field descriptions 672
Backup field descriptions 673
Schedule Backup field descriptions 675
Restore field descriptions 676
Managing data retention rules 677
Accessing the Data Retention Rules service 677
Data retention rules 677
Viewing data retention rules 678
Modifying data retention rules 678
Data Retention field descriptions 678
Data Replication Service 679
Data Replication Service 679
Synchronization in a Geographic Redundancy scenario 680
DRS client audit 680
Viewing replica groups 681
Viewing replica nodes in a replica group 681
Repairing a replica node 681
Repairing all replica nodes in a replica group 682
Viewing replication details for a replica node 682
Removing a replica node 683
Removing a replica node from the queue 683
Replica Groups field descriptions 683
Replica Nodes field descriptions 684
Replication Node Details field descriptions 686

Managing scheduled jobs..... 688
Scheduler..... 688
Accessing scheduler..... 689
Viewing pending jobs..... 689
Viewing completed jobs..... 690
Viewing logs for a job..... 690
Filtering jobs..... 691
Editing a job..... 691
Deleting a job..... 692
Disabling a job..... 693
Enabling a job..... 693
Stopping a job..... 694
Pending Jobs field descriptions..... 694
Completed Jobs field descriptions..... 696
Job Scheduling-View Job field descriptions..... 698
Job Scheduling-Edit Job field descriptions..... 699
Job Scheduling-On Demand Job field descriptions..... 701
Disable Confirmation field descriptions..... 702
Stop Confirmation field descriptions..... 703
Delete Confirmation field descriptions..... 704
Chapter 13: SIP phone pre-configuration template..... 705
Creating a new customized SIP phone template..... 706
Creating a SIP phone template from a default template..... 706
Applying a SIP phone template to an existing user..... 707
Modifying endpoint settings for an existing user..... 708
Modifying endpoint settings for a group of existing users..... 708
Removing a SIP phone template..... 709
Chapter 14: SIP Team Button..... 710
SIP Team button..... 710
Administering the SIP Team button..... 710
Appendix A: Restricted commands for the ASSET interface..... 713
Appendix B: Regular Expression constructs..... 714
Appendix C: SNMP support for Session Manager..... 716
Configuring Session Manager Serviceability Agent..... 717
Managing SNMPv3 user profiles..... 718
Creating an SNMPv3 user profile..... 718
Editing an SNMPv3 user profile..... 718
Viewing an SNMPv3 user profile..... 719
Deleting an SNMPv3 user profile..... 719
Filtering SNMPv3 user profiles..... 720
SNMP User profile list..... 720
SNMPv3 user profiles field descriptions..... 721
Managing SNMP target profiles..... 722

Creating an SNMP target profile..... 722
Editing an SNMP target profile..... 723
Viewing an SNMP target profile..... 723
Deleting an SNMP target profile..... 724
Filtering target profiles..... 724
SNMP Target profile list..... 724
SNMP target profiles field descriptions..... 725
Managing Serviceability Agents..... 726
Activating a serviceability agent..... 726
Managing SNMPv3 user profiles for the selected serviceability agents..... 726
Managing target profiles for the selected serviceability agents..... 727
Serviceability Agents list..... 727
System Manager TrapListener service..... 728
Configuring the TrapListener service..... 728
TrapListener service field descriptions..... 728
Session Manager SNMP MIB..... 729
Appendix D: Product notifications..... 734
Viewing PCNs and PSNs..... 734
Registering for product notifications..... 735
Appendix E: List of XML Schema Definitions and sample XMLs for bulk import..... 736
Attribute details defined in Import user XSD..... 839
Attribute details defined in Delete User XSD..... 848
Attribute details defined in the CM Endpoint profile XSD..... 848
Attribute details defined in the Messaging communication profile XSD..... 872
Attribute details defined in the Session Manager communication profile XSD..... 879
Attribute details defined in the Avaya Aura® Conferencing profile XSD..... 883

Chapter 1: Introduction

Purpose

This guide describes how to administer and manage Avaya Aura® Session Manager.

Intended audience

The primary audience for this document is anyone who configures and verifies Session Managerat a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

The audience must have a basic understanding and working knowledge of the following areas:

- Operating systems in general
- TCP/IP
- SSH
- SIP
- FTP and SFTP
- LAN and WAN
- Hostname and DNS

This document does not include optional or customized aspects of a configuration.

Document changes since last issue

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

- Clarified the IP address matching order in the **About Locations** section.
- Added the **RBAC permissions** sections for Routing Import/Export operations, Local host Name Resolution imports, and Bulk Communication Profile edits.
- Added information regarding the **Endpoint Concentrator** to the **About SIP Entities** section.

- Added **endpt conc** as a Connection Policy choice in the **SIP Entity Details field descriptions for other SIP Entity Types** section.

Related resources

Documentation

See the following related documents at http://support.avaya.com.

For the latest information, see the Session Manager Release Notes.

Title	Description	Audience
Overview		
Avaya Aura® Session Manager Security Design	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
Avaya Aura® Session Manager Overview and Specification	Describes the key features of Session Manager.	IT management
Implementation		
Deploying Avaya Aura® Session Manager	Describes how to install and configure a Session Manager instance.	Services and support personnel
Deploying Avaya Aura® Branch Session Manager	Describes how to install and configure Branch Session Manager.	Services and support personnel
Deploying Avaya Aura® Communication Manager on System Platform	Describes how to install the appropriate Communication Manager template, including Branch Session Manager, on the server.	Services and support personnel
Deploying Avaya Aura® Session Manager using VMware® in the Virtualized Environment	Describes how to deploy the Session Manager virtual application in a VMware environment.	Services and support personnel
Upgrading Avaya Aura® Session Manager	Describes the procedures to upgrade a Session Manager to the latest software release.	Services and support personnel
Installing Service Packs for Avaya Aura® Session Manager	Describes the procedures to install service packs on Session Manager.	Services and support personnel
Installing Patches for Avaya Aura® Session Manager	Describes the procedures to install patches on Session Manager.	Services and support personnel
Installing the Avaya S8800 Server for Avaya Aura® Communication Manager	Describes the installation procedures for the S8800 Server.	Services and support personnel

Table continues…

Title	Description	Audience
Installing the Avaya S8510 Server Family and Its Components	Describes the installation procedures for the S8510 Server.	Services and support personnel
Installing the Dell™ PowerEdge™ R610 Server	Describes the installation procedures for the Dell™ PowerEdge™ R610 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R620 Server	Describes the installation procedures for the Dell™ PowerEdge™ R620sServer.	Services and support personnel
Installing the HP ProLiant DL360 G7 Server	Describes the installation procedures for the HP ProLiant DL360 G7 server.	Services and support personnel
Installing the HP ProLiant DL380p G8 Server	Describes the installation procedures for the HP ProLiant DL380p G8 server.	Services and support personnel
Maintaining		
Maintaining and Troubleshooting Avaya Aura® Session Manager	Describes the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and support personnel
Administration		
Administering Avaya Aura® Session Manager	Describes the procedures to administer Session Manager using System Manager.	System administrators
Administering Avaya Aura® Communication Manager Server Options	Describes the procedures to administer Communication Manager as a feature server or an evolution server. Provides information related to Session Manager administration.	System administrators
Avaya Aura® Session Manager Case Studies	Provides case studies about common administration scenarios.	System administrators

Training

The following courses are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go** .

Course code	Course title
1A00236E	Knowledge Access: Avaya Aura® Session and System Manager Fundamentals
4U00040E	Knowledge Access: Session Manager and System Manager Implementation
5U00050E	Knowledge Access: Session Manager and System Manager Support
5U00095V	System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00096V	Avaya Aura® Session Manager Implementation, Administration, Maintenance and Troubleshooting
5U00097I	Avaya Aura® Session and System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00103W	Session Manager 6.2 Delta Overview

Table continues…

Course code	Course title
5U00104W	Session Manager 6.2 Delta Overview
5U00105W	Avaya Aura® Session Manager Overview
ATU00171OEN	Session Manager General Overview
ATC00175OEN	Session Manager Rack and Stack
ATU00170OEN	Session Manager Technical Overview
ATC01840OEN	Survivable Remote Session Manager Administration
3U00100O	Designing Avaya Aura 6.2 Part 1
3U00101O	Designing Avaya Aura 6.2 Part 2

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes,

downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on Session Manager . For more information about the terms of the limited warranty, see the sales agreement or other applicable documentation . In addition, see the standard warranty and details about Session Manager support during the warranty period on the Avaya Support website at https://support.avaya.com. You can find the warranty information at the bottom of the page under **Help & Policies > Policies & Legal > Warranty & Product Lifecycle**. See also **Help & Policies > Policies & Legal > License Terms**.

Chapter 2: Getting started

Overview of System Manager

Avaya Aura® System Manager is the central administration component for Avaya Aura®.

System Manager centralizes provisioning, maintenance, and troubleshooting of Avaya Aura® components.

The System Manager common console is the management interface for Session Manager. You must log on to the System Manager common console to perform any administration or configuration task.

The System Manager common console provides a set of functionality and interfaces that are categorized as follows:

Category	Description
Users	Provides a single interface for provisioning users on most of the Avaya Aura® components. The different types of functionality under this category are as follows: • **Administrators**: Manage administrative users within Avaya Unified Communications Management. • **Directory Synchronization**: Synchronize users with the enterprise directory. • **Groups & Roles**: Manage groups, roles, and assign roles to users. • **User Management**: Administer users in Avaya Aura® elements such as Session Manager and associate Communication Profiles with users. • **User Provisioning Rule**: Assign user provisioning rules.
Elements	Provides features for managing each component of Avaya Aura® solution including the Session Manager element administration. The different types of functionality under this category are as follows: • **Collaboration Environment**: Manage Collaboration Environment elements.

Table continues…

Category	Description
	• **Communication Manager**: Manage Communication Manager objects. • **Communication Server 1000**: Manage Avaya Communication Server 1000 elements. • **Conferencing**: Manage Conferencing application services. • **IP Office**: Manage IP Office elements. • **Meeting Exchange**: Manage Meeting Exchange and Avaya Aura® Conferencing elements. • **Messaging**: Manage Messaging System objects. • **Presence**: Manage Presence-based configuration properties, classes, and access levels. • **Routing**: Configure Network Routing Policy. • **Session Manager**: Manage Session Manager and Branch Session Manager instances. Monitor the system status and analyze the system performance.
Services	Provides a single interface for managing common services. The different types of functionality under this category are as follows: • **Backup and Restore**: Provides the backup and restore functionality for the System Manager database. • **Bulk Import and Export**: Manage the bulk import and export of users, user global settings, roles, and elements. • **Configurations**: Manage systemwide configurations. • **Events**: Manage alarms, views, and, harvest logs that System Manager and other components of System Manager generate. • **Geographic Redundancy**: Manage the System Managergeographic redundancy. • **Inventory**: Manage elements deployed in System Manager. Synchronize the System Manager data with other elements. • **Licenses**: View and configure licenses for one or more Avaya software products. • **Replication**: Provides functionality to view, replicate, and repair replication nodes.

Table continues…

Category	Description
	• **Reports**: Generate reports for elements. • **Scheduler**: Provides the schedule management service for scheduling, tracking, and managing jobs. • **Security**: Manages security certificates. • **Shutdown**: Performs the graceful shutdown of System Manager. • **Software Management**: Perform the upgrade and patch management for Communication Manager devices and IP Office. • **Templates**: Manage templates for Communication Manager and Messaging System objects.

For more information about System Manager, see System Manager documentation on the Avaya Support website at http://support.avaya.com.

Log on to System Manager

Turning off the compatibility mode

About this task

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

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

Procedure

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

Logging on to System Manager web console

Before you begin

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

About this task

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

Important:

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

Procedure

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

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

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

Logon information for users with user name *admin*

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

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

  The system displays the Forced Change Password page. The Forced Change Password page does not contain the **Cancel** button. You must change the password when you log on to the system by using the default password.
- After an upgrade, when you log on to System Manager, you must reset the password.

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

Note:

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

Password and security policies for all administrators

Password aging policy enforcement

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

- Minimum password age
- Password expiration warning
- Password expiration

The system administrator configures the password threshold in days.

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

Password strength policy enforcement

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

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

- Password must not contain a character repeated more than twice consecutively.
- Passwords must not be your user ID, in forward or reverse order.

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

You can can disable the password strength policy.

Password history policy enforcement

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

Password lockout policy enforcement

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

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.

Logon warning banner

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

Editing password policies

About this task

Only an administrator can edit the password settings.

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Security** > **Policies**.
3. In the **Password Policy** section, click **Edit**.

4. On the Password Policy page, edit the required fields.
5. Click **Save**.

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

   Important:

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

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

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

Related Links

Password policies field descriptions on page 31

Editing Session Properties

Procedure

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

Related Links

Session Properties field descriptions on page 32

Security settings

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

Editing the logon warning banner

Procedure

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

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

   Note:

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

Password policies field descriptions

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

Aging section

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

History section

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

Strength section

Field	Description
Strength	The option to enforce password content standards.

Table continues…

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

Lockout section

Name	Description
Lockout	The option to enforce lockout after failed login attempts.
Consecutive Invalid Login Attempts	The number of failed attempts before lockout. Type a value from 1 through 20. The default is 3.
Interval for Consecutive Invalid Login Attempts	The time interval in minutes between invalid login attempts. Type a value from 0 through 120. The default is 10 minutes.
Lockout Time	The number of minutes that the account must be locked after invalid login attempts. Type a value from 0 through 120. The default is 2 minutes.

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

Session Properties field descriptions

Field	Description
Maximum Session Time	The maximum time a session can remain active. Type a value from 0 through 1440.
Maximum Idle Time	The maximum time a session can remain idle. Type any value from 0 through 1440.

Table continues…

Field	Description
	Note: The maximum idle time cannot exceed the maximum session time.

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

Chapter 3: Managing Session Manager using geographic redundant System Manager instances

The Geographic Redundancy feature of System Manager consists of two System Managers located in geographically remote locations. The Geographic Redundancy feature ensures that the enterprise communications remain unaffected during the failure of a single System Manager instance or during the network failures.

The Geographic Redundancy feature provides the following replication mechanisms to ensure data synchronization between the primary System Manager server and the secondary System Manager server:

- Database replication
- File replication
- LDAP replication

In a system consisting of geographic redundant System Managers, the primary components include:

- Two System Manager servers located in geographically diverse locations. One System Manager instance is designated as the primary System Manager. On a sunny day, the primary System Manager manages all elements in the system. The other System Manager instance is designated as the secondary System Manager. The secondary System Manager remains in the standby mode. You can administer the secondary server in the active mode if the primary System Manager fails or loses connectivity with the elements in the system.
- One or more elements that might include Session Manager or Branch Session Manager and other Avaya products.

Important:

In an environment of geographic redundant System Manager instances, the prerequisite is that both the primary System Manager server and the secondary System Manager server must reach each other using FQDN. FQDN must be reachable and resolvable through `/etc/hosts` or DNS.

Before configuring a Session Manager in a geographic redundant environment, ensure the following conditions:

- Both the primary and the secondary System Manager can resolve the Session Manager FQDN through `/etc/hosts`.

- The DNS server contains the IP address or the FQDN entry of all the Session Manager instances that are configured with System Manager. This configuration ensures that both the forward and the reverse lookups of Session Manager work from both the primary and the secondary System Manager servers.

Also, ensure that the servers can reach each other using FQDN.

Terminology

1. An *element* is an instance of an Avaya Aura® network entity. System Manager manages elements such as a Session Manager server or a Communication Manager server in the Avaya Aura® network.

   Note:

   A Session Manager element is *managed* by either the primary or the secondary System Manager in a geographically redundant solution.

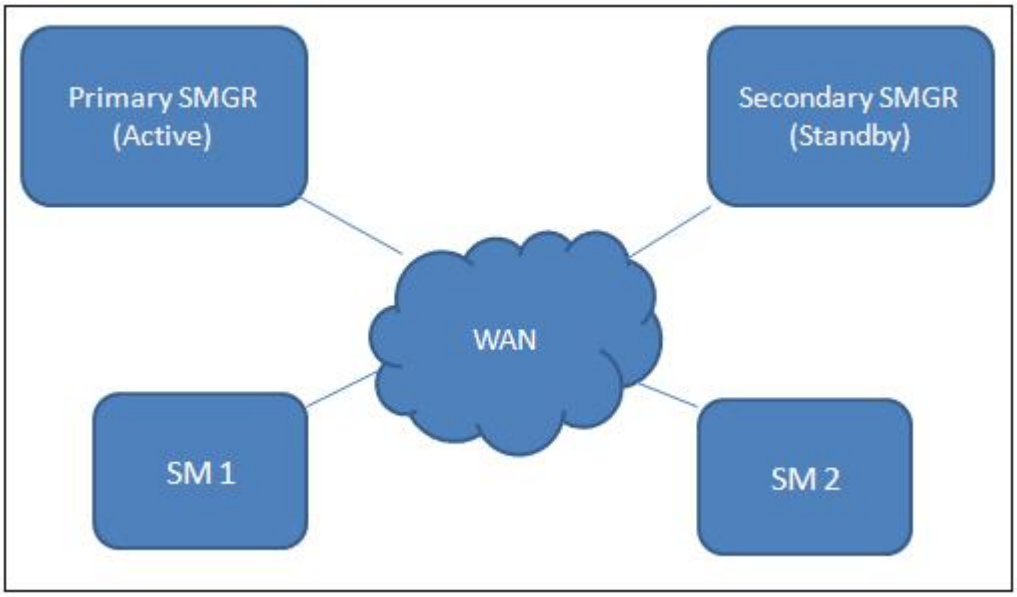
2. The primary System Manager is always in the *active* mode unless you turn off the server. In failback cases, the primary System Manager instance might not be in the active mode.
3. The normal mode of operation of the secondary System Manager is the *standby* mode. In a sunny day scenario, the primary System Manager manages all elements of the Avaya Aura® solution, including Session Manager. The secondary System Manager runs a limited set of services.
4. *Geographic Redundancy-aware* elements are those elements of the Avaya Aura® solution that support the **Geographic Redundancy** feature, such as Session Managers or Branch Session Managers of release 6.3.
5. *Geographic Redundancy-unaware* elements are those elements of the Avaya Aura® solution that do not support the **Geographic Redundancy** feature, such as Session Managers or Branch Session Managers of releases earlier than 6.3.

Geographic Redundancy scenarios

A network with a geographic redundant System Managers operates in the following different modes:

Sunny day scenario:

In this scenario, the primary System Manager is in the active mode and manages all elements in the system. The secondary System Manager is running in the standby mode with the database in the read-only mode.



- The primary System Manager is in the active mode and manages the normal System Manager responsibilities including:
  - Providing a web console for the call routing configuration, the user configuration, and the network configuration administration of Session Manager.
  - Replicating the database to the secondary System Manager.
  - Replicating portions of the database to the various elements.
  - Authenticating and authorizing the elements that require System Manager services.
  - Processing SNMP traps and alarms.
  - Responding to System Manager status requests from elements.
  - Performing normal fault management tasks such as handling alarms tests and maintenance tests.
  - Collecting the performance data from the Session Manager elements.
- The secondary System Manager is in the standby mode and performs the following functions:
  - Receiving the database replication data from the primary System Manager, and storing the data in the database.
  - Authenticating and authorizing the elements that require System Manager services.
  - Processing SNMP traps and alarms.
  - Collecting the performance data from the Session Manager elements.

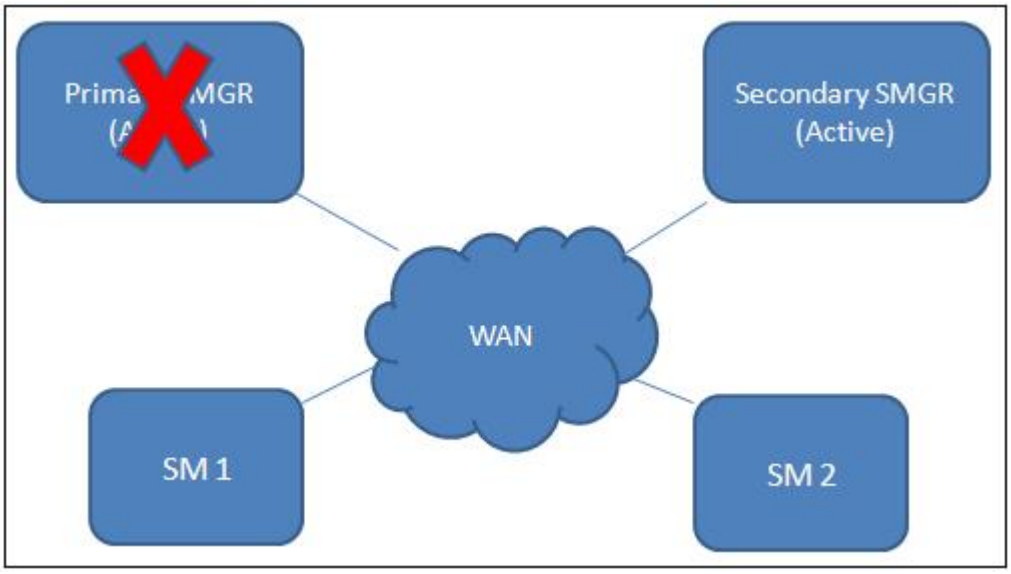
For more information about managing Session Manager in this scenario, see *Managing Session Manager in a Geographically Redundant Solution*.

For more information about upgrading to the geographic redundant system, see *Upgrading to a Geographic Redundancy enabled system*.

For more information about installing a new geographically redundant System Manager system, see *Setting up Geographic Redundancy enabled system*.

Rainy day scenario:

In this scenario, the primary System Manager has failed or has lost connectivity to the elements in the system. The system administrator manually administers the secondary System Manager to the active mode. The secondary System Manager manages all elements in the system.



The description of this scenario is as follows:

- The system sends an alarm to the system administrator.
- The system administrator evaluates the situation, verifies that the failure is real, and administers the secondary System Manager to the active mode.
- The secondary System Manager sends notifications to the elements in the network to indicate that the secondary System Manager is in the active mode.
- The elements in the network verify that the secondary System Manager is in the active mode.

  The Session Manager 6.3 elements automatically connect to the secondary System Manager. For the Session Manager elements that are earlier than the release 6.3, you must manually reconfigure these elements with the secondary System Manager.
- The secondary System Manager replicates the data to the elements. The network operates with the secondary System Manager as the managing System Manager.

The system remains in this state until the administrator restores the system to the Sunny Day configuration.

For more information about managing Session Manager in this scenario, see the topic *Managing Session Manager in a Geographically Redundant Solution*.

To understand the different procedures related to Geographic Redundancy related system failures for this scenario, see the following cases as listed in *Failure Use Cases and Recovery Using the System Manager Geographical Redundancy Feature*.

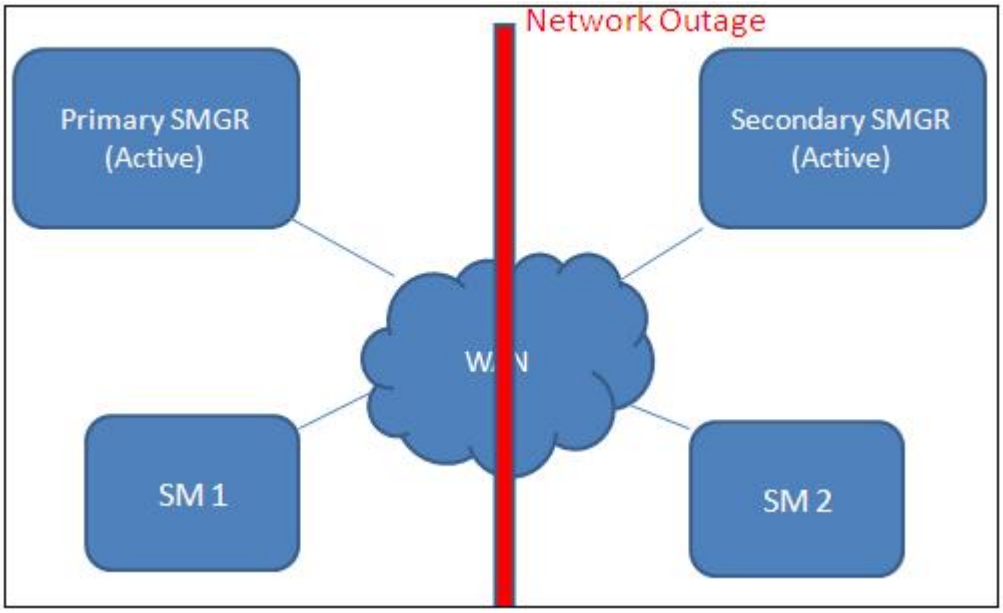
Case 1: The primary System Manager or the primary data center fails. You can recover the data by rebooting the System Manager server or the data center.

Case 2: The primary System Manager fails and needs hardware replacement.

Case 3: Shutting down the primary System Manager for maintenance purpose.

Split-network scenario:

In this scenario, the system administrator administers the secondary System Manager to the active mode when the primary System Manager is also in the active mode.



The description of this split WAN or split network scenario is as follows:

- Originally, the primary System Manager is in the active mode and is communicating with all elements in the network.
- When a connectivity failure occurs in the network:
  - Some elements can only communicate with the primary System Manager.
  - Some elements can only communicate with the secondary System Manager.
  - Some elements can communicate with both the primary System Manager and the secondary System Manager.
- The primary System Manager server and the secondary System Manager server send alarms to the system administrator about the network connectivity failure.
- The system administrator verifies that the network connectivity failure is real and that:
  - Some elements can only communicate with the primary System Manager.
  - Some elements can only communicate with the secondary System Manager.
  - Some elements can communicate with both the primary System Manager and the secondary System Manager.

- The system administrator administers the secondary System Manager to the active mode. Now, both the primary System Manager and the secondary System Manager are in the active mode.
- The secondary System Manager sends notifications to all elements in the network.
- The elements that can communicate with the primary System Manager function normally. The primary System Manager continues to manage these elements. The elements that cannot communicate with the primary System Manager search for a System Manager in the active mode.
- The elements in the network that cannot communicate with the primary System Manager verify that the secondary System Manager is in the active mode.
- The elements in the network that cannot communicate with the primary System Manager, but can communicate with the secondary System Manager, connect to the secondary System Manager. The secondary System Manager starts to manage these elements.
- Any elements that cannot communicate with the primary System Manager or the secondary System Manager cannot perform data replication. These elements continue to operate with the previously replicated data.

The system remains in this state until you restore the system to the Sunny Day configuration.

For more information about managing Session Manager in this scenario, see the topic *Managing Session Manager in a Geographically Redundant Solution*.

For more information about the different Geographic Redundancy related system failures, see the following cases as listed in *Failure Use Cases and Recovery Using the System Manager Geographical Redundancy Feature*.

Case 8: The primary System Manager cannot communicate with the secondary System Manager. Some system elements can only communicate with the primary System Manager while some system elements can communicate only with the secondary System Manager.

Managing Session Manager in a Geographic Redundancy solution

Either the primary or the secondary System Manager server manages Session Manager in different geographic redundancy scenarios. For more information, see *Geographic Redundancy Scenarios*.

1. Determining System Manager that manages each Session Manager:

Session Manager Release 6.3

To view the System Manager server that manages a particular Session Manager, see the **Managed By** column in the **Inventory** > **Manage Elements** webpage. The status can be *Primary*, *Secondary*, or *Unknown*. The *Unknown* value means that the System Manager instance cannot get the status from Session Manager. An active System Manager automatically refreshes this status in a periodic manner. Click **Get Current Status** to refresh the status for each Session Manager.

Session Manager releases earlier than 6.3 version

Session Managers of releases earlier than 6.3 version are not Geographic Redundancy-aware. These Session Manager instances can belong to the earlier deployments of System Managers. Usually, this System Manager instance is the primary server but can also be the secondary server. Run the **smconfig** command at the Session Manager command prompt to view the System Manager that manages the Session Manager.

Note:

For Session Managers of releases earlier than 6.3 version, the **Inventory** > **Managed Elements** webpage displays **Not Supported** in the **Managed By** column.

2. Session Manager administration:

This section provides information about the Session Manager administration for different Geographic Redundancy scenarios.

Sunny day scenario

In this case, the primary System Manager manages all the Session Manager instances. The primary System Manager replicates administration changes to all the Session Manager instances. The secondary server is in the standby mode and you cannot make any administration changes using this server.

Rainy day scenario

In this case, the secondary System Manager manages all the Session Manager instances. The secondary System Manager replicates the administration changes to all the Session Manager instances. The primary server is offline and you cannot make any administration changes using this server.

Split-network scenario

Caution:

Before making administration changes, you must assess the extent of the enterprise network split. The network split results in partitioning of Session Managers and other elements into two groups. The primary System Manager manages one group and the secondary System Manager manages the other group.

Before making administration changes, the administrator must confirm the group membership using the **Inventory** > **Managed Elements** webpage. The administrator must perform the administration changes on the primary System Manager for the Session Manager instances that the primary server manages. Similarly, the administrator must perform the administration changes on the secondary System Manager for the Session Manager instances that the secondary server manages. Each System Manager replicates the administration changes to the respective Session Manager instances. Administration changes must also be compatible with the non-Session Manager elements in the split network. For example, one System Manager must manage all elements that are referenced in a user Communication Profile.

Split-network warning messages

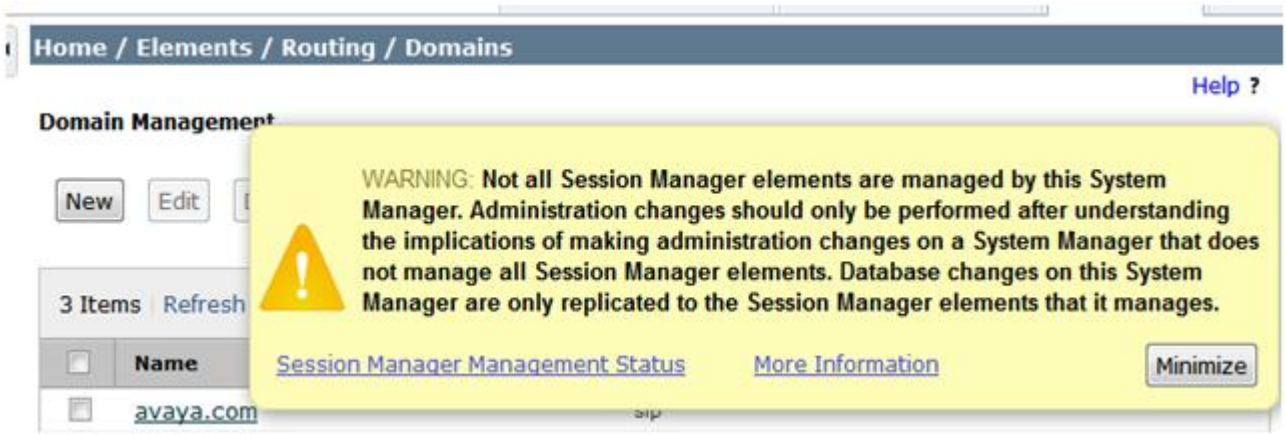
The call routing administration, the user administration, or the network administration webpages display a warning message when the System Manager server detects that the administrator is configuring for a split-network scenario. The primary System Manager can detect the possibility of a split-network configuration if:

- The primary System Manager does not manage all Session Managers.
- The secondary System Manager is not reachable on the network.
- The secondary System Manager is active.

The secondary System Manager can detect the possibility of a split-network configuration if:

- The secondary System Manager is active.
- The secondary server does not manage all Session Managers.

For example, see the following warning message. When the system displays a warning message, click the **Session Manager Management Status** link to go to the **Inventory** > **Manage Elements** webpage. In this webpage, view the status of the System Manager that manages each Session Manager. Click **Minimize** to hide the warning message.



Applicability

The following table lists all the Session Manager administration related functionalities for the respective webpages. When you make administration changes using any of these pages, System Manager replicates these changes only to those Session Manager instances that the System Manager manages.

Webpage	Functionality	Notes
Routing	Change the SIP call routing data.	
Session Manager > **Session Manager Administration**.	Add, edit, delete the Session Manager instances.	
Session Manager > **Communication Profile Editor**>	Edit the Session Manager profiles for the administered SIP users.	Only one System Manager must manage all of the elements that are linked with the Communication Profile of a user. For example,

Table continues…

		Session Managers and Communication Managers that are referred in a user Communication Profile.
Session Manager > **Network Configuration**	Change the Session Manager network configuration.	
Session Manager > **Device and Location Configuration**	Change the device and the location settings.	
Session Manager > **Application Configuration**	Change the Session Manager application sequencing configuration.	
Inventory > **Manage Elements**	Add, edit, or delete the Session Manager instances	
User Management > **Manage Users**>	Change the SIP user configuration or the endpoint configuration.	Only one System Manager must manage all of the elements that are linked with the Communication Profile of a user. For example, Session Managers and Communication Managers that are referred in a user Communication Profile.

3. Session Manager Status and Maintenance :

This section provides information about using a System Manager to view the Session Manager status and perform the maintenance operations on Session Managers. For example, you can view the status of a Session Manager on the **Session Manager** > **Dashboard** webpage or run the maintenance tests on a Session Manager using the **Session Manager** > **Maintenance Tests** webpage. For a full list of applicable status webpages and maintenance webpages, see the *Applicability* section.

Sunny day scenario

In this case, the primary System Manager manages all Session Manager instances. Using the primary System Manager, view the Session Manager system status and perform the maintenance operations. The secondary System Manager is in the standby mode. You cannot use the secondary server to view the Session Manager system status or perform the maintenance operations.

Rainy day scenario

In this case, the secondary System Manager manages all the Session Manager instances. Using the secondary System Manager, view the Session Manager system status and perform the maintenance operations. The primary System Manager is offline and you cannot use the primary server to view the Session Manager system status or perform the maintenance operations.

Split-network scenario

In this case, the administrator must assess the extent of the enterprise network split before viewing the Session Manager system status or performing the maintenance operations on Session Manager. The network split results in partitioning of Session Managers and other elements into two

groups. The primary System Manager manages one group and the secondary System Manager manages the other group.

The administrator must confirm the group membership using the **Inventory** > **Managed Elements** webpage. You must view the Session Manager status and perform the maintenance operations using the System Manager server that manages the Session Manager instance.

Split-network warning messages

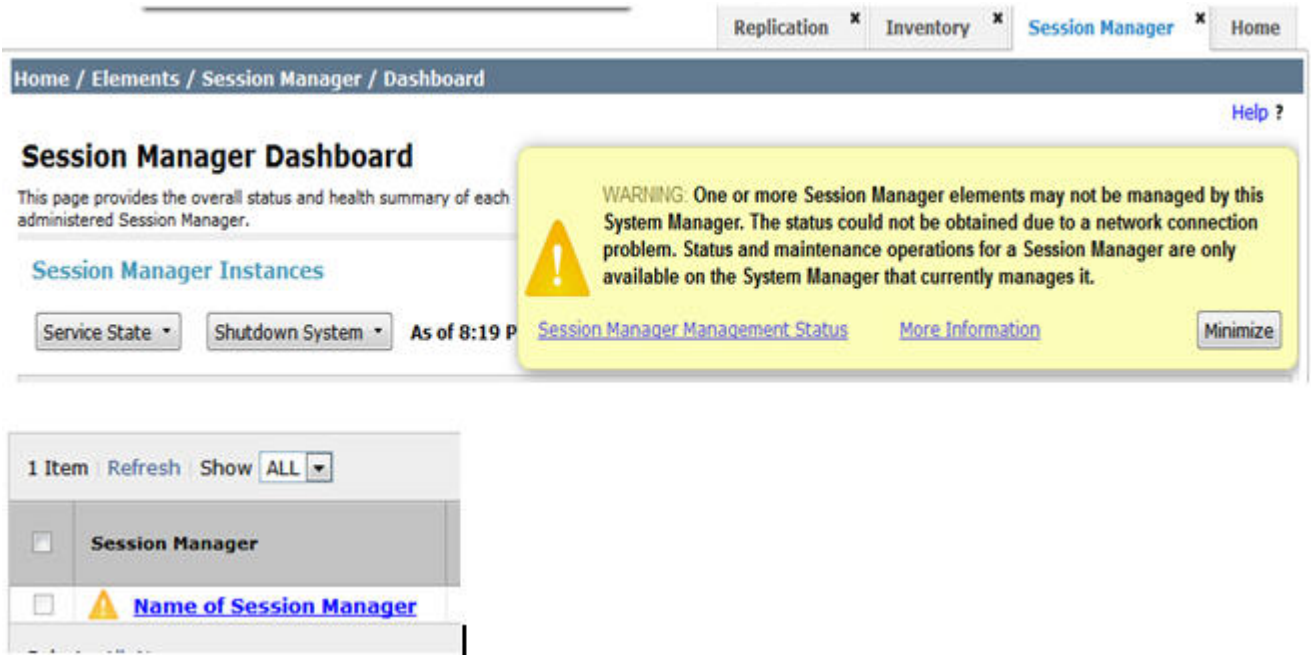
The Session Manager status webpages and the maintenance webpages display a warning message when the current System Manager detects a split-network scenario. The primary System Manager can detect a split-network configuration under the following conditions:

- The primary System Manager does not manage all Session Managers, and
- The secondary System Manager is not reachable on the network, or
- The secondary System Manager is active.

The secondary System Manager can detect a split-network configuration under the following conditions:

- The secondary System Manager is active, and
- The secondary System Manager does not manage all Session Managers.

See the following example of a warning message. If a webpage contains a list of Session Managers, then each Session Manager instance that the System Manager does not manage, remains highlighted with a warning icon. When the system displays a warning message, click the **Session Manager Management Status** link to go to the **Inventory** > **Manage Elements** webpage. In the webpage that contains a list of Session Managers, the system highlights each Session Manager instance that the System Manager does not manage with a warning icon. Click **Minimize** to hide the warning message.



Comments on this document? infodev@avaya.com

Applicability

The following table lists all the system status functions of Session Manager and maintenance operation functions for the respective webpages. The listed functions are only available for Session Managers that the System Manager manages.

Webpage	Functionalities	Notes
Session Manager > **Dashboard**	• View the Session Manager system status. • Accept or deny the new SIP service. • Shut down or restart Session Manager.	
Session Manager > **System Status**	• View the SIP Entity monitoring status. • View the managed bandwidth status. • View the security module status and the maintenance operations status. • View the user registration status and the maintenance operations status.	
Session Manager > **System Tools**	• Run the maintenance tests for Session Managers. • Configure and view the SIP traces. • Run the Session Manager call routing tests.	
Replication	Perform the Session Manager replica maintenance operations.	You can repair the Session Manager replicas from a System Manager that manages the Session Manager.
Inventory > **Manage Elements**	View and edit the trusted and the identify certificate configuration of a Session Manager.	

4. Fault Management (Alarming and Logging):

This section provides information on viewing the Session Manager alarms and the logs using the primary and secondary System Managers.

Sunny day scenario

Both the primary and the secondary System Manager collect alarms from all Session Managers. You can view all Session Manager related alarms from the primary System Manager using the

Events > **Alarms** webpage. The secondary System Manager runs in the standby mode and you cannot view alarms.

Collect logs from a Session Manager server using the **Events** > **Logs** > **Log Harvester** webpage of the primary System Manager. The secondary System Manager is in the standby mode. You cannot collect logs using the secondary System Manager.

View Session Manager audit logs from the primary System Manager using the **Events** > **Logs** > **Log Viewer** webpage. These logs provide details of administration changes made from the primary System Manager. The secondary System Manager runs in the standby mode. You cannot view these logs on the secondary System Manager.

Rainy day scenario

The secondary System Manager collects alarms from all Session Managers. After you configure the secondary System Manager into the active state, view the following alarms using the **Events** > **Alarms** webpage:

- Alarms collected when the secondary server was in the standby mode.
- New Session Manager related alarms.

The primary System Manager is offline. You cannot view alarms using the primary System Manager.

Collect logs from a Session Manager server using the **Events** > **Logs** > **Log Harvester** webpage of the secondary System Manager. The primary System Manager is offline. You cannot collect logs using the primary System Manager.

View Session Manager audit logs from the secondary System Manager using the **Events** > **Logs** > **Log Viewer** webpage. These logs provide details of the administration changes made after the activation of the secondary System Manager. The primary System Manager is offline. You cannot use the primary System Manager to view these logs.

Split-network scenario

In the split-network scenario, both the primary and the secondary System Manager collect alarms from any Session Manager that are reachable on the enterprise network. View these alarms from the **Events** > **Alarms** webpage. If a Session Manager cannot connect to a System Manager because of the network split, the Session Manager forwards all logs to that System Manager when the network connectivity restores. Use the **Inventory** > **Manage Elements** webpage to view the status of the network connectivity from the current System Manager to each Session Manager instances.

View the logs collected from a Session Manager server using the **Events** > **Logs** > **Log Viewer** webpage of the primary or the secondary System Manager that manages the Session Manager server. You cannot collect logs from a Session Manager that the current System Manager does not manage.

View the Session Manager audit logs from both the primary and secondary System Manager using the **Events** > **Logs** > **Log Viewer** webpage. Each System Manager displays audit logs for the administration changes made on that System Manager after the server became active.

5. Performance Management:

This section provides information on the performance data collection and the performance data analysis of Session Manager.

Sunny day scenario

The primary and the secondary System Manager collect the performance data from all Session Managers based on the configuration settings. The configuration settings are available on the **Session Manager** > **Performance** > **Data Collection** webpage of the primary System Manager. Analyze the data in the primary System Manager using the webpages under **Session Manager** > **Performance**. The secondary System Manager is in the standby mode. You cannot analyze the collected performance data using the secondary System Manager.

Rainy day scenario

The secondary System Manager collects the performance data from all Session Managers based on the configuration settings on the **Session Manager** > **Performance** > **Data Collection** webpage of the secondary System Manager. Analyze the data on the secondary System Manager using the webpages under **Session Manager** > **Performance**. The primary System Manager is offline. You cannot analyze the collected performance data using the primary System Manager.

Split-network scenario

The primary and the secondary System Manager collect the performance data from all Session Managers that are reachable on the enterprise network. The system performs the performance data collection on each System Manager based on the settings configured on the **Session Manager** > **Performance** > **Data Collection** webpage of the System Manager.

Note:

You cannot collect the performance data from a Session Manager that is not reachable on the network from the System Manager. When the connectivity restores, the system resumes the performance data collection. Use the **Inventory** > **Manage Elements** webpage to view the status of the connectivity from the current System Manager to each Session Manager.

Both the primary and the secondary System Manager can analyze the performance data using the **Session Manager** > **Performance** webpage. A System Manager server cannot collect the performance data from a Session Manager that is not reachable. This results in data gaps for the unobtainable data until the connection to all Session Managers restores.

Managing data center failures

About this task

This section covers all the possible System Manager failures and enterprise network failure scenarios. This section also provides the detailed procedures for restoring the System Manager back into the normal mode of operation.

For more information about system monitoring, see *Geographic Redundancy Health Monitoring* in *Administering Avaya Aura® System Manager*.

Case 1: The primary System Manager or the primary data center fails.

Procedure

1. Determine whether the System Manager failure is severe.
   - If you can gain access to the primary System Manager in a short duration, restart the primary System Manager and keep the secondary System Manager in the standby mode. In this case, do not follow the procedure in this section.
   - If you cannot gain access to the primary System Manager in a short duration, activate the secondary System Manager and continue to follow the procedures in this section.
2. Manually activate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information, see *Activating the secondary System Manager Server* in *Administering Avaya Aura® System Manager*. Manual activation of the secondary System Manager takes between 10 to 20 minutes. Wait until the secondary System Manager is accessible.

   Avoid making any changes to the call routing configuration, the user configuration, or the network configuration administration on the secondary System Manager. Retaining the same configuration as on the primary System Manager simplifies the process of restoring the system back into the sunny day configuration.
3. Verify that the secondary System Manager is active. Confirm this fact by viewing the Geographic Redundancy webpage of the secondary System Manager.
4. Verify that the secondary System Manager is managing all the Session Manager instances that are Geographic Redundancy-aware.

   For more information, see *Determining the System Manager that Manages each Session Manager*
5. Reconfigure Geographic Redundancy-unaware elements to use the secondary System Manager. Run the **`changeMgmtIP`** command from the Session Manager command line to reconfigure the Session Manager to use the secondary System Manager.

   For more information, see *Changing the IP address or FQDN in System Manager* of *Maintaining and Troubleshooting Avaya Aura® Session Manager*.
6. Verify that the data replication from the secondary System Manager to the Session Manager elements is working.

   To verify the data replication, view the Replication page of the secondary System Manager.

   For more information, see *Managing system data* of *Administering Avaya Aura® Session Manager*.
7. In the **Session Manager** > **System Status** > **User Registrations** webpage of the secondary System Manager, verify that the endpoints can complete the registrations.

For more information, see *User Registration* in *Administering Avaya Aura® Session Manager*.

8. On the secondary System Manager Web Console, using the **Session Manager** > **System Tools** > **Maintenance Tests** webpage, perform the maintenance tests on the Session Manager instances that are managed by the secondary System Manager.

   For more information, see *Maintenance tests* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

9. After the primary System Manager comes back to service, recover the server and configure the secondary System Manager to the standby mode similar to the sunny day scenario. Follow the steps as mentioned below:

   a. Deactivate the secondary System Manager by using the Geographic Redundancy webpage from the secondary System Manager.

      Note:

      For more information, see *Deactivating the secondary System Manager server* in *Administering Avaya Aura® System Manager*.

      Manual deactivation of the secondary System Manager takes between 10 to 20 minutes.

   b. Verify that the secondary System Manager is in the standby mode by checking the Geographic Redundancy webpage of the primary System Manager.

      Logging in to the secondary System Manager Web Console must indicate that the System Manager is in the standby mode.

   c. From the primary System Manager, run the database recovery procedure in the Geographic Redundancy webpage.

      Using this step, you can keep the current primary System Manager database or replace with the secondary System Manager database. For more information, see *Restoring the primary System Manager server* in *Administering Avaya Aura® System Manager*.

   d. Verify that the primary System Manager is managing all the Geographic Redundancy-aware elements.

      For more information, see *Determining the System Manager that Manages each Session Manager*.

   e. Reconfigure the Geographic Redundancy-unaware elements to use the primary System Manager. To reconfigure a Session Manager to use the primary System Manager, run the **`changeMgmtIP`** command from the command line.

      For more information about changing the IP address or the FQDN, see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

Case 2: Primary System Manager fails and needs a hardware replacement.

Procedure

1. Shut down the primary System Manager.

   For more information, see *Graceful shutdown* in *Administering Avaya Aura® System Manager*.

2. Activate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information about activating the server, see *Activating the secondary System Manager Server* in *Administering Avaya Aura® System Manager*. Manual activation of the secondary System Manager takes between 10 to 20 minutes. Wait until the secondary System Manager is accessible.

   Avoid making any changes to the call routing configuration, the user configuration, or the network configuration administration on the secondary System Manager. Retaining the same configuration as on the primary System Manager simplifies the process of restoring the system back into the sunny day configuration.

3. Verify that the secondary System Manager is active by logging into the Web Console.

4. Verify that the secondary System Manager is managing all Geographic Redundancy-aware elements.

   For more information about determining the System Manager that manages each Session Manager, see *Determining the System Manager that Manages each Session Manager*.

5. If you have not enabled geographic redundancy for some Session Managers, then you must manually reconfigure these elements to use the secondary System Manager. Run the **`changeMgmtIP`** command from the Session Manager command line to reconfigure the Session Manager to use the secondary System Manager.

   For more information about changing the IP address or the FQDN, see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

6. Perform the hardware replacement procedure.

   For more information about the field replacement of the primary System Manager, see the related server documentation from the Avaya support site.

7. Deactivate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information about deactivating the secondary System Manager, see *Deactivating the secondary System Manager server* in *Administering Avaya Aura® System Manager*.

Note:

Manual deactivation of the secondary System Manager takes between 10 to 20 minutes.

8. Verify that the secondary System Manager is in the standby mode by checking the *Geographic Redundancy* webpage of the primary System Manager.

   Logging in to the secondary System Manager Web Console must indicate that the System Manager is in the standby mode.

9. From the primary System Manager, run the *database recovery* procedure from the Geographic Redundancy webpage. Using this step, you can keep the current primary System Manager database or replace with the database from the secondary System Manager.

   For more information about restoring the primary System Manager server, see *Restoring the primary System Manager server* in *Administering Avaya Aura® System Manager*.

10. Verify that the primary System Manager is managing all the Geographic Redundancy-aware elements.

    For more information, see the topic *Determining the System Manager that Manages each Session Manager*.

11. Reconfigure the Geographic Redundancy-unaware elements to use the primary System Manager. To reconfigure a Session Manager to use the primary System Manager, run the **`changeMgmtIP`** command from the command line.

    For more information about changing the IP address or the FQDN, see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

Case 3: Replacing the secondary System Manager due to hardware failures.

For more information about the field replacement of the secondary System Manager, see *Activating the secondary System Manager Server* in *Administering Avaya Aura® System Manager*.

Case 4: Shutting down the primary System Manager for maintenance.

Follow the procedure in Case 2.

Case 5: The primary System Manager cannot communicate with the secondary System Manager. The system elements can

communicate with the primary System Manager and the secondary System Manager

Restore the network connection between the primary System Manager and the secondary System Manager.

Case 6: The primary System Manager cannot communicate with the system elements, but the elements can communicate with the secondary System Manager

Procedure

1. Activate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information about activating the secondary System Manager server, see *Activating the secondary System Manager Server* in the book *Administering Avaya Aura® System Manager*. Manual activation of the secondary System Manager takes between 10 to 20 minutes. Wait until the secondary System Manager is accessible.

   Avoid making any changes to the call routing configuration, the user configuration, or the network configuration administration on the secondary System Manager. Retaining the same configuration as on the primary System Manager simplifies the process of restoring the system back into the sunny day configuration.

2. Verify that the secondary System Manager is managing all the geographical redundancy-aware Session Manager instances.

   For more information about determining the System Manager that manages each Session Manager, see *Determining the System Manager that Manages each Session Manager*.

3. Reconfigure the Geographic Redundancy-unaware elements to use the secondary System Manager. Run the **`changeMgmtIP`** command from the Session Manager command line to reconfigure the Session Manager to use the secondary System Manager.

   For more information about changing the IP address or the FQDN , see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

4. Deactivate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information, see *Deactivating the secondary System Manager server* in *Administering Avaya Aura® System Manager*.

   Note:

   Manual deactivation of the secondary System Manager takes between 10 to 20 minutes.

5. Verify that the secondary System Manager is in the standby mode by checking the *Geographic Redundancy* webpage of the primary System Manager. Logging in to the secondary System Manager Web Console must indicate that the System Manager is in standby mode.
6. From the primary System Manager, run the *database recovery* procedure from the Geographic Redundancy webpage. Using this step, you can keep the current primary System Manager database or replace with the database from the secondary System Manager.

   For more information, see *Restoring the primary System Manager server* in *Administering Avaya Aura® System Manager*.
7. Verify that the primary System Manager is managing all the Geographic Redundancy-aware elements.

   For more information, see *Determining the System Manager that Manages each Session Manager*.
8. Reconfigure the Geographic Redundancy unaware-elements to use the primary System Manager. To reconfigure a Session Manager to use the primary System Manager, run the **`changeMgmtIP`** command from the command line.

   For more information about changing the IP address or the FQDN, see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

Case 7: System elements can communicate only with the primary System Manager

Restore the network connection between the system elements and the secondary System Manager.

Case 8: The primary System Manager cannot communicate with the secondary System Manager. Some system elements can communicate only with the primary System Manager while some system elements can communicate only with the secondary System Manager

Procedure

1. Activate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information about activating the secondary System Manager server, see *Activating the secondary System Manager Server* in *Administering Avaya Aura® System Manager*.

Manual activation of the secondary System Manager takes between 10 to 20 minutes. Wait until the secondary System Manager is accessible.

Avoid making any changes to the call routing configuration, the user configuration, or the network configuration administration on the secondary System Manager. Retaining the same configuration as on the primary System Manager simplifies the process of restoring the system back into the sunny day configuration.

2. Verify that the secondary System Manager is managing the Geographic Redundancy-enabled Session Manager instances that cannot communicate with the primary System Manager.

   For more information, see *Determining the System Manager that Manages each Session Manager*.

3. Reconfigure the Geographic Redundancy-unaware elements that cannot communicate with the primary System Manager to use the secondary System Manager. Run the **changeMgmtIP** command from the Session Manager command line to reconfigure the Session Manager to use the secondary System Manager.

   For more information, see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

4. Restore the network connection between the primary System Manager and the elements that are not connected to the primary System Manager. Restore the network connection between the secondary System Manager and the elements that cannot connect to the secondary System Manager.

5. Deactivate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information, see *Deactivating the secondary System Manager server* in *Administering Avaya Aura® System Manager*.

   Note:

   Manual deactivation of the secondary System Manager takes between 10 to 20 minutes.

6. Verify that the secondary System Manager is in standby mode by checking the *Geographic Redundancy* webpage of the primary System Manager.

   Logging in to the secondary System Manager Web Console must indicate that the System Manager is in the standby mode.

7. From the primary System Manager, run the *database recovery* procedure from the Geographic Redundancy webpage. Using this step, you can keep the current primary System Manager database or replace with the database from the secondary System Manager.

   For more information about restoring the primary System Manager server, see *Restoring the primary System Manager server* in *Administering Avaya Aura® System Manager*.

8. Verify that the primary System Manager is managing all the Geographic Redundancy-aware elements.

For more information about determining the System Manager that manages each Session Manager, see *Determining the System Manager that Manages each Session Manager*.

9. Reconfigure the Geographic Redundancy-unaware elements to use the primary System Manager. To reconfigure a Session Manager to use the primary System Manager, run the **changeMgmtIP** command from the command line.

   For more information about changing the IP address or the FQDN, see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

   For more information about managing Session Manager in a split-network scenario, see *Managing Session Manager in a Geographically Redundant Solution*.

Setting up a Geographic Redundancy enabled system

Before you begin

Ensure that the installed primary and the secondary System Manager servers:

- Contain the same hardware.
- Satisfy the following requirements:
  - Must have the same hardware configuration.
  - Must contain the same version of the System Manager software that includes the template, the software packs, and the patches.
  - Must contain the same version of the System Platform software that includes the software packs.
  - Must be able to communicate with each other over the network.
  - Must have synchronized network time.

The high-level steps for setting up the Geographic Redundancy-enabled system are as follows:

Procedure

1. Install the primary System Manager with the release 6.3 software or upgrade the System Manager server to the release 6.3.
2. Install the System Manager 6.3 software version on the secondary System Manager.
3. Configure the two System Managers for the Geographic Redundancy operation. For more information, see *Configuring Geographic Redundancy* in *Administering Avaya Aura ® System Manager*.
4. Enable the replication of the primary System Manager data to the secondary System Manager. For more information, see *Enabling the Geographic Redundancy replication* in *Administering Avaya Aura® System Manager*.
5. Conduct the system verification tests to verify the Geographic Redundancy-enabled system. For more information, see *System Verification Tests*.

Upgrading to a Geographic Redundancy-enabled system

About this task

The two basic ways to upgrade an Avaya Aura® solution to a Geographic Redundancy-enabled system, where System Manager is geographically redundant, are:

- Simultaneous element upgrade method
- Selected element upgrade method

Simultaneous element upgrade method

Procedure

1. Upgrade the System Manager server to the release 6.3. The upgraded System Manager server becomes the primary System Manager.
2. Fresh install the System Manager release 6.3 software for the secondary System Manager server.
3. Log in to the secondary System Manager and enable the Geographic Redundancy feature. This step configures the current System Manager as the secondary and the upgraded System Manager as the primary. For more information about configuring the geographic redundancy feature, see *Configuring Geographic Redundancy* in *Administering Avaya Aura® System Manager*.
4. Associate the secondary System Manager and the SAL Gateway with the primary System Manager as the new trap destination. This step ensures that the alarms generated on the various elements are send to both System Managers, associated SAL Gateways, and to any customer designated Network Management Systems (NMS) within the solution. For more information about managing alarms, see *Managing Alarms* in *Administering Avaya Aura ® System Manager*.
5. Enable replication from the primary to the secondary System Manager. For more information about enabling the geographic redundancy replication, see *Enabling the Geographic Redundancy replication* in *Administering Avaya Aura® System Manager*.
6. Upgrade Session Managers and Branch Session Managers to the release 6.3. For more information about upgrading Session Manager, see *Upgrading Avaya Aura® Session Manager*.
7. Now, System Managers and Session Managers operate in the Geographic Redundancy mode.
8. Conduct the system verification tests to verify the Geographic Redundancy-enabled system. For more information about the system verification tests, see *System Verification Tests*.

Selected element upgrade method

Procedure

1. Upgrade the System Manager server to System Manager 6.3. This server becomes the primary System Manager. Fresh install a new System Manager 6.3 server as the secondary server.
2. Log in to the secondary System Manager server and enable geographical redundancy. This step configures the current System Manager as the secondary and the upgraded System Manager as the primary. For more information about configuring geographic redundancy, see *Configuring Geographic Redundancy* in *Administering Avaya Aura® System Manager*.
3. Associate the secondary System Manager and the SAL Gateway with the primary System Manager as new trap destination. This step ensures that the alarms generated on the various elements are send to both System Managers, associated SAL Gateways, and to any customer designated Network Management Systems (NMS) within the solution. For more information about administering System Manager, see *Administering Avaya Aura ® System Manager*.
4. Enable replication from the primary to the secondary System Manager. For more information about enabling the Geographic Redundancy replication, see *Enabling the Geographic Redundancy replication* in *Administering Avaya Aura® System Manager*.
5. **(Optional)** Upgrade Session Managers and Branch Session Managers to the release 6.3.
6. Now the upgraded System Managers and Session Managers begin operating in Geographic Redundancy-enabled mode.
7. Conduct the system verification tests to verify the Geographic Redundancy-enabled system. For more information about the system verification tests, see *System Verification Tests*.
8. Using this upgrade method, upgrade the remaining elements at a later time.

Performing system verification tests

About this task

Use this procedure to verify that a Geographic Redundancy-enabled system is operating correctly in the *Sunny day scenario*.

Procedure

1. Check the Geographic Redundancy status of the system. Go to the Geographical Redundancy webpage of the primary System Manager and verify the expected configuration settings. To view the Geographic Redundancy condition, go to the **Geographic Redundancy** > **GR Health** webpage of the primary System Manager.

For more information about the Geographic Redundancy Health Monitoring, see *Geographic Redundancy Health Monitoring* in *Administering Avaya Aura® System Manager*.

2. In the **Session Manager Dashboard** webpage, verify the status for each Session Manager and Branch Session Manager. Optionally, run the System Manager maintenance tests and the Session Manager maintenance tests from the primary System Manager using the **Session Manager** > **System Status** > **Maintenance Tests** webpage.

   For more information about the maintenance tests, see *Maintenance Tests* in *Administering Avaya Aura® Session Manager*.

Chapter 4: Synchronizing Communication Manager data with the System Manager database

The following sections explain how to synchronize the Communication Manager station data with the System Manager database. The system automatically connects to System Manager and to Communication Manager in the core. The system, then synchronizes the provisioning data in the System Manager database with each managed Communication Manager instance.

Synchronize the endpoint data in a scheduled and incremental basis by:

- administering each Communication Manager instance as an entity or application instance.
- initializing the synchronization of Communication Manager and the messaging data with System Manager.

Creating a Communication Manager instance in the system

Creating a new element

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Click **New**.
4. On the New Elements page, in the **Type** field, select an element.
5. On the New <element-name> page, on the **General** and **Attributes** tabs, complete the required fields.
6. Click **Commit**.

   The system creates a new element.

Add Communication Manager field descriptions

General Attributes

Field	Description
Name	The name of Communication Manager instance.
Hostname or IP Address	The host name or the IP address of the Communication Manager instance. For the duplicated Communication Manager, this value references the active server IP address.
Login	The login name that you use to connect to the Communication Manager instance. **Note:** craft, craft2, dadmin, inads, init, rasaccess, sroot, and tsc are the restricted logins when you configure a Communication Manager system. Do not use the login name to connect to: • The Communication Manager instance from any other application. • The Communication Manager SAT terminal using command line interface (CLI).
Authentication Type	The authentication type. The following are the types of authentication: • **Password**: The password that authenticates the SSH or Telnet login name on the element. • **ASG Key**: The ASG key used to authenticate the ASG login.
Password	The password that authenticates the SSH or Telnet login name on the element.
Confirm Password	The password that you retype for confirmation. **Confirm Password** must match **Password**.
ASG Key	The ASG key used to authenticate the ASG login.
Confirm ASG Key	The ASG key that you retype for confirmation. **Confirm ASG Key** must match **ASG Key**.
SSH Connection	An option to use SSH for connecting to the element. By default, the system selects the check box. If you clear the check box, the system uses Telnet to connect to the element.

Table continues…

Field	Description
RSA SSH Fingerprint (Primary IP)	The RSA SSH key of the Communication Manager server. For duplex servers, the RSA SSH key is the key of the active server.
RSA SSH Fingerprint (Alternate IP)	The DSA SSH key of the standby Communication Manager server. Use the DSA SSH key only for duplex servers.
Description	A description of the Communication Manager server.
Alternate IP Address	The alternate IP address of the element. For duplex servers, the alternate IP address is the IP address of the standby server.
Enable Notifications	A real-time notification whenever an administrative change occurs in Communication Manager. For example, when you add or delete an extension from Communication Manager outside System Manager. Select the check box to enable the CM Notify sync feature for this Communication Manager instance. Clear the check box to disable 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 certain changes administered on Communication Manager to System Manager asynchronously. **Note:** Communication Manager 6.2 or later supports this feature.
Port	The port on which the service provided by the element is running. The default SSH port is 5022 if you select the **SSH Connection** check box. The default SSH port is 5023 if you do not select the **SSH Connection** check box.
Location	The location of the element.
Add to Communication Manager	Select the Communication Manager that you want to view in the communication manager list.

SNMPv1 Attributes

Field	Description
Version	The SNMP protocol type.
Read Community	The read community of the device.
Write Community	The write community of the device.

Table continues…

Field	Description
Retries	The number of times an application polls a device without receiving a response before timing out.
Timeout (ms)	The number of milliseconds an application polls a device without receiving a response before timing out.
Device Type	The type of device.

SNMPv3 Attributes

Field	Description
Version	The SNMP protocol type.
User Name	The user name as defined in the application.
Authentication Protocol	The authentication protocol that authenticates the source of traffic from SNMP V3 protocol users. The possible values are: • **MD5 (default)** • **SHA** • **None**
Authentication Password	The SNMP authentication password.
Confirm Authentication Password	The SNMP authentication password that you retype for confirmation. **Authentication Password** and **Confirm Authentication Password** must match.
Privacy Protocol	The encryption policy for SNMP V3 users. The possible values are: • **AES**: Use the AES encryption for the SNMP-based communication. AES is the default protocol. • **DES**: Use the DES encryption for the SNMP-based communication. • **None**: Do not encrypt traffic for this user.
Privacy Password	The pass phrase used to encrypt the SNMP data.
Confirm Privacy Password	Retype the privacy password in this field for confirmation.
Retries	The number of times the application polls a device without receiving a response before timing out.
Timeout (ms)	The number of milliseconds the application waits for the response from the device being polled.
Device Type	The type of device.

Button	Description
Commit	Click to add a Communication Manager instance in the inventory.
Clear	Click to clear all the entries.
Cancel	Click to cancel your action and return to the previous page.

Creating a Messaging instance

Procedure

1. On System Manager Web Console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**. The system displays the Manage Elements page.
3. Click **New**, and select a `Messaging` entity instance from the drop-down list. The system displays the New Messaging instance page.
4. On the **General** tab, enter the appropriate details for the following fields:
   a. **Name**: The name of the Communication Manager instance.
   b. **Type**: The type of the Communication Manager instance.
   c. **Description**: The details of the Communication Manager instance.
5. In the **Node** field, enter the FQDN or IP address details of Messaging Storage Server (MSS).
6. When you enter other details, ensure that you fulfill the following conditions:
   - Before you add the Messaging box in System Manager applications, ensure that:

     In the Trusted Server list on the Messaging box, add the System Manager server details or the Communication System Management server details.

     Note:

     You can find the Messaging box on the Messaging Administration/Trusted Servers screen.
   - The login credentials of the Messaging box trusted servers screen and the login credentials of the Session Manager application, entity, and attributes for a Messaging type of application must be identical.
   - The **Trusted Server Name** field on the Trusted Server page is mapped to the **Login** field in the Attributes section. The **Password** field on the Trusted Server page is mapped to the **Password** field in the Attributes section.
   - To allow the LDAP access to the Messaging box from the trusted server, on the Trusted Server page, set the **LDAP Access Allowed** field to `yes`.
7. Click **Commit**.

When you add an application entity through Manage Elements pages, in the background, System Manager imports relevant data from the application instance to the Communication System Management database.

Check the status of data import by accessing:

- The job scheduler located at **System Manager Data** > **Scheduler**.
- Log files on the Communication System Management server.

Synchronizing the Communication Manager data and configuring options

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Communication System**.
3. Select the Communication Manager device that you want to synchronize.
4. Select any of the following options that you want to synchronize for the selected device:
   - **Initialize data for selected devices**: To synchronize data in the System Manager database with each managed Communication Manager system.

     Note:

     When you add a Communication Manager instance to the system, System Manager automatically initiates an initialization task to get all the required Communication Manager data and stores the data in the System Manager database.
   - **Incremental Sync data for selected devices**: To synchronize incrementally the selected devices data in the System Manager database with each managed Communication Manager system.

     Note:

     This synchronization updates the data in the database in Communication Manager that is changed since last synchronization.
   - **Execute 'save trans all' for selected devices**: To save the configuration of the selected device on the same device, Communication Manager itself.
5. Perform one of the following:
   - Click **Now** to perform the synchronization now.
   - Click **Schedule** to perform the synchronization at a specified time.

Note:

To view the status of synchronization, on System Manager web console, click **Services** > **Scheduler**.

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.

Manage Elements field descriptions

Field	Description
Name	The name of the element.
Node	The node on which the application runs.
Type	The type of the element to which the instance belongs. **Note:** You can view this field only if you gain access to the Manage Elements page from **Inventory**.

The system also provides the following fields on System Manager that is configured with Geographic Redundancy.

Reachable	The state that mentions whether the element is reachable from the current server. The values are `Yes` and `No`.
Managed by	The field that specifies the server that manages this element. The options are `Primary` and `Secondary`. For a non-GR element, the field displays `Not Supported`.

Table continues…

Last Updated Time	The time when the system updates the status of the element
Error	Displays a red cross icon ( ) if the system generates errors. For more information, click the icon.
Warning	Displays an yellow triangle icon ( ) if the system generates warnings. For more information, click the icon.

Note:

At any given point of time, you can perform **Get Current Status**, **Manage**, or **Unmanage** operation.

Button	Description
View	Displays the View <Element-name> page. Use this page to view the details of the selected element.
Edit	Displays the Edit <Element-name> page. Use this page to modify the information of the instance.
New	Displays the New Elements page. Use this page to create a new element.
Delete	Displays the Delete <Element-name> page. Use this page to delete a selected element.
Get Current Status	Displays 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 > **Configure Trusted Certificates**	Displays the Trusted Certificates page. Use this page to view, add, export, and delete the trusted certificates for the element.
More Actions > **Configure Identity Certificates**	Displays the Identity Certificates page. Use this page to view, export, renew, and replace the identity certificates for the element.

Table continues…

Button	Description
More Actions > **Manage**	System Manager starts managing the element that you select.
More Actions > **Unmanage**	System Manager stops managing the element that you select.
More Actions > **Import**	Displays the Import Applications page. Use this page to import application data in bulk from a valid XML file.
More Actions > **View Notification Status**	Displays the status of notifications. The valid status values are Failed and Inprogress. The system displays the progress bar if a notification is pending. The system displays the **Resend Notification** button only when there are no notifications in progress and when you select the rows of the same event type. If you click **Resend Notification**, the system displays a progress bar until the resend action fails or completes. 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.
Filter: Enable	Displays 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.

Element details field descriptions

The fields on this page varies with the element that you manage.

General

Field	Description
Name	The name of the element.
Type	The type of the application to which the element belongs.
Description	A brief description of the element.
Node	The node on which you run the element. **Note:** The system displays the **Node** field when you select **Other** from the **Node** field.

Access Profile

Field	Description
Name	The name of the access profile.
Access Profile Type	The type of the access profile. The options are: • **URI**: For system web services API. • **SSH**: For Software Management functions. • **SNMP**: For discovering elements.
Access Profile Sub Type	The sub type of the URI access profile. The options are: • **EMURL**: To create a URL type access profile. • **WS**: To create a web service access profile. • **GUI**: To create a GUI access profile. • **GRCommunication**: To create a GR-aware element. • **TenantURL**: To create the tenant-related access profile. • **Other**
Protocol	The protocol that the element supports to communicate with other communication devices.
Host	The name of the host on which the element is running.
Port	The port on which the element is running.
Order	The order in which you gain access to access profiles.

Button	Description
View	Displays fields in the Access Profile section that you can use to view access profile details.
New	Displays fields in the Access Profile section that you can use to add access profile details.
Edit	Displays fields in the Access Profile section using which you can modify the access profile details that you select.
Delete	Deletes the selected access profile.

Application System Supported Protocol

The system displays the following fields when you click **New** or **Edit** in the **Access Profile** section:

Field	Description
Protocol	The protocol used to access profiles. The options are: • **URI**: For system web services API. • **SSH**: For Software Management functions. • **SNMP**: For discovering elements. **Note:** The page displays the button only when you click **Add** or **Edit** in the **Access Profile** section.

Access Profile Details

The page displays the following fields when you click **URI** in the **Protocol** field:

Field	Description
Name	The name of the access profile.
Access Profile Type	The type of the access profile. The options are: • **TrustManagement**: To create a trust management type of access profile. • **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**

Table continues…

Field	Description
Protocol	The protocol for communicating the element.
Host	The name of the host on which the element is running.
Port	The port on which the element is running.
Path	The path to gain access to the access profile.
Order	The order in which you gain access to access profiles.
Description	A brief description of the access profile.

The page displays the following fields when you click **SSH** in the **Protocol** field:

Field	Description
Name	The name of the access profile.
Login Name	The login name as configured on the element.
Port	The port on which the element is running.
Use ASG Key	The option to use the ASG encryption.
Password	The password to log in to the element.
Confirm Password	The password that you retype.

The page displays the fields when you click **SNMP** in the **Protocol** field and **V3** in the **Type** field:

Field	Description
Profile Name	The name of the profile.
Description	A brief description of the profile.
Type	The SNMP protocol type. The possible values are V1 and V3.
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. Passwords must contain at least eight characters.

Table continues…

Field	Description
Confirm Authentication Password	The SNMP V3 protocol authentication password that you retype for confirmation.
Privacy Type	The encryption policy for an SNMP V3 user. The possible values are: • **DES**: For SNMP-based communication. The default is **DES**. • **AES**: For SNMP-based communication. • **None**: Does not encrypt traffic for this user. Set **Privacy Type** only for an SNMP V3 user.
Privacy Password	The password used to enable the **DES** or **AES** encryption. DES passwords must contain at least eight characters.
Confirm Privacy Password	The privacy password that you retype for confirmation.
Privileges	The privileges that determine the operations that you can perform on MIBs. • **Read/Write**: To perform GET and SET operations. • **Read**: To perform only the GET operation. • **None** The default is None.
Timeout	The time in milliseconds for which the element waits for a response from the device being polled during discovery.
Retries	The number of times that the element polls a device without receiving a response before timing out.

The page displays the fields when you click **SNMP** in the **Protocol** field and **V1** in the **Type** field:

Field	Description
Profile Name	The name of the profile.
Description	A brief description of the profile.
Type	The SNMP protocol type. The possible values 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.

Table continues…

Field	Description
	Write Community applies only to the SNMP V1 protocol.
Timeout	The time in milliseconds for which the element waits for a response from the device that the element polls.
Retries	The number of times that the element polls a device and fails to receive a response. After the retries, the element times out.

Button	Description
Save	Saves the access profile details. **Note:** This button is visible only when you click **Add** and **Edit** in the **Access Profile** section.
Cancel	Cancels the operation of creating or editing an access profile and hides the fields where you enter or modify the access profile information. **Note:** This button is available only when you click **Add** and **Edit** in the **Access Profile** section.

Port

Field	Description
Name	The name of the port.
Port	The port on which the element is running.
Protocol	The protocol for the corresponding port.
Description	A brief description about the port.

Button	Description
New	Displays fields in the Port section that you can use to add a port.
Edit	Displays fields in the Port section with port information. You can change the port details in the port mode.
Delete	Deletes the selected configured port.
Commit	Saves the port details. **Note:** The section displays the **Save** button only when you click **Add** or **Edit** in the **Port** section.

Table continues…

Button	Description
Cancel	Cancels the current operation of creating or editing an access profile and hides the fields where you add or modify the port information. **Note:** The section displays the **Cancel** button only when you click **Add** or **Edit** in the **Port** section.

Attributes

Use this section to configure attributes for the selected element.

The following fields display the information about attributes defined for System Manager.

Field	Description
IP	The IP address of System Manager.
FQDN	FQDN of System Manager.
Virtual IP	The virtual IP address of System Manager.
Virtual FQDN	The virtual FQDN of System Manager.
isPrimary	The option to indicate if the element is primary or secondary.

Assign elements

Name	Description
Name	The name of the element.
Type	The type of the application to which the element belongs.
Description	A brief description about the element.

Button	Description
Assign elements	Displays the Assign elements page that you use to assign an element to another element.
Unassign elements	Removes an assigned element.

Button	Description
Commit	Creates or modifies an element by saving the information to the database. **Note:** The system displays the button only when you click **Add** or **Edit** on the Manage Elements page.
Cancel	Closes the page without saving the information and navigates back to the Manage Elements page.

For example, the following fields provide information about attributes that you can define for Messaging.

Field	Description
Login	The name in the **Trusted Server Name** field of the Trusted Servers page on the Messaging server.
Password	The password as given in the **Password** field of the Trusted Servers page on the Messaging server.
Confirm Password	The password that you retype for confirmation.
Messaging Type	The type of the Messaging server. The following types are supported: • **MM**: Modular Messaging • **CMM**: Communication Manager Messaging • **AURAMESSAGING**: Avaya Aura® Messaging
Version	The version of Messaging. Supported versions are 5.0 and later.
Secured LDAP Connection	An option to use the secure LDAP connection. 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.

Chapter 5: Managing security

The Trust Management module provides certificates to ensure secure communication between elements . Trust Management provides Identity and Trusted (root) certificates to establish mutually authenticated TLS sessions.

Using the Trust Management service, you can perform the following operations for an application instance:

- View installed Trusted and Identity certificates on the Session Manager server.
- Add or remove Trusted certificates on the Session Manager server.
- Replace or renew Identity Certificates on the Session Manager server.

Certificate management

Session Manager uses five unique certificates: WebSphere, SAL Agent, Management, SIP, and HTTPS. SIP and HTTPS are the most important because these certificates communicate with outside entities such as Communication Manager and endpoints.

Any changes to these interfaces can cause major service interruptions. *Be very careful when changing these certificates.* The near end and far end use the certificates to trust each other. Each side presents its identity certificate during TLS negotiation. If one side does not trust the identity certificate of the other side, the connect fails. For an entity to trust another certificate, the entity must contain the root CA certificate from the CA that issued the identity certificate. Some example CAs are VeriSign, Symantec, System Manager, and Avaya's SIP Product CA.

The root CA certificate must be stored in the entity's trusted list, also known as a trust store. To change the SIP or HTTPS identity certificate of a Session Manager, each far end entity must first contain the new root CA certificate in its trusted list. *You must add the new root CA certificate to the trusted list of the far end before changing the identity certificates.*

There are two options for handling certificates for a new installation:

- Use the new System Manager issued ID certificates (default behavior). See Using the System Manager CA on page 75.
- Use third party ID certificates. See Using a Third Party CA on page 78.

Using the System Manager CA

System Manager can act as a certificate authority similar to VeriSign and Symantec. Many adopters, such as Communication Manager, Session Manager, and Presence, already use certificates issued by System Manager.

For fresh installations, all Identity Certificates, including SIP and HTTPS, are issued by the System Manager CA. You must install the System Manager's trusted root certificates on endpoints that communicate with Session Manager over TLS for the endpoints to trust the Session Manager's identity certificate.

Use this checklist for using the System Manager issued Identity Certificates.

#	Action	Link	✔
1	Export the System Manager CA.	Exporting the System Manager CA on page 75.	
2	Add the System Manager's Root Certificate to Communication Manager.	Adding the System Manager CA to Communication Manager on page 76.	
3	Add System Manager's Root Certificate to 96xx phones.	Adding the System Manager Root Certificate to 96XX phones on page 77.	
4	Add the System Manager's Root Certificate to any other SIP connections, such as CS1K and Radvision.		
5	Replace the Session Manager SIP and HTTP Identity Certificates. **Note:** This step needs to be performed for all Session Managers and Branch Session Managers.	Installing Enhanced Validation Certificates on Session Manager on page 77.	
6	Remove the SIP CA Root Certificate from all trust lists, such as Communication Manager and phones.	Other Session Managers administered under the same System Manager will already trust the new Identity Certificate.	

Exporting the System Manager CA

Procedure

1. On the home page of the System Manager Web Console, under **Services**, select **Security** > **Certificates** > **Authority**.
2. On the main page, click **Download pem file**.
3. Save the file.

Note:

To avoid HTTP download issues, save the file with the **.txt** extension.

Adding System Manager CA to Communication Manager

When you configure the Session Manager's SIP Identity Certificate to use System Manager as the CA, links to Communication Manager will go down because the Communication Manager will not trust the System Manager CA. Use this procedure to make Communication Manager trust the System Manager CA certificate.

Procedure

1. Verify you can access the System Manager CA certificate.
2. Log in to the Communication Manager server web interface.
3. Click **Administration** and select **Service (Maintenance)**.
4. In the left menu, under **Miscellaneous**, click **Download Files**.
5. Select **File(s) to download from the machine I'm using to connect to the server**.
6. Click **Browse**.
7. Select the System Manager CA certificate you want to download and click **Open**.
8. Click **Download**.
9. In the left menu, under **Security**, click **Trusted Certificates**.
10. Click **Add**.
11. Enter the name of the downloaded System Manager CA certificate.

    Note:

    You only need to enter the name of the file.
12. Click **Open**.
13. Select the Communication Manager check box.
14. Click **Add**.
15. Restart Communication Manager.

    Warning:

    Select **Delayed Shutdown** and **Restart server after shutdown**. Restarting the Communication Manager server stops the SMI server you are currently using. You will be unable to access the Web pages until the server restarts.

Adding System Manager's Root Certificate to 96xx Phones

This procedure describes how to make phones trust the System Manager CA certificate.

Important:

To avoid a service outage, run this procedure before switching Session Manager to certificates issued by System Manager.

Procedure

1. Copy the file to the file server that the 96xx phones are using.
2. On the file server, edit the file **46xxsettings.txt**.
3. In the file, set the **TRUSTCERTS** option to include the System Manager CA certificate. For example:

   ```
   SET TRUSTCERTS "smgr.txt, av_sipca_pem_2027.txt"
   ```

4. Reboot all of the phones.

   After rebooting, the phones download the System Manager root CA and are ready to the replacing of the Session Manager's SIP identity certificate.

Installing Enhanced Validation Certificates for Session Manager

By default, 96xx phones perform enhanced validation of certificates. To make use of these certificates, you need to populate the **Common Name** and **Subject Alternate Name** of the certificate. You need to perform this procedure for all Session Managers and Branch Session Managers.

Important:

The 96xx phones need to trust the System Manager Root Certificate before you replace an SIP or HTTP certificates. Failure to do so results in the loss of communication with the phones.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. Select the appropriate Session Manager from the list and click **More Actions**.
3. Select **Configure Identity Certificates** from the drop-down menu.
4. On the **Identity Certificates** page, select **Security Module SIP**, or the name associated with **Common Name** securitymodule.
5. Click **Replace**.
6. On the **Replace Identity Certificate** page, select **Replace this Certificate with Internal CA Signed Certificate**.

7. Select the **Common Name (CN)** checkbox and enter the host name or IP address of the Security Module. The address is the same as the SIP Entity address.
8. Select **RSA** for the **Key Algorithm**.
9. Select **2048** as the **Key Size**.
10. Select the **DNS Name** checkbox and enter the SIP domain (for example, avaya.com). You can enter multiple SIP domains using commas (no spaces), such as `avaya.com,company.com,xyz.com`.
11. Click **Commit**.
12. On the **Identity Certificates** page, select **Security Module HTTP**.
13. Click **Replace**.
14. On the **Replace Identity Certificate** page, select **Replace this Certificate with Internal CA Signed Certificate**.
15. Select the **Common Name (CN)** check box and enter the host name or IP address of the Security Module. The address is the same as the SIP Entity address.
16. Select **RSA** for the **Key Algorithm**.
17. Select **2048** as the **Key Size**.
18. Select the **DNS Name** checkbox and enter the SIP domain (for example, company.com). You can enter multiple SIP domains using commas (no spaces), such as `abc.com,company.com,xyz.com`.
19. Click **Commit**.
20. Restart all phones.

    After rebooting, the phones download the System Manager Root CA and will be able to communicate with the Session Manager.

Using a third party CA

The use of third party certificates is optional. Third party certificates are not required.

A third party CA can be a commercial vendor such as VeriSign and Symantec, or an enterprise-run CA that is maintained by the customer's IT department. You can create third party certificates using openssl or open source tools such as EJBCA (http://www.ejbca.org).

Use this checklist for using third party Identity Certificates.

#	Action	Link	✔
1	Add the third party Root Certificate to Communication Manager. Repeat this step for each Communication Manager that is connected to the Session Manager.	Adding a third party Root Certificate to Communication Manager on page 79.	
2	Add the third party Root Certificate CA to 96xx phones.	Adding a third party root certificate CA to 96xx phones on page 80.	
3	Add the third party Root Certificate CA to the trusted list for any other adjunct device that uses TLS to connect to Session Manager through SIP. .	For example, Avaya Voice Portal and Meeting Exchange.	
4	Replace the Session Manager SIP and HTTP Identity Certificates.	Installing third party certificates on Session Manager on page 80.	
5	Add the third party certificate to the trusted list.	Adding trusted certificates on page 81.	

Adding a third party CA to Communication Manager

Configure Communication Manager to trust a third party root CA.

When you replace the SIP CA with the third party certificate, all Communication Manager TLS connections will go down.

Perform this procedure for each Communication Manager that is connected to the Session Manager.

Procedure

1. Verify you can access the third party root CA certificate.
2. Log in to the Communication Manager server web interface.
3. Click **Administration** and select **Service (Maintenance)**.
4. In the left menu, under **Miscellaneous**, click **Download Files**.
5. Select **File(s) to download from the machine I'm using to connect to the server**.
6. Click **Browse**.
7. Select the third party CA certificate you want to download and click **Open**.
8. Click **Download**.
9. In the left menu, under **Security**, click **Trusted Certificates**.
10. Click **Add**.

11. Enter the name of the downloaded third party CA certificate.

    Note:

    You only need to enter the name of the file.

12. Click **Open**.
13. Select the Communication Manager check box.
14. Click **Add**.
15. Restart Communication Manager.

    Warning:

    Select **Delayed Shutdown** and **Restart server after shutdown**. Restarting the Communication Manager server stops the SMI server you are currently using. You will be unable to access the Web pages until the server restarts.

16. Repeat this procedure for each Communication Manager connected to the Session Manager.

Adding a third party Root Certificate to 96xx Phones

This procedure describes how to make phones trust a third party Root Certificate CA.

Important:

To avoid a service outage, perform this procedure before switching the Session Manager to certificates issued by System Manager.

Procedure

1. Copy the third party root certificate file to the file server that the 96xx phones are using.
2. On the file server, edit the file **46xxsettings.txt**.
3. In the file, set the **TRUSTCERTS** option to include the third party CA certificate. For example:

   ```
   SET TRUSTCERTS "Third_Party_CA.txt, av_sipca_pem_2027.txt"
   ```

4. Reboot all the phones.

   After rebooting, the phones download the System Manager root CA and are ready to the replacing of the Session Manager's SIP identity certificate.

Installing third party certificates on Session Manager

This procedure describes how to install a third party certificate for SIP and HTTP on Session Manager.

When the certificate changes to the third party certificate, each SIP Entity must trust the third party CA.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. Select the appropriate Session Manager from the list and click **More Actions**.
3. Select **Configure Identity Certificates** from the drop-down menu.
4. Install the SIP third party certificate:
    a. On the **Identity Certificates** page, select **Security Module SIP**, or the name associated with **Common Name** securitymodule.
    b. Click **Replace**.
    c. On the **Replace Identity Certificate** page, select **Import third party PKCS#12 file**.
    d. When prompted for **Please select a file**, browse for the third party signed certificate.
    e. Enter the password in the **Password** field.
    f. Click **Retrieve Certificate**. The certificate details section displays the details of the certificate.
    g. Click **Commit**.
5. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
6. Select the appropriate Session Manager from the list and click **More Actions**.
7. Select **Configure Identity Certificates** from the drop-down menu.
8. Install the HTTP third party certificate:
    a. On the **Identity Certificates** page, select **Security Module HTTP**.
    b. Click **Replace**.
    c. On the **Replace Identity Certificate** page, select **Import third party PKCS#12 file**.
    d. When prompted for **Please select a file**, browse for the third party signed certificate.
    e. Enter the password in the **Password** field.
    f. Click **Retrieve Certificate**. The certificate details section displays the details of the certificate.
    g. Click **Commit**.

Adding trusted certificates

You can import a trusted certificate:

- from a file.

- by copying the contents of a PEM file.
- from a list of an existing certificates.
- from a remote location using a TLS connection.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **Add**.
5. To import a certificate from a file:
    a. Select **Import from file**.
    b. Click **Browse** and locate the file.
    c. Click **Retrieve Certificate**.
    d. Click **Commit**.
6. To import a certificate in the PEM format:
    a. Select **Import as PEM Certificate**.
    b. Locate the PEM certificate.
    c. Open the certificate using Notepad.
    d. Copy the entire contents of the file. You can include the start and end tags: -----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE----.
    e. Paste the contents of the file where indicated.
    f. Click **Commit**.
7. To import certificates from existing certificates:
    a. Select **Import from existing**.
    b. Select the certificate from the Global Trusted Certificate section.
    c. Click **Commit**.
8. To import certificates using TLS:
    a. Select **Import using TLS**.
    b. Enter the IP Address of the location in the **IP Address** field.
    c. Enter the port of the location in the **Port** field.
    d. Click **Retrieve Certificate**.
    e. Click **Commit**.

Demo certificates

Previously, Session Manager was shipped with demo certificates issued by the SIP CA to simplify TLS connection setup. Demo certificates are non-unique identity certificates issued by the Avaya SIP Product Certificate Authority. Demo certificates are very insecure and do not meet current NIST standards (SHA256 and 2048 bit keys).

Starting with Session Manager 6.3.8, Session Manager no longer uses or supports default demo certificates for new installations. Fresh installations of Session Manager result in SIP and HTTP certificates signed by System Manager. In most cases, existing TLS connections will break until the System Manager CA is installed on the far end. You can reinstall the demo certificates to quickly restore a previously working environment.

For upgrades, Session Manager preserves the previous certificates. If a demo certificate was in use in the previous release, the certificate is preserved through the upgrade.

Viewing the TLS version

Determine if you are using a demo identity certificate.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. Select the Session Manager instance.
3. Click **More Actions** > **Configure Identity Certificates**.
4. Select the **securitymodule**.
5. Check the **Issuer Name**.

   If the **Issuer Name** field contains **CN=SIP Product Certificate Authority, OU=SIP Product Certificate Authority, O=Avaya Inc., C=US**, you have a demo identity certificate.

Installing demo certificates

This procedure reinstalls demo certificates to quickly restore a previously working environment.

Important:

Avaya does not recommend this option. The demo certificates are not secure. Use the System Manager certificates or third party certificates instead.

Procedure

1. Log in to the Session Manager server using the customer login.
2. Enter the command **initTM -d** or **initTM --demo** to install the demo certificates.

The command displays **Trust Management Initialization started.**, followed by a WARNING message.

3. At the **Do you want to continue? (y/n)** prompt, enter **y**.

   The script installs the demo certificates.

Trusted Certificates

Viewing trusted certificates

Before you begin

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

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **View**.

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

View Trust Certificate field descriptions

Field	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	Specifies the fingerprint that authenticates the entire certificate.
Key Fingerprint	Specifies the fingerprint that authenticates the key. The Key fingerprint applies only for CA certificate. Therefore, any element, which calculates fingerprint using the key, can use this authentication.

Button	Description
Done	Closes the page and takes you back to the Trusted Certificates page.

Adding trusted certificates

You can import a trusted certificate:

- from a file.
- by copying the contents of a PEM file.
- from a list of an existing certificates.
- from a remote location using a TLS connection.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **Add**.
5. To import a certificate from a file:
   a. Select **Import from file**.
   b. Click **Browse** and locate the file.
   c. Click **Retrieve Certificate**.
   d. Click **Commit**.
6. To import a certificate in the PEM format:
   a. Select **Import as PEM Certificate**.
   b. Locate the PEM certificate.
   c. Open the certificate using Notepad.
   d. Copy the entire contents of the file. You can include the start and end tags: -----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE----.
   e. Paste the contents of the file where indicated.
   f. Click **Commit**.
7. To import certificates from existing certificates:
   a. Select **Import from existing**.
   b. Select the certificate from the Global Trusted Certificate section.
   c. Click **Commit**.

8. To import certificates using TLS:
    a. Select **Import using TLS**.
    b. Enter the IP Address of the location in the **IP Address** field.
    c. Enter the port of the location in the **Port** field.
    d. Click **Retrieve Certificate**.
    e. Click **Commit**.

Add Trusted Certificate field descriptions

Use this page to add a trusted certificate.

Name	Description
Store Type	Specifies the type of store based on inbound and outbound connection.
Import from existing	Use this option to import a certificate from the list of existing imported certificates.
Import from file	Use this option to import a certificate from a file. The file format is `.cer` or `.crt`.
Import as PEM Certificate	Use this option to import a certificate in PEM format.
Import using TLS	Use this option to import a certificate if the element requires to contact the certificate provider to obtain the certificate.

Global Trusted Certificate:

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

Name	Description
Certificate Name	Specifies the fully qualified domain name of the certificate.
Subject Name	Specifies the fully qualified domain name of the certificate holder.
Valid To	Specifies the date until which the certificate is valid.
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 certificates based on the filter criteria.
Select: All	Select 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 from file** option.

Name/Button	Description
Please select a file	The file that contains the certificates.
Browse	Opens the choose file dialog box. Use this dialog box to 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	Specifies the details of the certificate holder.
Valid From	Specifies the date and time from when the certificate is valid.
Valid To	Specifies the date and time until when the certificate is valid.
Key Size	Specifies the size of the key in bits for encryption.
Issuer Name	Specifies the name of the issuer of the certificate.
Certificate Fingerprint	Specifies the fingerprint that authenticates the entire certificate.
Key Fingerprint	Specifies 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	Specifies whether the certificate is a CA certificate.

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

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

Removing trusted certificates

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.

2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. Select the certificates you want to remove, then click **Remove**.

   The system removes the certificates from the list of trusted certificates in the Session Manager instance.

Delete Trusted Certificate Confirmation field descriptions

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

Field	Description
Certificate Name	The common name of the certificate.
Store Type	The type of the store associated with the certificate.
Subject Name	The name of the certificate holder.

Button	Description
Delete	Deletes the trusted certificate from the corresponding store.
Cancel	Cancels the delete operation and takes you back to the Add Trusted Certificate page.

Exporting a Session Manager Certificate

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. Select the appropriate certificate to export.
5. Click **Export** .

Trusted Certificates field descriptions

Use this page to view, export, and remove the trusted certificates listed on the page. You can add more certificates in the existing list of trusted certificates.

Field	Description
Store Description	The purpose of the trusted certificate.

Table continues…

Field	Description
Store Type	The type of the store associated with the certificate.
Subject Name	The name of the certificate holder.

Button	Description
View	Opens the View Trust Certificate page. Use this page to view the certificate details.
Add	Opens the Adds Trusted Certificate page. Use this page to import certificates from the selected resource.
Remove	Removes the selected certificate from the list of trusted certificates.
Export	Exports the selected certificate from the list of trusted certificates to a PEM formatted file.

Identity Certificates

Multiple Identity Certificates exist on Session Manager. This section describes two of the Identity Certificates: **SIP** and **HTTPS (PPM)**.

SIP Identity Certificate

Generate the Session Manager SIP Identity Certificate with the following X509v3 extensions and attributes.

Attribute	Value	Required?
Authority Information Access	OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}	Optional
Authority Key Identifier	*hash*	Required[1]
CRL Distribution Points	URI:http://{crl-server}{:crl-port}{/crl-path}	Optional
	URI:ldap://{crl-server}{:crl-port}{/crl-dn}[2]	Optional

Table continues…

[1] Authority key identifiers are required elements in end entity certificates to properly establish the trust chain.
[2] URLS and DNs that identify the location of CRLs in LDAP directories can be complex. Entities must be able to handle characters as defined by the LDAP URI specification in RFC 4516.

Attribute	Value	Required?
Extended Key Usage	id-kp-serverAuth = 1.3.6.1.5.5.7.3.2.1 id-kp-clientAuth = 1.3.6.1.5.5.7.3.2.2 id-kp-sipDomain = 1.3.6.1.5.5.7.3.20	Required Optional[3] Contraindicated [4]
Key Usage	digitalSignature nonRepudiation keyEncipherment dataEncipherment	All values are Optional. [5]
Subject	CN={fqdn}	Required
Subject Alternative Name	IP:{ip} URI:sip:{domain} DNS:{domain} DNS:{fqdn}	Optional Required [6] Required [7] Required
Subject Key Identifier	*hash*	Recommended
Validity	*validity period*	Required

HTTPS Identity Certificate

Generate the Session Manager HTTPS Identity Certificate with the following X509v3 extensions and attributes.

Attribute	Value	Required?
Authority Information Access	OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}	Optional
Authority Key Identifier	*hash*	Required[8]
CRL Distribution Points	URI:http://{crl-server}{:crl-port}{/crl-path} URI:ldap://{crl-server}{:crl-port}{/crl-dn}[9]	Optional Optional
Extended Key Usage	id-kp-serverAuth = 1.3.6.1.5.5.7.3.2.1	Required

Table continues…

[3] Required if the same Identity Certificate is used when the server is acting as a client.
[4] Validation of the presence of the `id-kp-sipDomain` extended key usage as described in RFC 5924 is discouraged, as it limits use of the certificate to SIP only and forces certificate proliferation.
[5] Values may vary as specified in RFC 5280 and RFC 3279.
[6] The SIP domain may not be known at install time, so the `URI:sip:{domain}` Subject Alternative Name value suggested by RFC 5922 is not likely to be present.
[7] See Footnote 6. Also, the 96xx endpoints require the SIP domain to be present in the **CN** or as a `DNS:{domain}` entry in the Subject Alternative Name field.
[8] Authority key identifiers are required elements in end entity certificates to properly establish the trust chain.
[9] URLS and DNs that identify the location of CRLs in LDAP directories can be complex. Entities must be able to handle characters as defined by the LDAP URI specification in RFC 4516.

Attribute	Value	Required?
	id-kp-clientAuth = 1.3.6.1.5.5.7.3.2.2	Optional[10]
Key Usage	digitalSignature nonRepudiation keyEncipherment dataEncipherment	All values are Optional. [11]
Subject	CN={fqdn}	Required
Subject Alternative Name	IP:{ip} DNS:{fqdn}	Optional [12] Required
Subject Key Identifier	*hash*	Recommended
Validity	*validity period*	Required

Identity Certificates field descriptions

Field	Description
Service Name	The name of the service that uses the identity certificate.
Common Name	The common name to identify the service.
Valid To	The date until which the certificate is valid.
Expired	Specifies whether the certificate is expired.
Service Description	A brief description about the service.

Button	Description
Replace	Opens the Replace Identity Certificate page. Use this page to replace a selected identity certificate with a new certificate.
Export	Exports the certificate that you select. The exported certificate is in the form of a PEM file.
Renew	Renews the certificate that you select. After you renew a certificate, the system automatically updates the **Valid To** column.

[10] Required if the same Identity Certificate is used when the server is acting as a client.
[11] Values may vary as specified in RFC 5280 and RFC 3279.
[12] For the 96xx endpoints, PPM is defined as an IP address so PPM certificates must contain the `IP:{ip}` Subject Alternative Name entry when these endpoints are part of the solution.

Viewing Identity Certificates

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Identity Certificates**.
4. Click **View**.

Replacing a Session Manager Identity Certificate

Use this procedure to replace the Identity Certificate of a Session Manager.

Before you begin

Ensure that you have the following:

- A certificate with the hostname as the Common Name (CN) that is signed by the third party certificate authority (CA). This certificate must be in PKCS#12 format.
- The third-party Root CA certificate.

Procedure

1. Add Root CA to the System Manager Trusted List. See Adding Root CA to the System Manager Trusted List on page 94.
2. Add Root CA to the Session Manager Trusted List. See Adding Root CA to the Session Manager Trusted List on page 94.
3. Administer the SIP Identity Certificate. See Administering a SIP Identity Certificate on page 95.
4. Activate the new Identity Certificate. See Activating a new Identity Certificate on page 96.

Replace Identity Certificate field descriptions

Certificate Details section

Field	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 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 issuer of the certificate.

Table continues…

Field	Description
Certificate Fingerprint	The fingerprint that authenticates the certificate.
Subject Alternative Name	An alternate name for the certificate holder.

Field	Description
Replace this Certificate with Internal CA Signed Certificate	The option to replace the current certificate with the internal CA signed certificate.
Import third party certificate	The option to replace the identity certificate with the PKCS #12 file that you imported from a third-party source.

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

Field	Description
Common Name (CN)	The common name of the certificate holder. You must select the check box to enter the name.
Key Algorithm	The algorithm used to generate the key for the certificate. The available option is RSA. System Manager uses the SHA2 algorithm for generating certificates.
Key Size	The size of the key in bits or bytes for encryption. The available values are: • 1028 • 2048 Use 2048 as the key size.
Subject Alternative Name	An alternate name for the certificate holder. The following fields are available: • **DNS Name**: DNS IP address. • **IP Address**: IP address. • **URI**: URI address. **Note:** You must select the check boxes to enter the values. In all three fields, you can enter more than one values separated by a comma.

The page displays the following fields when you select the **Import third party certificate** option.

Field	Description
Please select a file (PKCS #12 format)	The full path of the PKCS #12 file where you saved the certificate.
Password	The password that is used to retrieve the certificate.

Button	Description
Retrieve Certificate	Retrieves the details of the imported certificate and displays in the **Certificate Details** section.
Commit	Replaces the current identity certificate with the selected certificate.
Cancel	Cancels the certificate replacement operation.

Adding Root CA to the System Manager Trusted List

About this task

System Manager must trust the third-party certificate that the Session Manager uses.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select **System Manager**.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. Click **Add**.
5. On the Add Trusted Certificate page, select **Select Store Type to add trust certificate as All**.
6. If the Root CA is in PKCS#12 format:
   a. Select **Import from file**.
   b. Browse for the Root CA certificate using **Please select a file**.
   c. Click **Retrieve Certificate**.
7. If the Root CA is in PEM format, select **Import as PEM Certificate**.
8. Copy and paste the Root CA certificate contents in the space provided.
9. Click **Commit**.

Adding Root CA to the Session Manager Trusted List

For internal communications, Session Manager must trust the third party certificate.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select **Session Manager**.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificate page, click **Add**.
5. On the Add Trusted Certificate page, select **Select Store Type to add trust certificate as All**.
6. If the Root CA is in PKCS#12 format:
   a. Select **Import from file**.
   b. Browse for the Root CA certificate using **Please select a file**.
   c. Click **Retrieve Certificate**.
7. If the Root CA is in PEM format, select **Import as PEM Certificate**.
8. Copy and paste the Root CA certificate contents in the space provided.
9. Click **Commit**.

Administering a SIP Identity Certificate

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Identity Certificates**.
4. Select **securitymodule**.
5. Click **Replace**.
6. Choose one of the following options:
   - If you are replacing the Identity Certificate with an Internal CA Signed Certificate:
     a. Click **Replace this Certificate with Internal CA Signed Certificate**.
     b. Enter the common name, org unit, organization, and country information in the respective fields.
     c. Select the key size/type.
     d. Click **Commit**.
   - If you are replacing the Identity Certificate by importing a third party PCKS # 12 file:
     a. Click **Import third party PCKS # 12 file**.
     b. Enter the file name in the **Please select a file** field.

c. Enter the password in the **Password** field.

d. Click **Retrieve Certificate**.

e. Click **Commit** to replace the certificate with the imported third-party certificate.

Restoring the default SIP Identity Certificate

Restore the default certificate issued by the SIP CA on the selected Session Manager. You can reinstall demo certificates to quickly restore a previously working environment.

Important:

Starting with Session Manager 6.3.8, the "demo" certificates are no longer installed by default. A fresh installation of Session Manager will result in SIP and HTTP certificates signed by System Manager. In most cases, existing TLS connections will break until the System Manager CA is installed on the far end

Procedure

1. Log into the Session Manager CLI.
2. Enter the command **initTM --demo**
3. At the warning message prompt, enter **y**.

   The message **Trust Management initialization completed successfully.** appears when the default certificate has installed.

Activating a new Identity Certificate

To activate a new Identity Certificate, you reboot the Session Manager and restart the jboss service on System Manager.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. Select a Session Manager instance.
3. Select **Shutdown System** > **Reboot**.
4. Click **Confirm**.
5. Login to the System Manager command line interface.
6. Enter the command **service jboss restart**.

Chapter 6: Managing users

This chapter explains Session Manager user administration.

System Manager provides bulk importing of user profiles and user attributes. For more information, see Bulk import and export on page 153.

For information on the Multi Tenancy feature, see *Administering Avaya Aura® System Manager*.

Note:

While administering a user, the secondary Session Manager should not be hosted on the VMware platform unless the primary Session Manager has been hosted on the VMware platform.

Before administering a Session Manager profile

Perform the following steps before administering a Session Manager profile.

Important:

Verify the sequence of the primary Session Manager and the secondary Session Manager, as specified in the following configurations, is identical to the sequence of the primary Session Manager and the secondary Session Manager in the Session Manager communication profile:

1. In the phone settings file.
2. In the Communication Manager Route Pattern administration. The first trunk choice or signaling Group in the route pattern (Far-End Node Name) must be the primary Session Manager, and the second choice is the secondary Session Manager.
3. On the user endpoint under SIP proxy settings.

If the sequence of the primary Session Manager and the secondary Session Manager is not identical to the sequence of the primary Session Manager and the secondary Session Manager in the Session Manager profile, errors such as, Message Waiting Indicator errors and Presence errors can occur.

Procedure

1. Administer the primary Session Manager by adding a SIP entity of type *Session Manager* with listen ports. See:
   - Creating SIP Entities on page 298.
   - Adding a SIP entity as Session Manager Instance on page 364.
2. (Optional step required for redundancy purposes.) Administer the secondary Session Manager by adding a SIP entity of type *Session Manager* with listen ports. See:
   - Creating SIP Entities on page 298.
   - Adding a SIP entity as Session Manager Instance on page 364.
3. Add SIP domains. Administer the SIP domain using the Routing application. See Creating domains on page 255.
4. Administer applications to be added in the Origination and Termination application sequences:
   a. Administer Communication Manager as a Feature Server.
      - Add the Communication Manager Feature Server SIP entity. See Creating SIP Entities on page 298.
      - Administer the Communication Manager Feature Server as an application instance. See Creating a new element on page 58.
      - Add the Communication Manager Feature Server as an application. See Creating an application on page 476.

   b. Repeat the above step to add other applications in the Application Sequence.
5. Create an Application Sequence from existing applications to specify the Origination Application Sequence and Termination Application Sequence. See Creating an Application Sequence on page 480.
6. If you have conference products that support the Conference Factory feature, add Conference Factory Sets. See Adding a new Conference Factory Set and setting the respective parameters on page 488.
7. To use a Branch Session Manager as a Survivability Server, add SIP entities of type **Session Manager** and **Branch Session Manager** with listen ports. See:
   - Creating SIP Entities on page 298.
   - Adding a SIP entity as a Branch Session Manager instance on page 394.
8. To modify the Home Location, configure values that are similar to Locations. To add a new value, add a Location. See Creating Locations on page 260.

   Note:

   The Home Location needs to be specified to support mobility for a user. Session Manager profiles must be defined only for SIP endpoints. Assign SIP handles to all endpoints registered with Communication Manager.

9. Synchronize Communication Manager station data and messaging data with the System Manager:
    a. Administer each Communication Manager and Messaging application as an application instance. See:
        - Creating a new element on page 58.
        - Creating a Messaging instance on page 62.
    b. Synchronize Communication Manager and messaging data with the System Manager. See:
        - Synchronizing data and configuring options on page 63.
        - Synchronizing the messaging data on page 64.

Adding users

Use this procedure to add users in Session Manager. There are a number of input fields that are not necessary for Session Manager user administration. You can ignore any input fields that are not mentioned in the steps.

Important:

When you register a SIP endpoint of a user to the Avaya core, you must assign a communication profile to the user. The communication profile contains a Communication Manager endpoint profile and a Session Manager profile. The Communication Manager profile associates the user with a station on a Communication Manager that is in the Avaya core network. The Session Manager profile assigns the primary Session Manager and the secondary Session Manager, relevant application sequences, and the survivability server. For correct application sequencing to Communication Manager, each application in the application sequence must reference the same Communication Manager as the Communication Manager endpoint profile. For correct survivability configuration, if a Branch Session Manager is specified as the survivability server, the Branch Session Manager must also reference the same Communication Manager as the Communication Manager endpoint profile.

A user can have more than one Communication Profile.

For details on other sections of the User Management page, see the System Manager online help.

Procedure

1. On the home page of the System Manager Web Console, under **Users**, click **User Management** > **Manage Users**.
2. On the User Management page, click **New**.
3. On the New User Profile page, under the **Identity** tab:
    a. **(Optional)** In the Organization section, select a tenant from the Tenant field. You must select a tenant only if the user must belong to a tenant.

b. **(Optional)** In the User Provisioning Rule field, select a user provisioning rule.

You can select only one user provisioning rule.

Important:

When you create a user with a user provisioning rule, the system populates the values for user attributes from the user provisioning rule. Do not modify the populated values.

For assigning user provisioning rules, see User provisioning rule on page 131.

4. Enter the last name and the first name of the user.
5. **(Optional)** In the **Description** field, enter a description of the user.
6. In the **Login Name** field, enter a name for the login of the user.

   The login name is unique. System Manager converts the name to the SIP username format. For example, username@domain.
7. In the **Authentication Type** field, select Basic from the drop-down menu.
8. In the **Localized Display Name** field, enter the localized display name of the user. System Manager displays the name as the calling party name.
9. In the **Endpoint Display Name** field, enter the name of the user.
10. Click the **Communication Profile** tab.
11. In the **Communication Password** field, enter a password for the user. The user must enter this password to log in to the endpoint.
12. For each SIP handle:

    Note:

    When you add a non-SIP endpoint user, for example, an H.323 endpoint user or a DCP endpoint user, ensure that the communication address of the user conforms to the Avaya E.164 type.

    a. In the **Communication Address** section, click **New**.
    b. In the **Type** field, select `Avaya SIP` from the drop-down menu.
    c. In the **Fully Qualified Address** field, enter the extension number.
    d. Click **Add**.
13. In the **Session Manager Profile** section:
    a. Select the **Session Manager Profile** check box.
    b. In the **Primary Session Manager** field, select the appropriate primary Session Manager instance from the drop-down menu.
    c. **(Optional)** In the **Secondary Session Manager** field, select the appropriate secondary Session Manager instance from the drop-down menu for redundancy.
    d. **(Optional)** In the **Survivability Server** field, specify a survivability server. For example, Branch Session Manager. This step is required only for survivability.

e. In the **Max. Simultaneous Devices** field, select the appropriate value from the drop-down menu.

f. **(Optional)** Select the checkbox for **Block New Registration When Maximum Registrations Active?**.

g. In the **Origination Sequence** field, select the origination application sequence from the drop-down menu.

h. In the **Termination Sequence** field, select the termination application sequence from the drop-down menu.

i. In the **Home Location** field, enter the location. This field is mandatory for mobile users. You can administer locations using **Routing** > **Locations**.

j. In the **Conference Factory Set** field, select the Conference Factory Set from the drop-down menu.

k. **(Optional)** Select the checkbox for **Enable Centralized Call History**.

Important:

Ensure that the sequence of the primary Session Manager and the secondary Session Manager in the following administration steps is identical to the sequence of the primary Session Manager and the secondary Session Manager in the Session Manager profile.

a. In the phone settings file.

b. In the Communication Manager Route Pattern administration. The first choice trunk or signaling Group in the route pattern – the Far-End Node Name must be the primary Session Manager and the second choice is the secondary Session Manager.

c. On the User endpoint in SIP Proxy settings,

If the sequence of the primary Session Manager and the secondary Session Manager is not identical to the sequence of the primary Session Manager and the secondary Session Manager in the Session Manager profile, users may face errors, such as, Message Waiting Indicator errors and Presence errors.

14. Assign the user to a Communication Manager station:

Note:

You can assign a user to a Communication Manager station only after the data synchronization is complete. To view the synchronization status, on the System Manager console, click **Communication System Management** > **Telephony**. The system displays the status in the **Sync Status** column.

a. Select the **CM Endpoint Profile** checkbox.

b. From the **System** drop-down menu, select `Communication Manager`.

c. If the station already exists on the Communication Manager that is associated with the user, select the **Use Existing Endpoints** check box.

You must select this checkbox to associate the user with the selected Communication Manager station settings. Deselect the checkbox for the system to create a station automatically .

d. In the **Extension** field, enter the extension that is administered on Communication Manager for the existing or new station . Click **Endpoint Editor** to modify the Communication Manager station data.

e. In the **Template** field, if the user is not associated with an existing Communication Manager station, select a phone template for the station of the user.

f. In the **Port** field, enter the port that is associated with the extension.

g. **(Optional)** Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** box. This step applies only if you want to delete the station when you delete the user.

15. Click **Commit**.

Note:

When you administer a user with a **Survivability Server**, the system verifies that valid SIP Entity links exist between the Branch Session Manager and the administered Primary and Secondary Session Managers.

Related Links

New User Profile field descriptions on page 198

Managing communication profiles

Session Manager communication profile administration

You can use the Session Manager profile subsection of the Communication Profile section to 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 Aura network.

All Communication Addresses (handles) of type SIP for the Communication Profile are associated with the 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 not available.

You might configure the system to invoke Application Sequences when routing calls from (origination application sequence) or to (termination application sequence) the currently displayed user.

You can specify a Conference Factory Set for users for experiencing improved voice, video and text conferencing.

For local survivability, you can specify a Survivability Server to provide survivability communication services for devices associated with a Communication Profile that is used when local connectivity to Session Manager instances in the Aura Core is lost. If you select a Branch Session Manager, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application will continue 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 not assigned to a location.

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 about Multi Device Access, 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. However, if the endpoint with the oldest registration is active on a call then the system does not unregister the endpoint until the call completes.
- Selected, the system denies any new registrations and sends the 403 Forbidden response with an appropriate warning header to the registering device.

The system forks incoming INVITE requests (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 forks an incoming CANCEL request to all the registered devices if the caller hangs up before the call is answered.

Communication profiles

Using the Users feature, you can provide communication profiles to associate elements with users. Communication Profiles supports communication interactions established through Avaya Communication Services. Communication Profiles can be CM Endpoint, Messaging, Session Manager, CS 1000, CallPilot Messaging, IP Office, Presence, Collaboration Environment, or Conferencing profile.

You can provide communication profiles in User Management through Communication Profile Extension Pack (EP). You can use a communication profile to represent a subscription of the user to a communication subsystem and the specific configuration needs for the user. A communication subsystem is a service or infrastructure that manages the establishment and controls or routes the communication interactions.

Adding a communication profile for the user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a new user account, click **New**.
   - To add a communication profile to an existing user, select the user and click **Edit**.
4. On the New User Profile or the User Profile Edit page, click the **Communication Profile** tab.
5. In the communication profile section, click **New**.
6. In the **Name** field, enter the name of the new communication profile.
7. To mark the profile as default, select the **Default** check box.
8. Click **Done**.
9. Click **Commit**.

Deleting the communication profile of a user

About this task

You cannot delete default communication profiles.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - Select a user and click **Edit**.
   - Select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **Communication Profile** section, click a profile.
6. Click **Delete**.
7. Click **Commit**.

Result

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

Creating a new communication address for a communication profile

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a new user account, click **New**.
   - To add a communication profile address to an existing user, select the user and click **Edit**.
4. On the New User Profile or the User Profile Edit page, click the **Communication Profile** tab.
5. In the Communication Profile section, click a communication profile.
6. In the Communication Address section, click **New**.
7. In the **Type** field, enter a communication protocol.
8. In the **Fully Qualified Address** field, enter a contact address in the format supported by the value that you selected in the **Type** field. A contact address can be an e-mail ID, instant messenger ID, or the SIP address of a SIP-enabled device.
9. Enter the domain name from the field next to **Fully Qualified Address** field.
10. Click **Add**.
11. Click **Commit**.

Modifying the communication address

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - Select a user and click **Edit**.
   - Select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **Communication Profile** section, select a profile.
6. In the **Communication Address** section, select a communication address.
7. Click **Edit**.
8. Modify the information in the respective fields.
9. Click **Add**.

10. Click **Commit**.

Deleting a communication address from a communication profile

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following:
   - Select a user and click **Edit**.
   - Select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Communication Profile section, click a communication profile.
6. In the Communication Address section, select a communication address from the table.
7. Click **Delete**.
8. Click **Commit**.

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.

CM Endpoint profile administration

CM Endpoint and Messaging profiles of a user

With User Profile Management, you can create the following types of communication profiles for a user:

- CM Endpoint Profile, to create an association between an endpoint and a user
- Messaging Profile, to create an association between a subscriber mailbox and a user

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

Login name of endpoint or messaging profile

The login name in the Identity section on the New User Profile and Edit User Profile pages is the user name that is associated with the communication profile, CM Endpoint and Messaging. This user name appears in the User column in the Endpoint List or Subscriber List.

For endpoints, the **Localized Display Name** and **Endpoint Display Name** fields in the Identity section of the User Profile Management user profile map to the **Name** and **Localized Display Name** fields of CM Endpoint. The **Localized Display Name** and **Endpoint Display Name** fields are optional. They default to the **Last Name** and **First Name** as given in the General section of the User Profile Management user profile. You can also fill in any other name of your choice.

For Subscribers, the **Last Name** and **First Name** fields in the General section of User Profile Management user profile directly map to the **Last Name** and **First Name** fields in Subscriber. The **Localized Display Name** and **Endpoint Display Name** fields are not applicable for Subscribers.

Creating CM Endpoint and Messaging profiles

You can create one default or primary Communication Profile for a user. To this default profile, you can add one CM Endpoint and one Messaging profile. In addition, you can add two more CM Endpoint profiles. You can add a maximum of three CM Endpoint profiles and one Messaging profile per user.

Adding a CM Endpoint profile for a user

Before you begin

Add Communication Manager by using Manage Elements or Discovery from **Inventory**.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - If you are creating a CM Endpoint profile for a new user profile, click **New**.
   - If you are creating a CM Endpoint profile for an existing user, select the user and click **Edit**.

4. Click the **Communication Profile** tab.
5. In the CM Endpoint Profile section, select the check box next to the **CM Endpoint Profile** label.
6. In the CM Endpoint Profile section, enter the relevant information.

   Note:

   To delete the endpoint from the communication management device after removing the association between the endpoint and the user, select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box.
7. Perform one of the following:
   - To save the changes, click **Commit**.
   - To save the changes and stay on the same page, click **Commit & Continue**.

   From User Management, you can create or add endpoints. After you select the Communication Manager in which you want to add an endpoint, the system allows you to complete the fields for creating a new endpoint.

   The **Preferred Handle** field specifies numeric only handles, SIP or non SIP, that are administered for a user. If the SIP entity is of Communication Manager type, Session Manager uses the **Preferred Handle** field in the CM Endpoint profile. By default, for a SIP station, Communication Manager uses the extension number as the phone number entry on an OPS station-mapping table. If your enterprise dial plan has SIP handles that are different from the Communication Manager extension, then use the **Preferred Handle** field to change the phone number entry on the OPS station-mapping table on the Communication Manager.

   To modify the phone number entry, the Communication Address in System Manager should have a SIP handle. In the CM Endpoint Communication Profile, set the **Preferred Handle** field to the SIP handle format. After you click **Commit**, System Manager sets the **Phone Number** field in the OPS station-mapping table on Communication Manager to the SIP handle format. If you do not need this feature then set the **Preferred Handle** value to **None**.

Viewing a station profile of a user

Procedure

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

Modifying a CM Endpoint profile of a user

Procedure

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

3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the CM Endpoint Profile section, modify the relevant information in the fields.
6. To save the changes to the database, click **Commit**.

   To cancel the action and return to the previous page, click **Cancel**.

Removing association between an CM Endpoint and a user

Before you begin

Ensure that you have not selected the **Delete Endpoint on Unassign of Endpoint from User or Delete User** check box while associating a station with a user.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **CM Endpoint Profile** section, clear the check box next to the **CM Endpoint Profile** label.
6. Click **Commit**.

Result

The system removes the association between the endpoint and the user. The endpoint is still provisioned on the communication management device.

Deleting a CM Endpoint profile of a user

Before you begin

Select the **Delete Endpoint on Unassign of Endpoint from User or Delete User** check box while associating a endpoint to a user.

About this task

The delete functionality removes the association between the endpoint and the user, and deletes the endpoint from the communication management device.

Procedure

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

3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **CM Endpoint Profile** section, clear the check box next to the **CM Endpoint Profile** label.
6. Click **Commit**.

Note:

You can delete only those endpoints that are associated with a user through User Management. You can delete nonuser associated endpoints through Endpoint management.

Messaging profile administration

Adding a messaging profile for a user

Procedure

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

Note:

To delete the subscriber mailbox from the communication management device after removing the association between the subscriber and the user, select the **Delete Messaging on Unassign of Subscriber from User or Delete User** check box.

7. Click **Commit** or **Commit & Continue** to add the messaging profile, or click **Cancel** to return to return to the previous page.

   The field names that are marked with an asterisk (*) are mandatory fields. You must enter valid information in these fields to create the CM Endpoint profile.

Note:

You must add the messaging devices through Runtime Topology System (RTS) before you add a messaging profile for a user. After you create the user-subscriber association, the user name appears in the **User** column in the subscriber list.

Modifying a messaging profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Messaging Profile section, modify the relevant information in the fields.
6. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Viewing a messaging profile of a user

Procedure

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

Result

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

Removing association between a subscriber mailbox and a user

Before you begin

The **Delete Subscriber on Unassign of Subscriber from User or Delete User** check box is clear while associating a mailbox with a user.

Procedure

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

3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Messaging Profile tab, clear the check box next to the **Messaging Profile** label.
6. Click **Commit**.

Result

The system removes the association between the subscriber mailbox and the user. The subscriber mailbox is still provisioned on the communication management device.

Deleting a subscriber mailbox

Before you begin

You have selected the **Delete Subscriber on Unassign of Subscriber from User or on Delete User** check box while associating a subscriber mailbox to a user.

About this task

This functionality deletes the subscriber mailbox from the messaging device after removing the association between the subscriber mailbox and the user.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Messaging Profile section, clear the check box next to the **Messaging Profile** label.
6. Click **Commit**.

Note:

You can delete only those subscribers that are associated with a user through User Management. You can delete non-user associated subscriber mailboxes only through Subscriber Management.

CS 1000 and CallPilot profile administration

CS 1000 and CallPilot profile administration

With User Management, you can create the following types of communication profiles for a user:

- CS 1000 Endpoint Profile. To create an association between an endpoint and a user.
- CallPilot Messaging Profile. To create an association between a subscriber mailbox and a user.

Note:

You cannot assign the mailbox number in the CallPilot communication profile by using the user provisioning rule. You must add the mailbox number for the CallPilot communication profile.

To modify an endpoint or subscriber field that is not available through User Management, navigate to the Endpoint or Subscriber Management pages and modify the information. For information, see Redirecting the CS 1000 or CallPilot user to Element Manager.

Redirecting the CS 1000 or CallPilot user to Element Manager

Before you begin

A user must exist with at least one communication profile. To create a user, navigate to **User Management** > **New**.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. Select **CS 1000 Endpoint Profile** or **CallPilot Messaging Profile** that you must update and click **Update**.

   The system opens the user profile in the element manager that you select.

   Note:

   The system discards all unsaved changes that you make to the current user including the changes to communication profiles.
6. Enter the relevant information and click **Save**.

   The system displays the User Management page.

Adding a CallPilot profile for a user

Before you begin

A user must exist. To create a user, navigate to **User Management** > **New**.

About this task

For a communication profile, you can provide a maximum of one CallPilot mailbox. To add additional mailboxes for a user, you must add another communication profile.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a profile for a new user, click **New**.
   - To create a profile for an existing user, select the user and click **Edit**.
4. On the New User Profile page, click the **Communication Profile** tab.
5. In the CallPilot Messaging Profile section, select the check box and complete the following fields:
   - In the **System** field, select a CallPilot system. The system displays a list of systems that are registered with the element registry.
   - In the **Target** field, select the location of CallPilot, if provisioned.
   - In the **Template** field, select a template that CallPilot Element Manager provisions.
   - In the **Mailbox Number** field, enter a mailbox number for CallPilot.

     Note:

     You must enter the mailbox number even if the value is same as Primary DN.
6. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Adding a CS 1000 profile for a user

Before you begin

A user must exist. To create a new user, navigate to **User Management** > **New**.

About this task

For a communication profile, you can provide a maximum of one CS 1000 phone. To add additional phones for a user, you must add another communication profile.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a profile for a new user profile, click **New**.
   - To create a profile for an existing user, select the user and click **Edit**.
4. On the New User Profile page, click the **Communication Profile** tab.
5. In the **CS1000 Endpoint Profile** section, select the check box and complete the following fields:
   a. In the **System** field, select a CS 1000 system.

      The system displays a list of systems that are registered with the element registry.

   b. Perform one of the following:
      - Click **Add new** and complete the following fields:
        a. In the **Target** field, select a CS 1000 customer number.
        b. In the **Template** field, select a template that CS 1000 Element Manager provides.
        c. In the **Primary DN** field, enter a preferred primary DN.

           Note:

           If you do not provide a primary DN, CS 1000 Element Manager automatically assigns a primary DN.

        d. In the **Terminal Number** field, enter a preferred TN.
      - Click **Link existing**, and in the **Existing TN** field, enter the terminal number from the list of existing numbers.

   c. Clear the **Include in Corporate Directory** check box to exclude the profile in the CS 1000 corporate directory.

   d. **(Optional)** Select **Delete Endpoint on Unassign of Endpoint from User** if you must delete the endpoint from CS 1000 when you remove the association between the endpoint and the user.
6. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Modifying a CS 1000 or CallPilot user profile

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the CS 1000 Endpoint Profile or CallPilot Messaging Profile section, enter the relevant information in the fields.
6. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Changing passwords of CS 1000 Presence users

Procedure

1. To log on to the System Manager personal agent console, enter `http://<SMGR server-name>/pa`.
2. Click **Change Password**.
3. Enter the old and new passwords, and then click **Save**.

   Presence Services recognizes the password change.

   Note:

   The system needs a synchronized password that is the same password as the password that Presence Services uses to update CS 1000.

IP Office profile administration

Adding an IP Office endpoint profile on a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a profile for a new user, click **New**.

- To create a profile for an existing user, select the user and click **Edit**.

4. On the New User Profile page, click the **Communication Profile** tab.
5. Select the **IP Office Endpoint Profile** check box.
6. Complete the **IP Office Endpoint Profile** section.
7. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Note:

To assign an extension to the user, perform one of the following actions:

- Assign an available extension to the user, select the **Use Existing Extension** check box, and select an unassigned extension from the drop-down box.
- Or assign an available module-port to the user from the **Module-Port** drop-down box, and type the new extension. The module-port combination is valid only when you associate a digital or an analog extension type to the user.

To assign an extension to a user with other set types, perform one of the following actions:

- Type an appropriate extension.
- Select the **Use Existing Extension** check box to choose an existing extension.
- Select an unassigned extension from the drop-down field.

Viewing an IP Office endpoint profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select the user whose profile you want to view.
4. Click **View**.
5. Click the **Communication Profile** tab.

   Click the **IP Office Endpoint** section to view the IP Office endpoint profile of the user you selected.

Modifying an IP Office endpoint profile of a user

Procedure

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

3. On the User Management page, select the user whose profile you want to edit.
4. Click **Edit**.
5. Select the **Communication Profile** tab.
6. Edit the required fields in the **IP Office Endpoint Profile** section.
7. Perform one of the following:
   - To save the changes to the database, click **Commit**.
   - To save the changes to the database and remain on the same page, click **Commit & Continue**.
   - To cancel the action and return to the previous page, click **Cancel**.

Note:

To assign an extension to the user, perform one of the following actions:

- Assign an available extension to the user, select the **Use Existing Extension** check box, and select an unassigned extension from the drop-down box.
- Or assign an available module-port to the user from the **Module-Port** drop-down box, and type the new extension. The module-port combination is valid only when you associate a digital or an analog extension type to the user.

To assign an extension to a user with other set types, perform one of the following actions:

- Type an appropriate extension.
- Select the **Use Existing Extension** check box to choose an existing extension.
- Select an unassigned extension from the drop-down field.

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

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user, and perform one of the following:
   - 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**.

Viewing details of a user

Before you begin

You require appropriate permissions.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user.
4. To view details of the selected user account, click **View**.

Note:

You can only view details of one user account at a time.

Related Links

User Profile View field descriptions on page 232

Modifying user accounts

Before you begin

- You require permissions to modify the user details. If you select a user that does not have the permission to modify the details, the system does not display the **Edit** button.
- The role must have the following permissions assigned:

  For resource type elements, all permissions in the **Role Resource Type Actions** section.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user.

Note:

At one time, you can edit only one user account.

4. To edit a user account, perform one of the following:
   - Click **Edit**.
   - Click **View** > **Edit**.
5. On the User Profile Edit page, perform the following:
   a. **(Optional)** In the **Organization** section, select a tenant from the **Tenant** field.

   You must select a tenant only if the user must belong to a tenant.

b. **(Optional)** In the **User Provisioning Rule** field, select a user provisioning rule.

You can provide only one user provisioning rule.

Note:

When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

c. Enter the required information in the remaining fields.

For information, see User Profile Edit field descriptions.

- You cannot edit the tenant. If you select a different level 1 for the tenant from the organization hierarchy, the **Level 2** and **Level 3** fields become blank. You can select new values for level 2 and level 3. If you select a different level 2 for the tenant from the organization hierarchy, the **Level 3** field becomes blank. You can select a new value for level 3.
- If you must change the tenant, delete the user and associate the user with the tenant.
- System Manager does not automatically modify the user if the user provisioning rule changes.
- You can select a different user provisioning rule when you modify the user information.

Note:

You can associate the user to an existing tenant.

6. Perform one of the following:
   - To save the changes, click **Commit**.
   - To save the changes and stay on the same page, click **Commit & Continue**.

Related Links

User Profile Edit field descriptions on page 216

Removing user accounts

About this task

When you remove a user, the system marks the user as deleted and saves the user in a list of deleted users. The system removes the roles associated with the user. However, the contacts, addresses, and communication profiles of the user still exist in the database. You can permanently remove the deleted users from the database.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select one or more users from the table, and click **Delete**.

4. On the User Delete Confirmation page, click **Delete**.

   Note:

   You cannot delete users:

   - With the login name *admin* from the User Management page.
   - Synchronized from LDAP.

Removing the deleted users from the database

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

Before you begin

Permission to delete the selected user.

Procedure

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

Viewing the deleted users

When you remove a user from the User Management page using the **Delete** option, the system removes the user temporarily and stores the user in the **Deleted Users** table. To view the temporarily deleted users, use the **Show Deleted Users** option.

Procedure

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

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

Restoring a deleted user

You can use this functionality to restore a user that you deleted using the **Delete** option on the User Management page.

Before you begin

You require permission to restore the selected user that is already deleted.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **More Actions** > **Show Deleted Users**.
4. On the Deleted Users page, select the user you want to restore, and click **Restore**.
5. On the User Restore Confirmation page, click **Restore**.
6. Click **Commit**.

Note:

For a restored user, if you assign a role other than End-User, the system prompts for a password.

Creating duplicate users

You can duplicate the user details to create a new user account by copying information from an existing user account. Using the Duplicate feature, you cannot copy the confidential information, such as addresses, private contacts and associated contacts in the contact list, password, and login name of the user.

Using the Duplicate feature, you can also copy the communication profiles like CM Endpoint and Session Manager. However, you cannot copy CS 1000 Endpoint Profile or CallPilot Messaging Profile communication. You must add the CS 1000 Endpoint Profile or CallPilot Messaging Profile communication profile after you create a duplicate user.

Before you begin

You require permission to copy the user details.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select the user account that you must duplicate.
4. Click **Duplicate**.

5. On the User Profile Duplicate page, enter the appropriate information.
6. Perform one of the following:
   - To save the changes, click **Commit**.
   - To save the changes and stay on the same page, click **Commit & Continue**.

Managing default contact list of the user

Adding a contact in the Default Contact list

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following:
   - To add a contact for a new user, click **New**.
   - To add a contact for an existing user, select a user and click **Edit**.
4. Click the **Contacts** tab.
5. In the **Default Contact List** section, enter a brief description of the contact list in the **Description** field.
6. In the **Associated Contacts** section, click **Add**.
7. On the Attach Contacts page, select one or more contacts and click **Select**.

   Note:

   In the Multi Tenancy environment, when the tenant administrator of a tenant creates or updates the user, the administrator can attach only the following contacts:

   - Private contacts of the user
   - Public contacts
   - Users who belong to that tenant

   The system displays the new contacts in the table in the **Associated Contacts** section.

Modifying membership details of a contact in a contact list

About this task

Use this feature to set the speed dial and presence buddy information for the contacts in the Default Contact list.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the **Associated Contacts** section, select a contact and click **Edit**.
6. On the Edit Contact List Member page, in the **Contact Membership Details** section, change the required information in the fields.

   You can only change the information in the fields displayed in the **Contact Membership Details** section.
7. Click **Add**.
8. Click **Commit** to save the changes.

Viewing membership details of a contact in the contact list

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.
4. On the User Profile View page, click the **Contacts** tab.
5. In the Associated Contacts section, click the last name link under the **Last Name** column.

Result

The View Contact List Member page displays the details of the selected contact.

Deleting contacts from the default contact list

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. Select one or more contacts from the Associated Contacts section and click **Remove**.

Attach Contacts field descriptions

In the Multi Tenancy environment, when the tenant administrator of a tenant creates or updates the user, the administrator can attach only the following contacts:

- Private contacts of the user
- Public contacts
- Users who belong to that tenant

Field	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Scope	The categorization of the contact based on whether the contact is a user, public, or private contact.
Display/Login Name	The unique login name or display name of the contact.
Contact Address	The address of a private or public contact. No contact address is associated with a contact type user.
User Handles	The communication handles associated with the user. These handles are defined in the communication profile of a user.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays fields under selected columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.
Advanced Search	Displays fields that you can use to specify the search criteria to search for contacts.

Button	Description
Select	Adds the selected contact in the list of associated contacts.
Cancel	Cancels your selection and takes you to the Contacts tab.

The page displays the following fields when you click **Advanced Search** at the upper-right corner of the contact table.

Field	Description
Search On	The search options that must base on the **Contact** or **User**.

Table continues…

Field	Description
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.
-	Clears the last search criteria. This button is applicable only if there is more than one search criteria.

Edit Contact List Member field descriptions

Contact Membership Details

Field	Description
Label	The text description for classifying this contact.
Alternative Label	The text description for classifying this contact. The field is similar to **Label**, and is used to store label in an alternate language.
Description	The brief description about the contact.
Presence Buddy	An option to indicate whether to allow monitoring of the presence information of the contact.
Speed Dial	An option to indicate whether to allow speed dial for the contact.
Address/Handle	The fully qualified URI for interacting with the contact. This field is available only if you select the **Speed Dial** check box.
Speed Dial Entry	The reduced number that represents the speed dial number. This field is available only if you select the **Speed Dial** check box.

Contact Details

Field	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Middle Name	The middle name of the contact.
Description	The brief description about the contact.
Company	The name of the company to which the contact belongs.
Localized Display Name	The localized display name of a user. The name is usually the localized full name.
Endpoint Display Name	The endpoint display name of the contact.
Language Preference	The list of languages from which you set a language as the preferred language for the contact.
Update Time	The time when the contact information was last updated.
Source	The source of provisioning the contact.

Postal Address

Field	Description
Name	The name of the contact.
Address Type	The type of mailing address such as, home or office address.
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	The postal code of the locality of the city or town.
Province	The full name of the province of the contact.
Country	The name of the country of the contact.

Contact Address

Field	Description
Address	The address that you can use to communicate with the contact. The address can be a phone number, email address, or IM of the contact.
Type	The type of communication medium for interacting with the user.
Category	The categorization of the address based on the location.
Label	The description for classifying this contact.

Table continues…

Field	Description
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.

Table continues…

Name	Description
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.

Filtering users

About this task

You can apply filter to the following user information:

- Last Name
- First Name
- Display Name
- Login Name
- SIP Handle

You can apply one or more filters to view users that match the filter criteria.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **Filter: Enable**.

   The system displays the **Filter: Enable** button at the upper-right corner of the table that displays users.
4. Enter the information for one or more of the following filter criteria:
   - To filter users by the last name, in the **Last Name** column, enter the last name of the user.
   - To filter users by the first name, in the **First Name** column, enter the name of the user.

     To filter names that begin with a specific letter, enter the letter in the field. You can enter a string of letters to filter the names that begin with the string.
   - To filter users by the login name, in the **Login Name** column, enter the login name.

     To filter the login names that begin with a specific letter, enter the letter in the field. You can enter a string of letters to filter login names that begin with the string.
   - To filter users by the SIP handle, in the **SIP Handle** column, enter the SIP handle of the user.
5. **(Optional)** To hide the column filters, click **Disable**.

   This action does not clear any filter criteria that you had set.
6. Click **Apply**.

   The table displays the users that match the filter criteria.
7. To clear the filter criteria, click **Clear**.

Searching for users

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **Advanced Search** at the upper-right corner of the page.
4. In the Criteria section, do the following:
   a. In the first field, select the search criterion.
   b. In the second field, select the operator.
   c. In the third field, enter the search value.

   To add another search criterion, click **+** (plus) and repeat Step a through Step c listed in Step 4.

   To delete a search criterion, click **-** (minus) next to the search criterion. The system displays the **-** button only if more than one search criterion is available.
5. Click **Search**.

Result

The **Users** table lists the users that match the search criteria.

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

Managing user provisioning rules

User Provisioning Rule

System Manager 6.3.4 introduced a new set of workflows to streamline the user provisioning process. You can apply a user provisioning rule with other LDAP Synchronization Capabilities to achieve fully automated user provisioning. You can also assign a communication profile to every user.

A user provisioning rule includes a master communication profile template and a set of provisioning rules. A user provisioning rule enables predefined templates that consist of user attributes found in the communication profile of the user. In the user provisioning rule, the administrator specifies the following information to provision the user:

- Basic information that includes the communication profile password, time zone, and language preference
- The communication system that the user must use, for example, Communication Manager
- The method to assign or create a communication profile for the user, for example, by assigning the next available extension for Communication Manager

When the administrator creates the user using the user provisioning rule, the system populates the following data based on the user provisioning rule:

- The default values
- The communication addresses
- The communication profiles for the user

You can create and apply the user provisioning rule only if you have administrator credentials. The administrator can assign only one user provisioning rule to every user. The administrator can provision the user using the user provisioning rule from one of the following System Manager user interfaces:

- Web Console
- Web Services
- Folder name Synchronization
- Bulk import

Note:

To perform the user provisioning by using the user provisioning rule, map the user to the role with the following permissions:

Resource type	Permissions
All elements of type:elements	view

Capabilities and guidelines of User Provisioning Rules

Capabilities of User Provisioning Rules

User provisioning rule is a template that you can use to create a user. You can define and apply a user provisioning rule only if you have administrator credentials. You can use the user provisioning rule for the initial provisioning and during the creation of the user. User provisioning rules cannot be used after they are applied. After you create a user a user provisioning rule, System Manager populates the following data based on the rules defined in the user provisioning rule:

- The default values
- The communication addresses

- The user attributes from the communication profiles

General guidelines

- After you define a user provisioning rule and apply the user provisioning rule to create a user, you cannot edit the communication profile associated with the user provisioning rule. You cannot change, delete, or add the data in the communication profile. To edit the communication profile, you must reapply the user provisioning rule to the user. You can assign only one communication profile to a user provisioning rule.
- However, you can edit the user attributes that are not the part of the communication profile. To edit such user attributes, you can use any of the following System Manager user provisioning interfaces:
  - System Manager native user interface
  - Web Services API
  - Bulk Import/Export Tool
  - Global Endpoint Change Editor

Adding User Provisioning Rules

About this task

Add a service defined in a communications profile to an existing user that was created 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. In this case, the new service defined in the communications profile gets added to the existing user.

   You can add any of the following services:

   - Presence
   - Messaging
   - Collaboration Environment
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.

Result

Creating the user provisioning rule

Procedure

1. Log on to System Manager as admin.
2. On the System Manager web console, click **Users** > **User Provisioning Rule**.
3. On the User Provisioning Rules page, click **New**.
4. On the New User Provisioning Rule page, perform the following:
   a. On the **Basic** tab, enter the appropriate information.
   b. On the **Communication Profile** tab, select the appropriate communication profile, and enter the information.

   For more information, see User Provisioning Rule field descriptions.
5. Click **Commit** to save the changes.

Modifying the user provisioning rule

Before you begin

Create a user provisioning rule.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager web console, click **Users** > **User Provisioning Rule**.
3. On the User Provisioning Rules page, select the user provisioning rule.
4. To edit the user provisioning rule, perform one of the following:
   - Click **Edit**.
   - Click **View** > **Edit**.
5. On the Edit User Provisioning Rule page, perform the following:
   a. On the **Basic** tab, modify the appropriate information.

      Note:

      - System Manager does not automatically modify the user if the user provisioning rule changes.
      - You can select a different user provisioning rule when you modify the user information.

   b. On the **Communication Profile** tab, modify the communication profile information as appropriate.

   For information, see User Provisioning Rule field descriptions.

6. Click **Commit**.

Viewing the user provisioning rule

Before you begin

Create a user provisioning rule.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager web console, click **Users** > **User Provisioning Rule**.
3. On the User Provisioning Rules page, select the user provisioning rule and click **View**.

Creating a duplicate user provisioning rule

About this task

You can duplicate a user provisioning rule to create a new user provisioning rule by copying the information from the existing user provisioning rule.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager web console, click **Users** > **User Provisioning Rule**.
3. On the User Provisioning Rules page, select the user provisioning rule.
4. Click **Duplicate**.
5. On the Duplicate User Provisioning Rule page, perform the following:
   a. On the **Basic** tab, change the appropriate information.
   b. On the **Communication Profile** tab, change the communication profile information as appropriate.

   For more information, see User Provisioning Rule field descriptions.
6. Click **Commit**.

Deleting the user provisioning rule

Procedure

1. Log on to System Manager as admin.
2. On the System Manager web console, click **Users** > **User Provisioning Rule**.
3. On the User Provisioning Rules page, select one or more user provisioning rules.

4. Click **Delete**.
5. On the Delete User Provisioning Rule page, click **Delete**.

   The system removes the user provisioning rule from System Manager.

   System Manager disassociates the user provisioning rule from the user if you have already provided the user provisioning rule for the user.

User Provisioning Rules Management field descriptions

Field	Description
Name	The name of the user provisioning rule.
SIP Domain	The name of the configured SIP domain name.
Description	A brief description of the user provisioning rule.

Button/Icon	Description
View	Displays the View User Provisioning Rule page with details of the user provisioning rule that you selected.
Edit	Displays the Edit User Provisioning Rule page where you can modify the selected rule.
New	Displays the New User Provisioning Rule page where you can create a new rule.
Delete	Deletes the user provisioning rule that you selected.
Duplicate	Copies the user provisioning rule that you selected.
	Refreshes the user provisioning rule information in the table.
Select	• All: Selects all user provisioning rules in the table. • None: Clears the check box selections.

User Provisioning Rule field descriptions

Basic

Field	Description
User Provisioning Rule Name	The name of the user provisioning rule.
Description	A description of the user provisioning rule.
SIP Domain	The name of the configured SIP domain name.

Table continues…

Field	Description
	If **SIP Domain** is nonblank, create an Avaya SIP communication address for this user.
Presence/IM Domain	The name of the configured Presence domain name. If **Presence/IM Domain** is nonblank, create an Avaya Presence/IM communication address for this user.
Communication Profile Password	The communication profile password.
Confirm Password	The communication profile password that you must re-enter.
Use Phone Number last ..... digits for Extension	The number of last digits of the phone number that the system uses from the LDAP attribute. E.164 numbers can contain maximum 15 digits. Usually, the numbers are written with a plus (+) as the prefix. The system populates the phone number that is mapped to the LDAP attribute with the value in the **Prefix for Avaya E164 Handle** field. The LDAP attribute is mapped to the `Phone Number` attribute of System Manager on the User Synchronization Datasource page.
Prefix for Avaya E164 Handle	The digits that the system must prefix to Avaya E. 164 Handle.
Language Preference	The preferred written or spoken language of the user. For example, English.
Time Zone	The preferred time zone of the user.

Button	Description
Commit	Creates the user provisioning rule and displays the User Provisioning Rule page.
Cancel	Cancels the create, edit, or delete operation of the user provisioning rule.
Done	Saves the changes that you make to the user provisioning rule. The system displays this button only during the view operation.
Edit	Displays the fields in the edit mode. The system displays this button only during the view operation.

Communication Profile tab: Session Manager Profile

Note:

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

Field	Description
Primary Session Manager	The instance that you want to use as the home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura® network. You must select the primary Session Manager server.
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. A selection is optional.
Survivability Server	For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile when the local connectivity to Session Manager instances in Avaya is lost. If you select a Branch Session Manager , and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional. **Note:** If a termination or origination application sequence contains a Communication Manager application, the Communication Manager instance associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.

Table continues…

Field	Description
Block New Registration When Maximum Registrations Active	If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint.
Origination Application Sequence	The application sequence that the system will invoke when routing the calls from this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Termination Application Sequence	The application sequence that will be invoked when the system routes the calls to this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Home Location	The home location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any of the location. You must specify a value.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.

Communication Profile tab: Collaboration Environment Profile

Field	Description
Service Profile	The profile that you assign to the user. The user can gain access to the service contained in the profile.

Communication Profile tab: CM Endpoint Profile

Note:

The system displays these fields only if a CM Endpoint profile exists for the user.

Field	Description
System	The Communication Manager system on which you add the endpoint. You must select the system.
Profile Type	The type of the Communication Manager Endpoint profile that you create. You must select the profile type.
Use Next Available Extension	Select the check box to instruct the system to create a new extension for the user. **Note:** For LDAP synchronization, the value in the **Use Phone Number last ..... digits for Extension** field takes priority.
Template	The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add. You must select the template.
Security Code	The security code for authorized access to the endpoint.
Preferred Handle	Avaya SIP or Avaya E.164 handle that is administered for the user. The field is optional. By default, the field is blank.
Password	The password to gain access to the endpoint. The system displays the field if you select Agent in the **Profile Type** field.
Delete Endpoint on Unassign of Endpoint from User or on Delete User	The option to specify whether to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.
Override Endpoint Name	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

Table continues…

Field	Description
	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: CS 1000 Endpoint Profile

Field	Description
System	The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.
Target	The phone or endpoint template that you can choose for the user. Select a template from the drop down list. The element manager maintains all the templates. You must select the template.
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. You must select the 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.

Table continues…

Name	Description
Password	The password for logging in to the mailbox. You must provide the password.
Delete Subscriber on Unassign of Subscriber from User or on Delete User	The option to specify whether to delete the subscriber mailbox from the Messaging device or Communication System Management when you remove this Messaging profile or when you delete the user.

Communication Profile tab: CallPilot Messaging Profile

You cannot assign the mailbox number in the CallPilot communication profile by using the user provisioning rule. You must add the mailbox number for the CallPilot communication profile.

Field	Description
System	The CallPilot system of the messaging profile. The selection is mandatory required.
Target	The field that maps to the CallPilot **Location** field. CallPilot Manager provides the **Target** field. You must select the target.
Template	The mailbox template that you use. Select a template from the drop down list. The element manager maintains all the mailbox templates. You must select the template.

Communication Profile tab: IP Office Endpoint Profile

Field	Description
System	The list of IP Office device names from which you can select the IP Office device that you associate with the user. You must select the template.
Extension	The extension of the endpoint to which you associate the profile. The options are: • Use CM Extension: Use this option only if Communication Manager profile is specified. • Use Next Available Extension: Use this option if the system must use the next extension to associate with this profile.
Template	A list of user templates from which you can select a template to set the user configurations.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the system automatically populates the set type value.

Communication Profile tab: Presence Profile

Field	Description
System	Selects 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 field used to route SIP based messages through the Presence Services This system selects the SIP entity only if you select a Presence Services instance in the **System** field. **SIP Entity** is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.
IM Gateway	The IP address of the IM gateway.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with the AES Collector. The options are: • **System Default** • **Off** • **On** The default is **System Default**. You can change the default value. You do not require to configure AES Collector in the Presence Services server.

Communication Profile tab: Conferencing Profile

Name/Button	Description
Template	The template that you use to set the user configurations.
Location	The location that Conferencing uses when the IP address of the calling phone does not match any IP address pattern of any location. Specify this field to support the mobility of the user.
Select Auto-generated Code Length	The number of digits in the security code that the system generates.
Auto Generate Participant and Moderator Security Codes	The check box that you select to instruct the system to generate the security codes for the participant and moderator.

Button	Description
Commit	Saves the changes and displays the User Provisioning Rules page.
Cancel	Cancels the operation and displays the User Provisioning Rules page.

Role Based Access Control

Role Based Access Control (RBAC) in System Manager supports two types of roles:

- Built-in
- Custom

Built-in roles are the default roles provided by System Manager. You can assign built-in roles to users. You cannot change or delete the permission mappings in the built-in roles.

Some of the important built-in roles and the privileges are as follows:

Role	*Privileges and Limitations*
Auditor	• Read-only access to the system. • Read-only access to logs, configuration information and audit files. Not allowed to run any commands.
Session Manager and Routing Administrator	Read-write access to the Session Manager and Routing web pages.
Session Manager and Routing Auditor	Read-only access to the Session Manager and Routing web pages.
Security Administrator	• Create other logins. • Create, modify, or assign roles. • Install ASG keys. • Install licenses. • Install PKI certificates and keys.
Backup Administrator	Perform backups and restores.
System Administrator	• Read-write access to system parameters. • Modify, assign, or define other roles. • Create and modify logins and all other functionalities.
Avaya Maintenance and Support	• Read-only access to maintenance logs. • Run diagnostics. • View the output of diagnostics tools. Not allowed to run any command that may provide access to another host.

This section explains the administration required for defining custom roles that have access to the Session Manager and Routing web pages.

Note:

Only the following built-in roles provide access to the Session Manager and Routing web pages:

- Auditor
- Session Manager and Routing Administrator
- Session Manager and Routing Auditor
- System Administrator
- Avaya Services Administrator

With the Session Manager RBAC feature, a system administrator can assign permissions to specific Session Manager and Routing web pages. A user can access or modify only those web pages for which the user is authorized.

The possible permissions include:

- Total read/write permissions. The administrator can view the page and can make modifications to all of the administered fields which are on the page.
- Read-only permissions. The administrator can view the entire page, but cannot make any changes to the fields on the page. The administered fields display the current contents, and the buttons are not operational.

Important:

Providing full access to the Session Manager and Routing web pages does not automatically entitle a user to access the following System Manager elements. You must explicitly grant access permissions to these System Manager web pages:

- Replication
- Inventory > Manage Elements
- User Management

RBAC permissions for Routing Import/Export operations

For a user to import Routing data, the administrator must assign one of the following roles:

- System Administrator
- Avaya Services Administrator and Scheduler operation
- Session Manager and Routing Administrator and Scheduler operation

A user with read/write permissions for a specific Routing page cannot import any Routing data.

For a user to export Routing data, the administrator must assign one of the following built-in default roles to the user:

- System Administrator

- Avaya Services Administrator
- Session Manager and Routing Administrator
- Auditor
- Session Manager and Routing Auditor

When exporting data as an Auditor, the user must perform the export operation from the Bulk Import and Export menu.

RBAC permissions for Local Host Name Resolution imports

For a user to import host name entries on the Local Host Name Resolution page, the administrator must assign one of the following roles:

- System Administrator
- Avaya Services Administrator and Scheduler operation
- Session Manager and Routing Administrator And Scheduler operation

The user must have read/write permissions for the Local Host Name Resolution page and scheduler operation permissions. Import operations can only be performed by a user with permissions to schedule jobs using the System Manager Scheduler.

RBAC permissions for Bulk Communication Profile edits

The administrator must assign one of the following roles to a user to edit more than 15 Communication Profiles on the Communication Profile Editor page:

- System Administrator
- Avaya Services Administrator and Scheduler operation
- Session Manager and Routing Administrator and Scheduler operation

The user must have read/write permissions for the Communication Profile Editor page and scheduler operation permissions.

For more than 15 users, LHNR imports and bulk communication profile edits are performed as scheduled jobs. The operations can only be performed by a user with permissions to schedule jobs using the System Manager Scheduler.

Creating a Scheduler operation role

You must assign the **Scheduler operation** role to the following roles to use the import operation:

- Avaya Services Administrator
- Session Manager and Routing Administrator

Procedure

1. On the home page of the System Manager Web Console, under **Users**, select **Groups & Roles** > **Roles**.
2. On the Roles page, select **System Administrator**.
3. Click **New**.
4. On the Add New Role page, enter a name in the **Role Name** field.
5. Enter a short description of the role in the **Role Description** field.
6. Click **Commit and continue**.
7. In the **Element/service Permissions** tab, click **Add mapping**.
8. On the **Select Element and/or network Service to Map to Role** page, select **Scheduler operation** from the drop-down menu for **Element or Resource Type**.
9. In the **Element or Resource Instance** field, select **ALL** from the drop-down menu.

   Note:

   Group selection is optional.
10. Click **Next**.
11. On the Permission Mapping page, select the **Select/Unselect All** check box.
12. Click **Commit**.

Creating an RBAC role with read-only permissions

This procedure creates an RBAC role with read-only access for all web pages or specific web pages under the Session Manager and Routing tabs.

On the Permission Mapping page, the administrator can grant the role:

- access to all Session Manager and Routing pages.
- access to specific pages.

To copy the permission mappings of an existing role, see Copying permission mapping for a role on page 151.

Procedure

1. On the home page of the System Manager Web Console, under **Users**, select **Groups & Roles** > **Roles**.
2. On the Roles page, select **System Administrator**.
3. Click **New**.
4. On the Add New Role page, enter a name in the **Role Name** field.
5. Enter a short description of the role in the **Role Description** field.

6. Click **Commit and continue**.
7. In the **Element/Service Permissions** tab, click **Add mapping**.
8. On the **Select Element and/or Network Service to Map to Role** page:
   a. In the **Element or Resource Type** field, select **Session Manager and Routing** from the drop-down menu.
   b. In the **Element or Resource Instance** field, select **All** from the drop-down menu.

   Note:

   Group selection is optional.
9. Click **Next**.
10. On the Permission Mapping page, do one of the following:
    - To grant access to all pages, select the **Read-only access to all web pages under the Session Manager and Routing tabs** check box.
    - To grant page-level access:
      a. Expand the section heading on the page corresponding to each of the Session Manager and Routing web pages.
      b. Select the read-only check box for the specific page.
11. Click **Commit**.

    The system displays the Role Details page with the permissions you have chosen.
12. Click **Commit**. The system creates the new role that is added to the displayed roles on the Roles page.
13. Assign the role to a user. See Assigning an RBAC role to a user on page 149.

Creating an RBAC role with read and write permissions

Create an RBAC role with read and write permissions for all web pages or specific web pages under the Session Manager and Routing tabs.

On the Permission Mapping page, the administrator can grant the role:

- Access to all Session Manager and Routing pages.
- Access to specific pages.

To copy the permission mappings of an existing role, see Copying permission mapping for a role on page 151.

Procedure

1. On the home page of the System Manager Web Console, under **Users**, select **Groups & Roles** > **Roles**.
2. On the Roles page, select **System Administrator**.

3. Click **New**.
4. On the Add New Role page, enter a name in the **Role Name** field.
5. Enter a short description of the role in the **Role Description** field.
6. Click **Commit and continue**.
7. In the **Element/Service Permissions** tab, click **Add mapping**.
8. On the **Select Element and/or Network Service to Map to Role** page:
   a. In the **Element or Resource Type** field, select **Session Manager and Routing** from the drop-down menu.
   b. In the **Element or Resource Instance** field, select **All** from the drop-down menu.

   Note:

   Group selection is optional.
9. Click **Next**.
10. On the Permission Mapping page, select the **Full Access or selected permissions** check box.
11. Click **Commit**.

    The system displays the Role Details page with the permissions you have chosen.
12. To confirm your settings, click **Commit**.

    The system creates the new role and adds the role to the displayed roles on the Roles page.
13. Assign the role to a user. See Assigning an RBAC role to a user on page 149.

    Note:

    If the user needs to import Routing data, perform LHNR imports, or edit Communication Profiles, the administrator must assign one more role Scheduler opertaion.

Assigning an RBAC role to a user

Assign a Role Based Access Control role to a user.

To assign a role to multiple users, see *Assigning users to an RBAC role* in *Administering Avaya Aura® System Manager* on the Avaya Support website at http://support.avaya.com.

Note:

If you assign a new role to a user and do not provide a new password, the system resets the password to match the login name of the user. When the user logs in, the system prompts the user to change the password.

Procedure

1. On the home page of the System Manager Web Console, under **Users**, select **User Management** > **Manage Users**.
2. On the User Management page, do one of the following:
   - To assign a role while setting up a new user account, click **New**.
   - To assign a role to an existing user, select the user and click **Edit** or **View** > **Membership** > **Edit**.
3. On the New User Profile or User Profile Edit page, click the **Membership** tab.
4. Click **Assign Roles**.
5. On the Assign Roles page, select a role from the **Available Roles** section.
6. To assign the role to the selected user, click **Select**.
7. On the New User Profile page or the User Profile Edit page, click **Commit** to save the changes.

Configuring a user to have access permissions for System Manager web pages

This procedure explains the administration required to grant access to the following System Manager element that is required for Session Manager administration and maintenance:**Elements** > **Inventory** > **Manage Elements**.

Procedure

1. On the home page of the System Manager Web Console, under **Users**, select **Groups & Roles** > **Roles**.
2. On the Roles page, select **System Administrator**.
3. On the Add New Role page, enter a name in the **Role Name** field.
4. Enter a short description of the role in the **Role Description** field.
5. Click **Commit and continue**.
6. In the **Element/Service Permissions** tab, click **Add mapping**.
7. To add operations permission, in the **Select Element and/or Network Service to Map to Role** page, click **operation** under the **Element or Resource Type** category.
8. Click **Next**.
9. For access to the **Inventory** > **Manage Elements** pages, select the **Elements/ ApplicationManagement** and **Services/Inventory/ManageElements** elements.
10. For read/write access to the page, select **RTS_Administration** and **RTS_Administration/ RTS_Edit_Operation**.

11. For read-only access to the Manage Elements web page, select **RTS_Administration**.

    Note:

    If a user is assigned to a role with read/write access to the Session Manager web pages, the user must also be authorized to add, edit or delete elements on the Manage Elements web page. Likewise, a user assigned to a role with read-only access to the Session Manager web pages must be given read-only permissions on the Manage Elements web page.

12. Click **Commit**. The system displays the Role Details page with the permissions you have chosen.
13. To confirm your settings, click **Commit**.

    The system adds the new role to the displayed roles in the Role page.

14. Assign the role to a user. See Assigning an RBAC role to a user on page 149.

Copying permission mapping for a role

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, click the **Element/Service Permissions** tab.
5. Click **Copy All From**.

   The system displays the Permission Mapping page.

6. In the **Copy From Role** field, select a role.

   The system displays all child roles of the parent of this role and all child roles of this role.

   Note:

   Using the **Copy From Role** option, you cannot copy permissions from the System Administrator role.

7. Click **Copy**.

   The system displays the Role Details page

8. Click **Commit**.

   The system displays the Roles page where you can view the details of the role.

Removing access permissions for Session Manager and Routing pages

For information about disassociating the roles from a user, see *Removing roles from a user* in *Administering Avaya Aura® System Manager* on the Avaya Support website at http://support.avaya.com. You can follow the same procedure as explained below for removing access permissions for other element pages.

To delete a custom role, see *Deleting a role* in *Administering Avaya Aura® System Manager*.

Procedure

1. On the home page of the System Manager Web Console, under **Users**, select **Groups & Roles** > **Roles**.
2. On the Roles page, select a role.
3. On the Role Details page, click the **Element/Service Permissions** tab.
4. Select an Element/Service Permission of type **Session Manager and Routing** from the list and click **Delete Mapping**.

   The system displays the Delete Mapping page.
5. Click **Delete** to delete the selected role mapping.

Removing the assigned RBAC role from a user

Procedure

1. On the home page of the System Manager Web Console, under **Users**, click **User Management** > **Manage Users**.
2. On the User Management page, select the appropriate user and click **Edit**.
3. On the User Profile Edit page, click the **Membership** tab.
4. Select the role you want to remove and click **UnAssign Roles**.
5. Click **Commit**.

Managing bulk import and export

Bulk import and export

In System Manager, you can bulk import and export user profiles and global settings. To import data in bulk, you must provide an XML file or an Excel file as input file. While exporting data in bulk, the system can export 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, Messaging, Session Manager, CS 1000 Endpoint, CallPilot Messaging, Conferencing, IP Office, Presence, and Collaboration Environment.

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 System Manager Web Console, the system exports the data to an XML file and an Excel file that System Manager supports.

Microsoft Office Excel 2007 and later support bulk import and export in the .xlsx format. You can download the Excel file from the User Management page.

Import and export in bulk using the Excel template provides the following features:

- Supports the following types of user information:
  - Basic. The identity attributes of the user that include user provisioning rule name for the user, the tenant, and organization hierarchy details
  - Profile Set. Entries for all communication profile sets for all users

The Profile Set sheet contains an entry for each communication profile set for a user. The user must set only one communication profile set as true for a user in the **Is Default** column. The value true indicates that the communication profile set of the user is default.

- Handle. The communication address of the user
- Session Manager profile
- Collaboration Environment profile
- CM Endpoint profile with all attributes of the station communication profile.

  System Manager supports import and export of the CM Agent profile data associated with the user using XML only. You cannot import or export the CM Agent profile data by using Excel. Therefore, with the Excel file bulk import functionality, you cannot create a user with the CM Agent profile. If you export a user with the CM Agent profile, the system exports the user without the agent profile data in the Excel file.
- Messaging profile
- CallPilot profile
- IP Office Endpoint profile
- CS 1000 Endpoint profile
- Presence profile
- Conferencing profile

- Supports more than one communication profile set.
- Supports the creation, updation, and deletion of the user using the same Excel file. However, you can perform one operation at a time.
- For updation, supports only the partial merge operation.

  Bulk import and export by using Excel does not support complete or partial replace of the user for imports in bulk.

Bulk import and export by using Excel supports a subset of user attributes that XML supports. For example, Excel does not support user contacts, address, and roles.

The Excel file

The sample Excel file contains the sample data of some key attributes of the user. The Excel file provides a description of header fields. When you download the Excel template from the **User Management** page, the values remain blank. To use the Excel file, export some users for reference in an Excel file.

The Excel file provides the login name in the **Basic** worksheet as the key attribute that you use to link the user records in other worksheets.

The login name of the user and the profile set name in the **Profile Set** worksheet are used as key to link to the user records in other worksheets for that user profile.

- Although you can edit the header fields in the Excel template, do not change any details of any headers in the worksheets. The import or export might fail if you change the details of the header.
- Do not change the column position in the Excel file or change the structure of the Excel template.

- Do not sort the data in worksheets.

CM Endpoint communication profile

The Excel file contains all attributes for the CM station endpoint profile. The Excel file provides the station endpoint attributes in more than one 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.

XML Schema definitions and sample XMLs for bulk import

See List of XML Schema Definitions and sample XMLs for bulk import on page 736.

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 the child worksheet contains only one record for that user profile.

Login Name*	Room	Jack	Cable	Floor	Building	Headset	Speaker	Mounting	Cord Length	Set Color	
johnmiller@avaya.com#Primary						false	false	d	0		

The following **Buttons** worksheet contains multiple records for johnmiller@avaya.com#Primary, the user profile, but the link points to the first record in the list.

Login Name*	Number*	Type*	Data1	Data2	Data3	Data4	Data5	Data6
johnmiller@avaya.com#Primary	1	call-appr						
johnmiller@avaya.com#Primary	2	call-appr						
johnmiller@avaya.com#Primary	3	call-appr						

Example of handling multiple communication profile sets for a user

In the exported Excel file, the system appends the login name with #profileSetName in all worksheets except the **Basic** and **Profile Set** worksheets. Appending the profile set name to the login name associates the communication profile set with the user record, for example, jmiller@avaya.com#profileSetName. When you export users in the Excel file, the association is automatic. When you provide data in a blank Excel template that you downloaded for import, you must make the association manually.

Note:

The **Profile Set** worksheet must contain all communication profile sets of a user, but only one communication profile set can be the default. The **Is Default** column is set to `true` only for the default profile.

In the **Profile Set** worksheet, the two communication profile sets for the user John Miller must contain the following information:

Login Name*	Name*	Is Default*
johnmiller@avaya.com	secondaryProfile	false
johnmiller@avaya.com	Primary	true

If a SIP e164 handle is associated with secondaryProfile of John Miller, the **Handle** worksheet must contain the following information:

Login Name*	Handle*	Type*	Sub Type	Domain
johnmiller@avaya.com#secondaryProfile	+1123	sip	e164	smgrdev.avaya.com

If a Session Manager communication profile is associated with secondaryProfile of John Miller, the **Session Manager Profile** worksheet must contain the following information:

Login Name*	Type*	Session Manager	Session Manager	Termination Application Sequence	Origination Application Sequence	Conference Factory Set	Survivability Server	Home Location*	Max. Simultaneous Devices	Block New Registration When Max Active	Enable Disable Call Log
johnmiller@avaya.com#secondary Profile	Session Manager	sm6						Pune	6	false	true

If a Collaboration Environment communication profile is associated with Primary for John Miller, the **CE Profile** worksheet must contain the following:

Login Name*	Type*	Service Profile*
johnmiller@avaya.com#Primary	AUS	TempProfile

Hierarchy in communication profile worksheets

The table provides the parent-child relation of communication profile worksheets in the Excel template for bulk import and export of user.

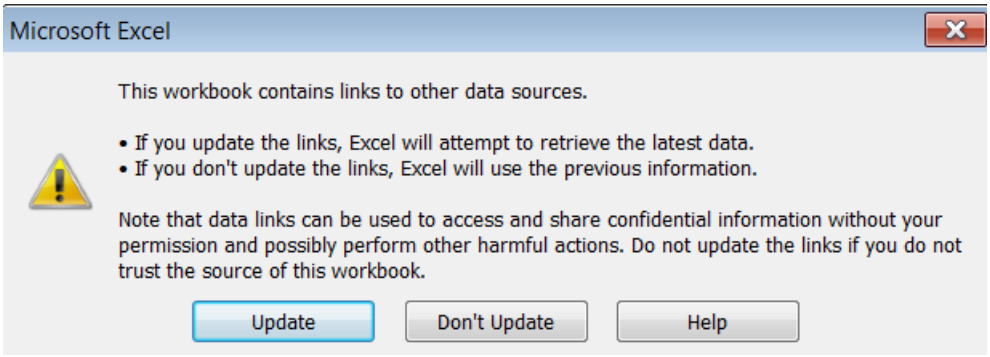
Element	Master worksheet	Child worksheets
Session Manager	Session Manager Profile	None
Communication Manager	CM Endpoint Profile	• Station Site Data • Buttons • Feature Buttons • Expansion Module Buttons • Soft Keys • Display Buttons • Station Abbr Dialing Data • Station Data Module • Station Hot Line Data • Native Name Data
Messaging	Messaging Profile	None
Conferencing	Conferencing Profile	None

Table continues…

Element	Master worksheet	Child worksheets
IP Office	IP Office Endpoint Profile	None
CS 1000	CS 1000 Endpoint Profile	None
Collaboration Environment	CE Profile	None
CallPilot	CallPilot	None
Presence	Presence Profile	None

Microsoft Excel data link error

Microsoft Excel 2010 displays a data link error.



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.

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.

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 737. See Sample XML for bulk import of users with all attributes on page 744 for the sample XML file for bulk import of user.

You can perform the following tasks with the bulk import functionality:

- Abort or continue the import process when the import user operation encounters first error in the user input file.
- Perform the following import types:
  - A *Partial* import type helps import of users with specific user attributes.
  - A *Complete* import type helps import of users with all user attributes.
- Skip import of the users that already exist in the database. Use this option to import new users from the XML file.
- Replace the users in the database with the new users from the file you imported. The system performs the following actions:
  - Replaces all items of user collection attributes such as CommprofileSet and Contactlist.
  - Removes the existing items.
  - Adds the new items from the XML.
  - Updates the single-value user attributes.

  For example, the user John Miller has StationA and EndpointB as existing commprofiles in default commprofileset and you import an XML file containing users with StationC and EndpointB with *Replace* option. After you import, John Miller has commprofiles StationC and EndpointB in the default commprofileset.

Note:

For CS1000 Endpoint Profile and CallPilot Messaging Profile, you cannot import both communication profile and user at the same time. You must add the user and then merge the profile.

- Update and merge the user attributes data from the imported file to the existing data. The system performs the following actions:
  - Merges items of user collection attributes such as CommprofileSet and Contactlist.
  - Retains and updates the existing items.
  - Adds the new items from the XML.
  - Updates the single-value user attributes.

  For example, the user John Miller has StationA and EndpointB as existing commprofiles in default commprofileset and you import an XML file containing users with StationC and EndpointB with *Replace* option. After you import, John Miller has commProfiles StationA, StationC, EndpointB in the default commprofileset.
- Delete the user records from the database that match the records in the input XML file.
- Schedule the bulk import job.
- View the details of an import job:
  - Job scheduled time
  - Job end time
  - Job status
  - Job completion status in percentage
  - Total number of user records in the input file
  - Total number of user records with warnings in the input file
  - Total number of user records that fail to import in the input file
  - The link to the Scheduler user interface
- Cancel or delete an import job.
- View logs of records that fail to import and require manual intervention.
- Download failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and import the records again to the database.

The following two XML schema definitions are available based on the complete and partial import types:

- XML schema definition for bulk import of users: See XML Schema Definition for bulk import of users on page 737. 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 744 and Sample XML for bulk import of users with all attributes on page 744.
- XML schema definition for partial import of users: See XML Schema Definition for partial import of user attributes on page 752. 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 754.

To delete bulk users, a separate XML schema definition is defined. See XML Schema Definition for bulk deletion of users on page 756. For a sample XML that conforms to delete bulk users XML schema definition, see Sample XML for bulk deletion of users on page 757.

Configuration options for bulk import using Excel

You can bulk import only the supported user attribute data for users. The Excel file must be the downloaded Excel template file or exported Excel file.

The following configuration options are available for import of users by using the Excel file:

- Abort or continue the import process when the import user operation encounters first error in the user input file.
- Import users with specific or all user attributes that Excel supports.
- If a matching record already exists, you can:
  - Merge the user attribute data from the imported file to the existing data. For example, you can add a new handle to the existing user.
  - Delete the user records from the database that match the records in the input Excel file.
- Schedule the bulk import job.
- View the details of an import job:
  - Job scheduled time
  - Job end time
  - Job status
  - Job completion status in percentage
  - Total number of user records in the input file
  - Total number of user records with warnings in the input file
  - Total number of user records that fail to import in the input file
  - The link to the Scheduler user interface
- Cancel or delete an import job.
- View logs of records that fail to import and require manual intervention.

Downloading the Excel template file

If you choose to import or export 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 a different Excel file.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **More Actions** > **Download Excel Template**.
4. In the Opening <Excel template file name>.xlsx dialog box, select **Save File** and click **OK**.

   Important:

   Though the header fields in the Excel template are editable, do not change any details of the headers in the worksheets. The import or export might fail if you modify the details of the headers.

   For the sample Excel template, see the Excel template for bulk import and export that you download from the User Management page.

About bulk export of users

In System Manager, you can export users in bulk from the System Manager database. While exporting in bulk, the system exports the data to an XML file.

You can export the following user attributes in bulk:

- Identity Data
- Communication Profile Set
- Handles
- Communication profiles

  The supported communication profiles are CM Endpoint, Messaging, Session Manager, CS 1000 Endpoint, CallPilot Messaging, Conferencing, IP Office, Presence, and Collaboration Environment.

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 737.

The system generates the XML file on the System Manager server. You can specify the location of the file you want to export while running the Export User job.

You can schedule an export user job. The job parameter provides an option to specify the schedule time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.

When you import the same file to a new system, you must provide the password for users with the *system administrator* role. For security reasons, the system does not export the **Password** fields to the XML file. Therefore, import of users with the *system administrator* role fails.

To import users with the *system administrator* role, in the XML file for the users, add the following XML tag after the `<username>` tag:

```
<userPassword> provide password for user </userPassword>
```

The system imports the other user records with non system administrator roles and automatically sets the password to `Avaya123$` for **Complete Merge/Replace** import type. For **Partial Merge/ Replace** import type, if you do not specify the password, the existing password remains.

You can export user data in bulk from System Manager web console and by using the bulk export that you run from CLI. The utility is in the *$MGMT_HOME*`/bulkadministration/exportutility` directory, where *MGMT_HOME* is an environment variable that represents the System Manager HOME path.

Exporting users in bulk from web console

Procedure

1. On 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 some criteria in **Advanced Search** and click **Export All**, the system exports only the records that match the criteria.
3. **(Optional)** On the Export Users page, in the **User Attribute Options** section, select one or more check boxes to export contacts and specific communication profiles.

   By default, the system exports basic attributes, communication profiles, and contacts.

   For more information, see Export Users field descriptions.
4. Select a schedule option for the export job.

For more information, see Export Users field descriptions.

5. Click **Export** to complete the export operation.

   The system exports the user data to the XML and Excel file.

6. To view the data, in the **Export List** section, click the link in the **Download File** column.

exportUpmUser.sh command

Use the **exportUpmUser** command to export users in bulk from the System Manager database.

Note:

You can change the default values for optional arguments from the `bulkexportconfig.properties` file that is located in the `$MGMT_HOME/ upm/ bulkexport/exportutility` directory. MGMT_HOME is an environment variable that represents the HOME path for System Manager.

Syntax

```
exportUpmUser.sh -f -r -d -s -e -t
```

For example, **# sh exportUpmUser.sh** -f userExport -r 1000 -s 0 -e 1000.

-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.

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 752. For a sample XML file for import of user, see Sample XML for partial import of users on page 754.

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 **ImportUser ManagementUsers**.

   Also, to gain access to **Import users**, from 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 type:
   - XML
   - Excel

Note:

Use the Excel template that System Manager supports. If you fail to use the template that System Manager supports, 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 options:
   - 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**.

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 737. Partial import type uses a different XML schema definition, for more information, see XML Schema Definition for partial import of user attributes on page 752.

Before you begin

Export the users in bulk and generate the XML file.

About this task

For partial import of users, make the following changes in the user export XML file. You can generate the XML file by exporting users in bulk.

Procedure

1. Perform the following steps:
   a. Locate the following content in the generated XML file:

```
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:ns3="http://xml.avaya.com/schema/import1"
```

```
xmlns:ns4="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
```

b. Modify `tns:users` to `tns:deltaUserList`.

c. Remove `tns="http://xml.avaya.com/schema/import"`.

d. Modify `ns4="http://xml.avaya.com/schema/deltaImport"` to `tns="http://xml.avaya.com/schema/deltaImport"`

e. Modify `xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">` to `xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport userdeltaimport.xsd ">`

After you modify the XML file as instructed in Step b through Step e, the content in Step a changes to:

```
<tns:deltaUserList xmlns:ns3="http://xml.avaya.com/schema/import1"
xmlns:tns="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport userdeltaimport.xsd ">
```

2. Replace all instances of:

   - <tns:user> with <tns:userDelta>
   - </tns:user> with </tns:userDelta>
   - <tns:users> with <tns:deltaUserList>
   - </tns:users> with </tns:deltaUserList>

Next steps

You can now make the updates in the XML file and import the changes to update the user attributes in the database.

About Bulk Import Encryption utility

System Manager Import User supports import of encrypted user password field and the plain text Communication Profile password field into the database. For importing a user XML file with encrypted password, System Manager provides BulkImportEncryptionUtil, a utility tool that encrypts the “userPassword” and “commPassword” fields in the user import input file.

The utility tool takes an XML file with plaintext password field values as input. This utility encrypts the password fields and generates an XML file with encrypted password field. You can use the XML file to import user.

BulkImportEncryptionUtil is a standalone Java program. You can run the utility on any machine that has Java installed on it.

Encrypting passwords in user import file using BulkImportEncryptionUtil running on Windows

Before you begin

JDK 1.6 is installed on your computer. If the computer does not have JDK 1.6 installed, use the http://java.sun.com/javase/downloads/index.jsp URL to download JDK 1.6.

Procedure

1. Extract the contents of the `um_bulkimport-encryptUtil.zip` file from `$MGMT_HOME/upm/utilities` into a local folder.

   The `um_bulkimport-encryptUtil.zip` file contains the following files:

   - `um_bulkimport-encryptUtil.jar`
   - `log4j.jar` and script files
   - `um_bulkimport-encryptUtil.bat`
   - `um_bulkimport-encryptUtil.sh`
   - `Readme.txt`

2. At the command prompt, type `um_bulkimport-encryptUtil.bat <import|deltaimport> <xmlfilename> <basenamespaceprefix> <deltanamespaceprefix>`, where:

   - *import*|*deltaimport* specifies whether the input XML file has data for complete import or partial import. For complete import, this option value is `import` and for partial import this option value is `deltaimport`.
   - `xmlfilename` is the name of the XML file with complete path of the XML file that contains the data for importing the users data
   - *basenamespaceprefix* is the namespace prefix in the input XML file. In the following example, `tns` is the value for the *basenamespaceprefix* parameter.

     ```
     <?xml version="1.0" encoding="UTF-8"?>
     <tns:users xmlns:tns="http://xml.avaya.com/schema/import"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="http://xml.avaya.com/schema/import
     userimport.xsd" >
     ```

   - *deltanamespaceprefix* is the namespace prefix given in the partial import file. Specify this parameter if you are performing a partial import. In the following example, the *deltanamespaceprefix* value is `delta` and *basenamespaceprefix* value is `tns`.

     ```
     <?xml version="1.0" encoding="UTF-8"?>
     <delta:deltaUserList
     xmlns:delta="http://xml.avaya.com/schema/deltaImport"
     xmlns:tns="http://xml.avaya.com/schema/import"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
     userdeltaimport.xsd ">
     ```

Encrypting passwords in user import file using BulkImportEncryptionUtil running on Linux

Before you begin

Install JDK 1.6 on your computer. If the computer does not have JDK 1.6 installed, use the http://java.sun.com/javase/downloads/index.jsp URL to download JDK 1.6.

Procedure

1. Extract the contents of the `um_bulkimport-encryptUtil.zip` file from `$MGMT_HOME/upm/utilities` into a local folder.

   The `um_bulkimport-encryptUtil.zip` file contains the following files:

   - `um_bulkimport-encryptUtil.jar`
   - `log4j.jar` and script files
   - `um_bulkimport-encryptUtil.bat`
   - `um_bulkimport-encryptUtil.sh`
   - `Readme.txt`

2. At the command prompt, type `um_bulkimport-encryptUtil.sh <import|deltaimport> <xmlfilename> <basenamespaceprefix> <deltanamespaceprefix>`, where:

   - *import* | *deltaimport* specifies whether the input XML file has data for complete import or partial import. For complete import, this option value is `import` and for partial import this option value is `deltaimport`.
   - `xmlfilename` is the name of the XML file with complete path of the XML file that contains the data for importing the users data
   - *basenamespaceprefix* is the namespace prefix in the input XML file. In the following example, `tns` is the value for the *basenamespaceprefix* parameter.

     ```
     <?xml version="1.0" encoding="UTF-8"?>
     <tns:users xmlns:tns="http://xml.avaya.com/schema/import"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="http://xml.avaya.com/schema/import
     userimport.xsd" >
     ```

   - *deltanamespaceprefix* is the namespace prefix given in the partial import file. Specify this parameter if you are performing a partial import. In the following example, the *deltanamespaceprefix* value is `delta` and *basenamespaceprefix* value is `tns`.

     ```
     <?xml version="1.0" encoding="UTF-8"?>
     <delta:deltaUserList
     xmlns:delta="http://xml.avaya.com/schema/deltaImport"
     xmlns:tns="http://xml.avaya.com/schema/import"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
     userdeltaimport.xsd ">
     ```

Import user considerations

- If the comprofileset has associated handlelist or commprofilelist, you cannot merge or replace commprofileset attributes name and Isprimary.

  To move handlelist and commprofilelist from one commprofileset to another, perform the following:

  1. Perform Replace - Import file with no commprofileset.
  2. Perform Update (merge/replace) - Import file with the new commprofileset with associated handlelist and commprofiles.

- For security reasons, you do not export the **Password** fields in the XML file.

  When you import the same file to a new system, you must provide the password for users with the *system administrator* role. For security reasons, the system does not export the **Password** fields to the XML file. Therefore, import of users with the *system administrator* role fails.

  To import users with the *system administrator* role, in the XML file for the users, add the following XML tag after the `<username>` tag:

  ```
  <userPassword> provide password for user </userPassword>
  ```

  For **Complete Merge/Replace** import type, the system imports user records with nonSystem Administrator roles and automatically sets the password to `Avaya123$`. For **Partial Merge/ Replace** import type, if you do not specify the password, the existing password remains.

- To enhance the performance of a file with large user records, split the file into smaller file sizes. For example, you can split a user import file of 15 Kb into three files of 5 Kb each. To speed up the import process, schedule three import jobs in parallel. System Manager does have the ability to process multiple files concurrently.

Scheduling a user import job

System Manager supports scheduling of bulk import jobs from the System Manager console. You can schedule a job to run immediately or at a later time.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **ImportUser ManagementUsers**.

   Also, to gain access to **Import users**, from 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 type:
   - XML
   - Excel

Note:

Use the Excel template that System Manager supports. If you fail to use the template that System Manager supports, 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 the 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 **ImportUser ManagementUsers**.

   Also, to gain access to **Import users**, from 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 type:
   - XML
   - Excel

   Note:

   Use the Excel template that System Manager supports. If you fail to use the template that System Manager supports, 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 the 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 **ImportUser ManagementUsers**.

   Also, to gain access to **Import users**, from 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 **ImportUser ManagementUsers**.

   Also, to gain access to **Import users**, from 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 **ImportUser ManagementUsers**.

   Also, to gain access to **Import users**, from 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 **ImportUser ManagementUsers**.

   Also, to gain access to **Import users**, from 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 823. For sample XML file for import global settings, see Sample XML for bulk import of global setting records on page 829.

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 823.

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 833. For a sample XML conforming to delete bulk global settings XML schema definition, see Sample XML for bulk deletion of users on page 757.

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 823.

The system generates the XML file on the System Manager server. You can specify the location of the file you want to export while running the Export User job.

You can schedule an export global settings job. The job parameter provides an option to specify the schedule time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.

You can export user data in bulk from System Manager web console and by using the bulk export that you run from CLI. The utility is in the *$MGMT_HOME*/bulkadministration/exportutility directory, where *MGMT_HOME* is an environment variable that represents the System Manager HOME path.

Bulk exporting of global user settings

In System Manager, you can export global settings from the System Manager database. The export global settings utility is located in the *$MGMT_HOME*/upm/bulkexport directory, where MGMT_HOME is an environment variable that represents the System Manager HOME path.

Before you begin

Start an SSH session.

Procedure

1. Log in to System Manager using SSH as `root`.
2. To change the directory to `exportutility`, at the prompt, type `cd` *`$MGMT_HOME`*`/bulkadministration/exportutility`.

   MGMT_HOME is an environment variable that represents the home path for System Manager.
3. Type `# sh exportUpmGlobalsettings.sh … [OPTIONS].`
4. **(Optional)** To modify the default values for optional parameters, change the `$MGMT_HOME/bulkadministration/exportutility/config/bulkexportconfig.properties` file, where *MGMT_HOME* is an environment variable that represents the System Manager HOME path.

   For example, `# sh exportUpmGlobalsettings.sh –f globalSettingExport –r 1000 –s 0 –e 1000 –o 1.`

exportUpmGlobalsettings.sh command

Use the **`exportUpmGlobalsettings`** command to export global settings from the System Manager database.

Syntax

```
exportUpmGlobalsettings.sh -f globalSettingExport-r-d -s -e-t
```

-f The prefix of the file name for the file that you require to export.

-r The number of records per file.

-d The location of the file that you want to export.

-s The start index of record.

-e The number of records you want to export.

-t The job scheduling time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.

-o The global settings export filter. The default is 0. You can set one of the following values for the global settings export filter:

- *0* No Filter. 0 is considered as the start index value.
- *1* System Default Type filter
- *2* Enforced users filter
- *3* System Rule Type filter
- *4* System ACL Entry Type filter
- *5* Shared Address filter
- *6* Public Contact filter

Note:

You can change the default values for optional arguments from the `bulkexportconfig.properties` file that is located in the `$MGMT_HOME/ upm/ bulkexport/exportutility` directory. MGMT_HOME is an environment variable that represents the HOME path for System Manager.

Scheduling a global user settings import job

About this task

System Manager supports scheduling of bulk import jobs from the System Manager console. With the scheduling utility, you can schedule an import job to run immediately or at a later time.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.
3. On the Import Global Settings page, enter the complete path of the file in the **Select file** field.

   Also, you can click **Browse** to select a file.
4. Select one of the following error configuration options:
   - **Abort on first error**
   - **Continue processing other records**

5. Select one of the import options:
   - **Skip**
   - **Replace**
   - **Merge**
   - **Delete**
6. In the **Job Schedule** section:
   a. Click **Schedule later**.

      To run the import job immediately, click **Run immediately**. After you select this option, the fields related to scheduling become unavailable.

   b. Enter the date in the **Date** field.

      You can use the calender icon to select a date.

   c. Enter time in the **Time** field in the HH:MM:SS format.

   d. From the **Time Zone** field, select a time zone.
7. Click **Import**.

   The system displays the scheduled job in the Manage Jobs section.

Viewing details of a global user settings import job

You can view the following details of an import job:

- Job name
- Job scheduled by
- Job scheduled start time
- Job end time
- Job status
- Import file name
- Total number of user records in the import file
- Total number of user records successfully imported
- Total number of user records that failed to import
- Percentage complete status

About this task

You can view the error message for each user record that fails to import. You can download the failed user records in an XML file format. You can modify the XML file and import the file again.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.

2. Click **Import > User Management > Global Settings**.

   To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.

3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
4. Click **View job**.

   The Job Detail page displays the details of the selected job.

Viewing a global user settings import job on the Scheduler page

About this task

You can view and perform all operations on an import job that the scheduler supports from the Scheduler page.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.

3. On the Import Global Settings page, select a job from the table in the Manage Job section.
4. Click the link in the **Job Name** column.

   The Scheduler page displays the details of the job.

Aborting a global user settings import job on first error

System Manager supports the following error configurations:

- Abort on first error. Aborts importing of the global settings records when the import global settings operation encounters the first error in the import file that contains the global settings records.
- Continue processing other records. Imports the next global settings record even if the import operation encounters an error while importing a global settings record.

About this task

You can abort an import process when the import process encounters the first error in the input file while processing the global user settings records.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.

2. Click **Import > User Management > Global Settings**.

   To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.

3. On the Import Global Settings page, enter the complete path of the file in the **Select file** field.

   Also, you can click **Browse** to select a file.

4. Select **Abort on first error** as the error configuration option.
5. Select one of the import options:
   - **Skip**
   - **Replace**
   - **Merge**
   - **Delete**
6. Choose or enter the appropriate information for the remaining fields.
7. Click **Import**.

Deleting a global user settings import job

System Manager supports deletion of an import job. The **Delete job** option removes the job information from the database. You can delete a job only when the job is in the *SUCCESSFUL* state.

To interrupt a job that is running or pending, use the **Cancel job** option.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.

3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
4. Click **Delete Job**.

Canceling a global user settings import job

You can cancel a job only when the job is in the PENDING EXECUTION or RUNNING state.

Procedure

1. On the System Manager web console, click **Services** > **Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

   To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users** > **User Management**. Click **Manage Users** and select **More Actions** > **Import Global Settings**.
3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
4. Click **Cancel job**.

List of XML Schema definitions and sample XMLs for bulk import

See XML Schema definitions and sample XMLs on page 155 for a list of XML Schema definitions and sample XML snippets for bulk import.

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 **More Actions** > **Download Excel Template**.

Button	Description
Browse	Displays a dialog box to select the file from which you import the users.

General

Name	Description
Select Error Configuration	The options are: • **Abort on first error**: Aborts importing the user records when the import user operation encounters the first error in the import file containing the user records. • **Continue processing other records**: Imports the next user record even if the import user operation encounters an error while importing a user record.
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.

Table continues…

Name	Description
	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.

Table continues…

Name	Description
	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.
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.

Table continues…

Name	Description
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.
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.

Table continues…

Button	Description
	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**.

Export Users field descriptions

User Attribute Options

Field	Description
Communications Profiles	The option to export one or more communication profiles from the list. By default, the system selects the **Communication Profiles** check box, which means the export operation exports all communication profiles.
Contacts	The option to export contacts. By default, the system selects the **Contacts** check box, which means the export operation exports contacts.

Schedule

Name	Description
Schedule Job	The settings to configure the schedule of the job. The options are: • **Run immediately**: To run the export job immediately. • **Schedule later**: To run the job at the specified date and time.
Date	The date when you must run the export job. The date format is mm dd yyyy. You can use the calendar icon to choose a date. This field is available when you select the **Schedule later** option for scheduling a job.

Table continues…

Name	Description
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.

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 job status options are: 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.
Scheduled Job	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 number of user records in the export file.
Failed Records	The number of user records in the input file that failed to export.
Download File	The link to download the zip file that contains an XML and Excel file that the system uses to export the user data.

Button	Description
View	Displays the details of the selected job.
Stop	Stops the export operation and takes you back to the User Management page.
Delete	Deletes the job that you selected.
Export	Exports or schedules the export job based on the option that you selected.
Done	Takes you back to the **User Management** page.

Job Details field descriptions

The Job Details page displays the details of the selected Job.

Name	Description
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	Takes you back to the Import Users page.

Import Global Settings field descriptions

Use this page to bulk import shared addresses, public contacts, and presence access control list (ACLs) from a valid XML file. These imported items are also called global user settings.

File Selection

Name	Description
Select File	The path and name of the XML file from which you must import the global settings records.

Button	Description
Browse	Opens a dialog box to select the file from which you must import the global user settings.

General

Name	Description
Select Error Configuration	The options are: • **Abort on first error**: Stops importing the global user settings records when User Management encounters the first error in the import file containing the global user settings records. • **Continue processing other records**: Imports the next global user settings record even if User Management encounters an error while importing a global user settings record.
If a matching record already exists	The options are: • **Skip**: Skips a matching global user settings record that already exists in the system database during an import operation. Currently, using this option you can add a new public contact to a public contact set but you cannot update an existing public contact in a public contact set. • **Merge**: Imports the global user settings data at an even greater degree of granularity. For example, add a shared address to a shared address list or update a public contact. • **Replace**: Re-imports or replaces all the global user setting records in the import file. This is essentially the ability to replace a user along with the other data related to the global user settings. • **Delete**: Deletes the global setting records from the database that matches the records in the input XML file.

Job Schedule

Name	Description
Schedule Job	The settings for configuring the schedule of the job: • **Run immediately**: Use this option to run the import job immediately. • **Schedule later**: Use this option to run the job at the specified date and time.

Table continues…

Name	Description
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	Takes you back to the **User Management** page.
Cancel	Cancels the import operation and takes you back to the User Management 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

Following are the minimal elements for mapping the user import XML with user interface fields:

Table 1: 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.

Table continues…

UI field	Description	XML tag	Possible value
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>	Log-in 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.

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 2: 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 3: 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 4: Mapping of Session Manager Communication Profile elements

UI field	Description	XML tag	Possible value

Primary Session Manager	Specifies the name of the primary Session Manager instance that is used as the home server for a communication profile.	`<sm:primarySM>`
		...
		`</sm:primarySM>`
			Enter the name of Session Manager.

Origination Application Sequence	Specifies the Application Sequence that is invoked when calls are routed from this user.	`<sm:originationAppSequence>`
		...
		`</sm:originationAppSequence>`
			True or False.

Termination Application Sequence	Specifies the Application Sequence that is invoked when calls are routed to this user.	`<sm:terminationAppSequence>`
		...
		`</sm:terminationAppSequence>`	

Home Location	Specifies the routing home location.	`<sm:homeLocation>`
		...
		`</sm:homeLocation>`	

The following is the mapping of CM Endpoint Profile elements with the corresponding user interface fields.

Table 5: 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.

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>`	

Table continues…

UI field	Description	XML tag	Possible value
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>	

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>
```

New User Profile field descriptions

Use the New User Profile page to create a new user. This page has four tabs:

- **Identity**
- **Communication Profile**
- **Membership**
- **Contacts**

Note:

Fields marked with an asterisk are mandatory and you must enter appropriate information in these fields.

Organization

Field	Description
Tenant	The name of the tenant that you must select.
Level 1	The name of the level 1 hierarchy of the tenant organization. For example, Site. The tenant administrator provides the hierarchy on the Tenant Management page.
Level 2	The name of the level 2 hierarchy of the tenant organization. For example, Department.
Level 3	The name of the level 3 hierarchy of the tenant organization. For example, Team.

User Provisioning Rule

Field	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

Field	Description
Last Name	The last name of the user. For example, Miller.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the end points. For example, Miller. Typically, the name is the written or spoken language of the user.
First Name	The first name of the user. For example, John.
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Login Name	The login name of the user. The login name is not case-sensitive. For example, if you enter JMILLER@AVAYA.COM, the system converts the login name to lowercase, that is, jmiller@avaya.com. However, on the login page, you can enter JMILLER@AVAYA.COM or jmiller@avaya.com. The login name can be in uppercase or lowercase. If you log in to the system as admin, you cannot edit the login name. **Note:** To create the user data by using a blank excel template, append the login name with #ProfileSetName in all worksheets except Basic and Profile Set. The system associates the user records with the communication profile that you have provided. For example, jmiller@avaya.com#ProfileSetName.
Authentication Type	The type of authentication that defines how the system performs the authentication of the user. The options are: • **Enterprise**: Directory servers that are external to System Manager authenticate the user login. • **Basic**: Avaya authentication service authenticates the user login. For bulk import of users by using Excel, **Authentication Type** is always Basic. Therefore, the

Table continues…

Field	Description
	Authentication Type field remains invisible in the Excel file.
Password	The password to log in to System Manager Web Console.
Confirm Password	The password that you reenter for confirmation.
Localized Display Name	The localized display name of a user. The name is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. The display name supports displays that cannot handle localized text, for example, some endpoints.
Title	The personal title that is set to address a user. The title is typically a social title and not the work title. For example, Mr.
Language Preference	The preferred written or spoken language of the user. For example, English.
Time Zone	The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.
Employee ID	The employee number for the user. For example, 20081234.
Department	The department to which the user belongs. For example, Human Resources.
Company	The organization where the user works. For example, Avaya Inc.

Identity tab: Address

Field	Description
Select check box	The option to select an address in the table.
Name	The name of the addressee. For example, Avaya.
Address Type	The type of address. The values are: • **Office** • **Home**
Street	The name of the street. For example, Magarpatta.
City	The name of the city or town. For example, Pune.
Postal Code	The postal code used by postal services to route mail to a destination. For example, 411028. For United States, the postal code is the Zip code.
Province	The full name of the province. For example, Maharashtra.
Country	The name of the country. For example, India.

Button	Description
New	Displays the Add Address page. Use the page to add the address details.
Edit	Displays the Edit Address page. Use the page to modify the address.
Delete	Deletes the selected address.
Choose Shared Address	Displays the Choose Address where you choose a shared or common address.

Identity tab: Localized Names

Note:

Use the **Localized Names** section only for the CS 1000 system. The section does not apply for Session Manager and Communication Manager.

Field	Description
Language	The localized languages for displaying the user name. For example, English. You must select the language.
Display Name	The user name in the localized language you choose. For example, John Miller.

Button	Description
New	Displays fields that you can use to create a new localized name for the user.
Edit	Displays fields that you can use to modify the localized name for the user.
Delete	Deletes the localized names that you select for the user.
Add	Adds or edits the localized name for the user.
Cancel	Cancels the addition or edits of the localized name.

Communication Profile tab: Communication Profile

Use this section to create, modify, and delete a communication profile of the user. Each communication profile can contain one or more communication addresses for a user.

Field	Description
Communication Profile Password	The communication profile password. The field is available only if you enable the communication profile. The password policy is configured from **Users** > **User Management** > **Communication Profile Password Policy**.

Table continues…

Field	Description
Confirm Password	The communication profile password that you reenter for confirmation.
Option button	The option to view the details of the selected communication profile.
Name	The name of the communication profile. You must select the name.

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Done	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding of a communication profile.

The system enables the following fields when you click **New** in the **Communication Profile** section.

Field	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.

Field	Description
Type	The type of the handle.
Handle	A unique communication address of the user.
Domain	The name of the domain with which the handle is registered.

Button	Description
New	The fields for adding a new communication address.
Edit	The button to edit the information of a selected communication address.
Delete	Deletes the selected communication address.

The page displays the following fields when you click **New** and **Edit** in the Communication Address section. The following fields define the communication address for the user.

Field	Description
Type	The type of the handle. The different types of handles are: • **Avaya SIP**: Indicates that the handle supports Avaya SIP-based communication. • **Avaya E.164**: Indicates that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix. • **Microsoft SIP**: Indicates that the handle supports SIP-based communication. • **Microsoft Exchange**: Indicates that the handle is an email address and supports communication with Microsoft SMTP server. • **Lotus Notes**: Indicates that the handle is for Lotus Notes and domino calender. • **IBM Sametime**: Indicates that the handle is for IBM Sametime. The address must be in the DN=IBMHandle format. • **Avaya Presence/IM**: Indicates that the handle is an address used for Extensible Messaging and Presence Protocol (XMPP)-based Internet Messaging (IM) services, and XMPP or Session Initiation Protocol-based (SIP) Presence services. • **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.
Fully Qualified Address	The fully qualified domain name or uniform resource identifier. The address can be an email address, IM user, or an address of a communication device by using which the user can send or receive messages. You must provide the fully qualified address.

Button	Description
Add	Saves the new communication address or modified communication address information in the database.
Cancel	Cancels the addition of communication address.

Communication Profile tab: Session Manager

Note:

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

Field	Description
Primary Session Manager	The instance that you want to use as the home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura® network. You must select the primary Session Manager server.
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. A selection is optional.
Survivability Server	For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile when the local connectivity to Session Manager instances in Avaya is lost. If you select a Branch Session Manager , and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional. **Note:** If a termination or origination application sequence contains a Communication Manager application, the Communication Manager instance associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.

Table continues…

Field	Description
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.
Block New Registration When Maximum Registrations Active	If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint. If you clear the check box, the system accepts the new registration and unregisters the endpoint with the oldest registration. However, if the endpoint with the oldest registration is active on a call then the system does not unregister the endpoint until the call completes.
Origination Application Sequence	The application sequence that the system will invoke when routing the calls from this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Termination Application Sequence	The application sequence that will be invoked when the system routes the calls to this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Home Location	The home location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any of the location. You must specify a value.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities.

Table continues…

Field	Description
	Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.
Enable Centralized Call History	The option to enable the call history feature for SIP users. By default, the system disables the call history feature. The maximum number of call logs per communication profile is 100.

Communication Profile tab: Collaboration Environment Profile

Field	Description
Service Profile	The profile that you assign to the user. The user can gain access to the service contained in the profile.

Communication Profile tab: CM Endpoint Profile

Note:

The system displays these fields only if a CM Endpoint profile exists for the user.

Field/Button	Description
System	The Communication Manager system on which you add the endpoint. You must select the system.
Profile Type	The type of the Communication Manager Endpoint profile that you create. You must select the profile type.
Use Existing Endpoints	Select the check box to use the existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint that you associate this profile with. You must select the extension. The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.
Endpoint Editor button	Click to start the Communication Manager application where you can edit or view details of the endpoint. After you save the changes in Communication Manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Template	The template, system defined or user defined, that you associate with the endpoint. Select the template

Table continues…

Field/Button	Description
	based on the set type you add. You must select the template.
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. You must select the port. The field lists the possible ports based on the selected set type.
Voice Mail Number	The voice mail number of the endpoint you associate with.
Preferred Handle	Numeric only handles, SIP handles,or nonSIP handles, that are administered for a user. The **Preferred Handle** field is optional. By default, the field is blank. If the SIP entity is of the Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
Enhanced Callr-Info display for 1–line phones	The option to activate the enhanced Callr-info operation on the phone. The **Enhanced Callr-Info display for 1-line phones** field on the station form is valid for the following set types: • 1603, 1608, 1616, 1408, 1416 • 2402, 2410, 2420 • 4606, 4612, 4612CL, 4624, 4602, 4602+, 4630, 4610, 4622, 4620, 4621, 4625, • 6402D, 6408D, 6408D+, 6416D+, 6424D+, 607A1 • 7506D, 7507D • 8405D+, 8410D, 8405D, 8411D • 9404, 9408, 9601, 9601+, 9610, 9620, 9621, 9608, 9611, 9630, 9640, 9641, 9650 The valid options are: • **No**: The default setting and does not change the callr-info interactions with the connected phone. • **Yes**: Activates the enhanced Callr-info operation including the application of the existing feature related system parameters. Clear Callr-Info option

Table continues…

Field/Button	Description
	settings of leave-ACW, next-call and on-call-release. If the **callr-info** button is not assigned to the phone on the station form, **Enhanced Callr-Info display for 1-line phones** does not apply.
Delete Endpoint on Unassign of Endpoint from User or on Delete User	The option to specify whether to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.
Override Endpoint Name	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: CS 1000 Endpoint Profile

Field	Description
System	The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.
Add new	The option to create a new phone.
Target	The system customer number for the CS 1000 system. You must select the target. The system displays the field only if you select **Add new**.
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. You must select the template. The system displays the field only if you select **Add new**.
Update	Updates the station profile information for the user. When you click **Update**, the system takes you to the element manager cut-through for the updates.

Table continues…

Field	Description
Service Details	The service details of endpoints, such as set type, after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values for this field. The system displays the field only if you select **Add new**.
Terminal Number	The terminal number of the phone. The system displays the field only if 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.

Field	Description
System	The messaging system on which you add the subscriber. You must select the system.
Use Existing Subscriber on System	The option to specify whether to use an existing subscriber mailbox number to associate with this profile.
Mailbox Number	The mailbox number of the subscriber. You must select the mailbox number. The field takes the existing mailbox number that you associate with this profile. This value in the field is valid only if you select the **Use Existing Subscriber on System** check box.
Messaging Editor	Click to start the Messaging application where you can edit or view details of the profile of the messaging endpoint. After you save the changes in the Messaging system, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.

Table continues…

Field	Description
Template	The system-defined or user-defined template that you associate with the subscriber.
Password	The password for logging in to the mailbox. You must provide the password.
Delete Subscriber on Unassign of Subscriber from User or on Delete User	The option to specify whether to delete the subscriber mailbox from the Messaging device or Communication System Management when you remove this Messaging profile or when you delete the user.

Communication Profile tab: CallPilot Messaging Profile

Field	Description
System	The CallPilot system to which you add a mailbox. You must select the system.
Target	The field that maps to the CallPilot **Location** field. CallPilot Manager provides the **Target** field. You must select the target.
Template	The mailbox template that you use. Select a template from the drop down list. The element manager maintains all the mailbox templates. You must select the template.
Update	Updates the mailbox information for the user. If you click the **Update** button, the system cuts through to the element manager for the updates.
Service Details	Displays mailbox service details from the endpoint after you create the mailbox.
Mailbox Number	The mailbox number or the extension DN of the user. You must select the mailbox number.

Communication Profile tab: IP Office Endpoint Profile

Use this profile to assign a new or an existing user to a System Manager device in User Management.

While adding a user, if you choose to assign a CM endpoint profile and an IP Office endpoint profile to the user, then the system uses the IP Office endpoint profile as the survivability option for the CM endpoint profile. That is, the endpoint extension used in the CM endpoint profile is also used for creating an IP Office endpoint profile so that when Communication Manager is unavailable, the IP Office device can serve the extension.

Note:

If a Communication Manager endpoint profile is present while adding or editing a user, the user administration functions in the centralized mode. If a Communication Manager endpoint profile is present, the user administration functions in the distributed mode.

Before you add an IP Office endpoint profile for a centralized user, commit the changes to the Communication Manager endpoint profile and the Session Manager endpoint profile.

Field/Button	Description
System	The list of IP Office device names from which you can select the IP Office device that you associate with the user. You must select the template.
Template	The list of user templates from which you can select your preferred template to set the user configurations. You must select the template.
Use Existing Extension	Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint you associate with. You must select the extension. The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.
Endpoint Editor	Starts the IP Office application where you can edit or view the details of the IP Office endpoint. After you save the changes in the IP Office manager, the system updates the modified data on the device or database only when you commit the changes on the User Profile Edit page.
Module-Port	The module port combination list for IP Office analog extensions. You must select **Module-Port** for centralized users with Set Type as **Analog**.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the system populates the set type.
Delete Extension On User Delete	The option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with **Analog** and **Digital** set types.

Communication Profile tab: Presence Profile

You can create Presence profiles only for the default communication profile.

Field	Description
System	Selects the Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile: • Aggregate presence

Table continues…

Field	Description
	• Archive instant messages if the Instant Messages option is enabled
SIP Entity	The field used to route SIP based messages through the Presence Services This system selects the SIP entity only if you select a Presence Services instance in the **System** field. **SIP Entity** is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.
IM Gateway	The IP address of the IM gateway.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with the AES Collector. The options are: • **System Default** • **Off** • **On** The default is **System Default**. You can change the default value. You do not require to configure AES Collector in the Presence Services server.

Communication Profile tab: Conferencing Profile

Field	Description
Select Auto-generated Code Length	The number of characters in PIN. The default is 6. The system displays this field if you select the **Auto Generate Participant and Moderator Security Code** check box.
Auto Generate Participant and Moderator Security Code	Select the check box if the system must generate the participant security code and moderator security code for this user. Clear the check box to assign a specific participant security code or moderator security code for this user.
Participant Security Code	The participant security code that you assign for this user. The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Moderator Security Code	The moderator security code that you assign for this user.

Table continues…

Field	Description
	The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Location	The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users. For SIP users, the system uses the location value from the **Home Location** field in the Session Manager profile.
Template	The Conferencing template that you assign to this user.

Button	Description
Get Templates	Displays the list of Conferencing templates that you can assign to this user.

Membership tab: Roles

Field	Description
Select check box	Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account.
Name	The name of the role.
Description	A brief description about the role.

Button	Description
Assign Roles	Displays the Assign Role page that you can use to assign the roles to the user account.
Unassign Roles	Removes the selected role from the list of roles associated with the user account.

Membership tab: Group Membership

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

Button	Description
Add To group	Displays the Assign Groups page that you can use to add the user to a group.
Remove From Group	Removes the user from the selected group.

Contacts tab: Default Contact List

Field	Description
Description	A brief description of the contact list.

Contacts tab: Associated Contacts

Field	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Scope	The categorization of the contact based on whether the contact is a public or private contact.
Speed Dial	The value specifies whether the speed dial is set for the contact or not.
Speed Dial Entry	The reduced number that represents the speed dial number.
Presence Buddy	The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you cannot track the presence of the contact.

Button	Description
Edit	Displays the Edit Contact List Member page. Use this page to modify the information of the selected contact.
Add	Displays the Attach Contacts page. Use this page to select one or more contacts from the list of contacts. In the Multi Tenancy environment, when the tenant administrator of a tenant creates or updates the user, the administrator can attach only the following contacts: • Private contacts of the user • Public contacts • Users who belong to that tenant
Remove	Removes one or more selected contacts from the list of the associated contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.

Table continues…

Button	Description
Filter: Enable	Displays the text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab: Private Contacts

Use this section to add new private contacts, and edit and delete the existing contacts.

Field	Description
Last Name	The last name of the private contact.
First Name	The first name of the private contact.
Display Name	The display name of the private contact.
Contact Address	The address of the private contact.
Description	A brief description about the contact.

Button	Description
Edit	Displays the Edit Private Contact page. Use this page to edit the information of the contact you selected.
New	Displays the **New Private Contact** page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Commit & Continue	Creates the user account in the database and retains you on the same page for further modifications.
Commit	Creates the user account and takes you to the User Management page.
Cancel	Cancels the user creation operation.

Related Links

Adding users on page 99

User Profile Edit field descriptions

Organization

Field	Description
Tenant	The name of the tenant that you must select.
Level 1	The name of the level 1 hierarchy of the tenant organization. For example, Site. The tenant administrator provides the hierarchy on the Tenant Management page.
Level 2	The name of the level 2 hierarchy of the tenant organization. For example, Department.
Level 3	The name of the level 3 hierarchy of the tenant organization. For example, Team.

Note:

You cannot edit the tenant. If you select a different level 1 for the tenant from the organization hierarchy, the **Level 2** and **Level 3** fields become blank. You can select new values for level 2 and level 3. If you select a different level 2 for the tenant from the organization hierarchy, the **Level 3** field becomes blank. You can select a new value for level 3.

User Provisioning Rule

Name	Description
User Provisioning Rule	The user provisioning rule that you must edit.

Identity tab — Identity section

Name	Description
Last Name	The last name of the user. For example, Miller.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the end points. For example, Miller. Typically, the name is the written or spoken language of the user.
First Name	The first name of the user. For example, John.
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Status	The login status of the user

Table continues…

Name	Description
Update Time	The time when the user details were last modified.
Login Name	The login name of the user. The login name is not case-sensitive. For example, if you enter JMILLER@AVAYA.COM, the system converts the login name to lowercase, that is, jmiller@avaya.com. However, on the login page, you can enter JMILLER@AVAYA.COM or jmiller@avaya.com. The login name can be in uppercase or lowercase. If you log in to the system as admin, you cannot edit the login name. **Note:** To create the user data by using a blank excel template, append the login name with #ProfileSetName in all worksheets except Basic and Profile Set. The system associates the user records with the communication profile that you have provided. For example, jmiller@avaya.com#ProfileSetName.
Authentication Type	The type of authentication that defines how the system performs the authentication of the user. The options are: • **Enterprise**: Directory servers that are external to System Manager authenticate the user login. • **Basic**: Avaya authentication service authenticates the user login. For bulk import of users by using Excel, **Authentication Type** is always Basic. Therefore, the **Authentication Type** field remains invisible in the Excel file.
Change Password	The new password. The selection is required.
Source	The entity that created this user record. The possible values for this field is either an IP Address/Port, or a name representing an enterprise LDAP, or Avaya.
Localized Display Name	The localized display name of a user. The name is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. The display name supports displays that cannot handle localized text, for example, some endpoints.
Title	The personal title that is set to address a user. The title is typically a social title and not the work title. For example, Mr.

Table continues…

Name	Description
Language Preference	The preferred written or spoken language of the user. For example, English.
Time Zone	The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.
Employee ID	The employee number for the user. For example, 20081234.
Department	The department to which the user belongs. For example, Human Resources.
Company	The organization where the user works. For example, Avaya Inc.

Identity tab — Address section

Name	Description
Time Zone	The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.
Department	The department to which the user belongs. For example, Human Resources.
Address Type	The type of address. The values are: • **Office** • **Home**
Street	The name of the street. For example, Magarpatta.
City	The name of the city or town. For example, Pune.
Postal Code	The postal code used by postal services to route mail to a destination. For example, 411028. For United States, the postal code is the Zip code.
Province	The full name of the province. For example, Maharashtra.
Country	The name of the country. For example, India.

Button	Description
New	Displays the Add Address page. Use the page to add the address details.
Edit	Displays the Edit Address page. Use the page to modify the address.
Delete	Deletes the selected address.
Choose Shared Address	Displays the Choose Address where you choose a shared or common address.

Identity tab — Localized Names section

Name	Description
Language	The localized languages for displaying the user name. For example, English. You must select the language.
Display Name	The user name in the localized language you choose. For example, John Miller.

Button	Description
New	Displays fields that you can use to create a new localized name for the user.
Edit	Displays fields that you can use to modify the localized name for the user.
Delete	Deletes the localized names that you select for the user.
Add	Adds or edits the localized name for the user.
Cancel	Cancels the addition or edits of the localized name.

Communication Profile tab — Communication Profile

Use this section to create, modify, and delete a communication profile of the user. Each communication profile can contain one or more communication addresses for a user.

Name	Description
Communication Profile Password	The communication profile password. The field is available only if you enable the communication profile. The password policy is configured from **Users** > **User Management** > **Communication Profile Password Policy**.
Option button	The option to view the details of the selected communication profile.
Name	The name of the communication profile. You must select the name.

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Done	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding of a communication profile.

The system enables the following fields when you click **New** in the Communication Profile section.

Name	Description
Name	The name of the communication profile for the user.
Default	The profile that is made default as the active profile. There can be only one active profile at a time.

Communication Profile tab — Communication Address

Use this section to create, modify, and delete the communication address of a user. Each communication profile can contain one or more communication addresses for a user.

Name	Description
Type	The type of the handle.
Handle	A unique communication address of the user.
Domain	The name of the domain with which the handle is registered.

Button	Description
New	The fields for adding a new communication address.
Edit	The button to edit the information of a selected communication address.
Delete	Deletes the selected communication address.

The page displays the following fields when you click **New** or **Edit** in the Communication Address section.

Name	Description
Type	The type of the handle. The different types of handles are: • **Avaya SIP**: Indicates that the handle supports Avaya SIP-based communication. • **Avaya E.164**: Indicates that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix. • **Microsoft SIP**: Indicates that the handle supports SIP-based communication. • **Microsoft Exchange**: Indicates that the handle is an email address and supports communication with Microsoft SMTP server. • **Lotus Notes**: Indicates that the handle is for Lotus Notes and domino calender. • **IBM Sametime**: Indicates that the handle is for IBM Sametime. The address must be in the DN=IBMHandle format.

Table continues…

Name	Description
	• **Avaya Presence/IM**: Indicates that the handle is an address used for Extensible Messaging and Presence Protocol (XMPP)-based Internet Messaging (IM) services, and XMPP or Session Initiation Protocol-based (SIP) Presence services. • **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.
Fully Qualified Address	The fully qualified domain name or uniform resource identifier. The address can be an email address, IM user, or an address of a communication device by using which the user can send or receive messages. You must provide the fully qualified address.

Button	Description
Add	Saves the new communication address or modified communication address information in the database.
Cancel	Cancels the addition of communication address.

Communication Profile tab:— Session Manager

Note:

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

Name	Description
Primary Session Manager	The instance that you want to use as the home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura® network. You must select the primary Session Manager server.
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager provides continued service to SIP devices associated with this

Table continues…

Name	Description
	communication profile when the primary Session Manager server becomes unavailable. A selection is optional.
Survivability Server	For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile when the local connectivity to Session Manager instances in Avaya is lost. If you select a Branch Session Manager , and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional. **Note:** If a termination or origination application sequence contains a Communication Manager application, the Communication Manager instance associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.
Block New Registration When Maximum Registrations Active	If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint.
Origination Application Sequence	The application sequence that the system will invoke when routing the calls from this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.

Table continues…

Name	Description
Termination Application Sequence	The application sequence that will be invoked when the system routes the calls to this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Home Location	The home location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any of the location. You must specify a value.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.

Communication Profile tab: Collaboration Environment Profile

Field	Description
Service Profile	The profile that you assign to the user. The user can gain access to the service contained in the profile.

Communication Profile tab — CM Endpoint Profile

Note:

The system displays these fields only if a CM Endpoint profile exists for the user.

Name/Button	Description
System	The Communication Manager system on which you add the endpoint. You must select the system.
Profile Type	The type of the Communication Manager Endpoint profile that you create. You must select the profile type.
Use Existing Endpoints	Select the check box to use the existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint that you associate this profile with. You must select the extension.

Table continues…

Name/Button	Description
	The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.
Template	The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add. You must select the template.
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. You must select the port. The field lists the possible ports based on the selected set type.
Voice Mail Number	The voice mail number of the endpoint you associate with.
Preferred Handle	Numeric only handles, SIP handles,or nonSIP handles, that are administered for a user. The **Preferred Handle** field is optional. By default, the field is blank. If the SIP entity is of the Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
Enhanced Callr-Info display for 1–line phones	The option to activate the enhanced Callr-info operation on the phone. The **Enhanced Callr-Info display for 1-line phones** field on the station form is valid for the following set types: • 1603, 1608, 1616, 1408, 1416 • 2402, 2410, 2420 • 4606, 4612, 4612CL, 4624, 4602, 4602+, 4630, 4610, 4622, 4620, 4621, 4625, • 6402D, 6408D, 6408D+, 6416D+, 6424D+, 607A1 • 7506D, 7507D • 8405D+, 8410D, 8405D, 8411D • 9404, 9408, 9601, 9601+, 9610, 9620, 9621, 9608, 9611, 9630, 9640, 9641, 9650

Table continues…

Name/Button	Description
	The valid options are: • **No**: The default setting and does not change the callr-info interactions with the connected phone. • **Yes**: Activates the enhanced Callr-info operation including the application of the existing feature related system parameters. Clear Callr-Info option settings of leave-ACW, next-call and on-call-release. If the **callr-info** button is not assigned to the phone on the station form, **Enhanced Callr-Info display for 1-line phones** does not apply.
Delete Endpoint on Unassign of Endpoint from User or on Delete User	The option to specify whether to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.
Override Endpoint Name	The option to override the following endpoint names: • The endpoint name on Communication Manager with the value you configured on the Manage Users page during synchronization. If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization. • The localized display name on the Manage Users page in the **Localized Display Name** field of Communication Manager. If you clear the check box, the system does not override the localized display name in the **Localized Display Name** field.

Communication Profile tab - CS1000 Endpoint Profile

Field	Description
System	The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.
Target	The system customer number for the CS 1000 system. You must select the target. The system displays the field only if you select **Add new**.
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. You must select the template.

Table continues…

Field	Description
	The system displays the field only if you select **Add new**.
Update	Updates the station profile information for the user. When you click **Update**, the system takes you to the element manager cut-through for the updates.
Service Details	The service details of endpoints, such as set type, after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values for this field. The system displays the field only if you select **Add new**.
Include in Corporate Directory	The option to add this profile to the CS 1000 Corporate Directory feature.

Communication Profile tab — Messaging Profile

Note:

The system displays the following fields only if you can configure a messaging profile for the user.

Name	Description
System	The messaging system on which you add the subscriber. You must select the system.
Use Existing Subscriber on System	The option to specify whether to use an existing subscriber mailbox number to associate with this profile.
Mailbox Number	The mailbox number of the subscriber. You must select the mailbox number. The field takes the existing mailbox number that you associate with this profile. This value in the field is valid only if you select the **Use Existing Subscriber on System** check box.
Messaging Editor	Click to start the Messaging application where you can edit or view details of the profile of the messaging endpoint. After you save the changes in the Messaging system, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Template	The system-defined or user-defined template that you associate with the subscriber.
Password	The password for logging in to the mailbox. You must provide the password.

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 when you delete the user.

Communication Profile tab - CallPilot Messaging Profile

Field	Description
System	The CallPilot system of the messaging profile you edit. The selection is required.
Target	The field that maps to the CallPilot **Location** field. CallPilot Manager provides the **Target** field. You must select the target.
Template	The mailbox template that you use. Select a template from the drop down list. The element manager maintains all the mailbox templates. You must select the template.
Update	Updates the mailbox information for the user. If you click the **Update** button, the system cuts through to the element manager for the updates.
Service Details	Displays mailbox service details from the endpoint after you create the mailbox.
Mailbox Number	The mailbox number or the extension DN of the user. You must select the mailbox number.

Communication Profile tab — IP Office Endpoint Profile

Use this profile to assign a new or an existing user to a System Manager device in User Management.

While adding a user, if you choose to assign a CM endpoint profile and an IP Office endpoint profile to the user, then the system uses the IP Office endpoint profile as the survivability option for the CM endpoint profile. That is, the endpoint extension used in the CM endpoint profile is also used for creating an IP Office endpoint profile so that when Communication Manager is unavailable, the IP Office device can serve the extension.

Note:

If a Communication Manager endpoint profile is present while adding or editing a user, the user administration functions in the centralized mode. If a Communication Manager endpoint profile is present, the user administration functions in the distributed mode.

Commit the Communication Manager endpoint profile and the Session Manager endpoint profile before you add an IP Office endpoint profile for a centralized user.

Name/Button	Description
System	The list of IP Office device names from which you can select the IP Office device that you associate with the user. You must select the template.
Template	The list of user templates from which you can select your preferred template to set the user configurations.
Use Existing Extension	Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Endpoint Editor button	The option to start the IP Office application, where you can edit or view the details of the IP Office endpoint. After you save the changes in IP Office manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Extension	The extension of the endpoint you associate with. You must select the extension. The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.
Module-Port	The module port combination list for IP Office analog extensions. You must select **Module-Port** for centralized users with Set Type as **Analog**.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the system populates the set type.
Delete Extension On User Delete	The option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with **Analog** and **Digital** set types.

Communication Profile tab — Presence Profile

Note:

Name	Description
System	Selects the Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the

Name	Description
	Presence Services instance can perform the following for the communication profile: • Aggregate presence • Archive instant messages if the Instant Messages option is enabled

Communication Profile tab: Conferencing Profile

Field	Description
Select Auto-generated Code Length	The number of characters in PIN. The default is 6. The system displays this field if you select the **Auto Generate Participant and Moderator Security Code** check box.
Auto Generate Participant and Moderator Security Code	Select the check box if the system must generate the participant security code and moderator security code for this user. Clear the check box to assign a specific participant security code or moderator security code for this user.
Participant Security Code	The participant security code that you assign for this user. The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Moderator Security Code	The moderator security code that you assign for this user. The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Location	The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users. For SIP users, the system uses the location value from the **Home Location** field in the Session Manager profile.
Template	The Conferencing template that you assign to this user.

Button	Description
Get Templates	Displays the list of Conferencing templates that you can assign to this user.

Membership tab — Roles

Name	Description
Select check box	Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account.
Name	The name of the role.
Description	A brief description about the role.

Button	Description
Assign Roles	Displays the Assign Role page that you can use to assign the roles to the user account.
Unassign Roles	Removes the selected role from the list of roles associated with the user account.

Membership tab — Group Membership

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

Button	Description
Add To group	Displays the Assign Groups page that you can use to add the user to a group.
Remove From Group	Removes the user from the selected group.

Contacts tab — Default Contact List

Name	Description
Description	A brief description of the contact list.

Contacts tab — Associated Contacts

Name	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Scope	The categorization of the contact based on whether the contact is a public or private contact.
Speed Dial	The value specifies whether the speed dial is set for the contact or not.

Table continues…

Name	Description
Speed Dial Entry	The reduced number that represents the speed dial number.
Presence Buddy	The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you cannot track the presence of the contact.

Button	Description
Edit	Displays the Edit Contact List Member page. Use this page to modify the information of the selected contact.
Add	Displays the Attach Contacts page. Use this page to select one or more contacts from the list of contacts. In the Multi Tenancy environment, when the tenant administrator of a tenant creates or updates the user, the administrator can attach only the following contacts: • Private contacts of the user • Public contacts • Users who belong to that tenant
Remove	Removes one or more selected contacts from the list of the associated contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Displays the text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab — Private Contacts

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

Name	Description
Last Name	The last name of the private contact.
First Name	The first name of the contact.
Display Name	The display name of the private contact.
Contact Address	The address of the private contact.
Description	A brief description about the contact.

Button	Description
Edit	Displays the Edit Private Contact page. Use this page to edit the information of the contact you selected.
New	Displays the **New Private Contact** page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Commit & Continue	Saves your changes and retains you on the same page for further modifications.
Commit	Modifies the user account and takes you back to the User Management or User Profile View page. **Note:** While restoring a deleted user, use the **Commit** button to restore a deleted user.
Cancel	Cancels the operation of modifying the user information and takes you back to the User Management or User Profile View page.

Related Links

Modifying user accounts on page 119

User Profile View field descriptions

Use this page to view the details of the selected user account.

The User Profile View page has the following four tabs:

- **Identity**
- **Communication Profile**
- **Membership**
- **Contacts**

Organization

Field	Description
Tenant	The name of the tenant that you must select.
Level 1	The name of the level 1 hierarchy of the tenant organization. For example, Site. The tenant administrator provides the hierarchy on the Tenant Management page.
Level 2	The name of the level 2 hierarchy of the tenant organization. For example, Department.
Level 3	The name of the level 3 hierarchy of the tenant organization. For example, Team.

User Provisioning Rule

Field	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 end points. For example, Miller. Typically, the name is the written or spoken language of the user.
First Name	The first name of the user. For example, John.
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Status	The login status of the user.
Update Time	The time when the user details were last modified.
Login Name	The unique system login name given to the user. The login name takes the form of

Table continues…

Name	Description
	username@domain. You use the login name to create the user's primary handle. The login name is not case-sensitive. For example, if you enter JMILLER@AVAYA.COM, the system converts the login name to lowercase, that is, jmiller@avaya.com. However, on the login page, you can enter JMILLER@AVAYA.COM or jmiller@avaya.com. The login name can be in uppercase or lowercase. You cannot edit the **Login Name** field for users with the login name admin.
Authentication Type	Authentication type defines how the system performs user authentication. The options are: • **Enterprise**: The enterprise authenticates the user login. • **Basic**: Avaya Authentication Service authenticates the user login.
Source	Specifies 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. 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

Table continues…

Name	Description
	• Home
Street	The name of the street.
City	The name of the city or town.
Postal Code	The postal code used by postal services to route mail to a destination. In United States, this is Zip code.
Province	The full name of the province.
Country	The name of the country.

Identity tab — Localized Names section

Name	Description
Language	The localized languages for displaying the user name.
Display Name	The user name in the localized language you choose.

Button	Description
New	Allows you to add a new localized name for the user.
Edit	Allows you to edit the localized name for the user.
Delete	Deletes the localized names you select for the user.
Add	Adds or edits the localized name for the user.
Cancel	Cancels your add or edit of the localized name.

Communication Profile tab — Communication Profile

Use this section to create, modify, and delete a communication profile of the user. Each communication profile can contain one or more communication addresses for a user.

Name	Description
Communication Profile Password	The communication profile password. The field is available only if you enable the communication profile. The password policy is configured from **Users** > **User Management** > **Communication Profile Password Policy**.
Option button	The option to view the details of the selected communication profile.
Name	The name of the communication profile. You must select the name.

Button	Description
New	Creates a new communication profile for the user.

Table continues…

Button	Description
Delete	Deletes the selected communication profile.
Done	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding of a communication profile.

The system enables the following fields when you click **New** in the Communication Profile section.

Communication Profile tab — Communication Address section

Name	Description
Type	The type of the handle.
Handle	The unique communication address for the user.
Domain	The name of the domain with which the handle is registered.

Communication Profile tab — Session Manager section

Note:

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

Name	Description
Primary Session Manager	The Session Manager instance that you use as home server for the currently displayed communication profile. As a home server, the selected primary Session Managerinstance is used as the default access point to connect devices that are associated with the communication profile to the Avaya network. A selection is required.
Secondary Session Manager	If you select a secondary Session Manager instance, this Session Manager provides continued service to SIP devices associated with this Communication Profile when the primary Session Manager becomes unavailable. A selection is optional.
Survivability Server	For local survivability, a Survivability Server 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 Avaya Aura® 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

Table continues…

Name	Description
	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, the Communication Manager associated with the application must be the main Communication Manager 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 using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.
Block New Registration When Maximum Registrations Active	If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint.
Origination Application Sequence	An application sequence that will be invoked when the system routes the calls from this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Termination Application Sequence	An application sequence that will be invoked when calls are routed to this user. A selection is optional. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities.

Table continues…

Name	Description
	Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.
Home Location	The location that Session Manager uses when the IP address of the calling phone does not match any IP address pattern of any location. This field is specified to support mobility of the user.

Communication Profile tab: Collaboration Environment Profile

Field	Description
Service Profile	The profile that you assign to the user. The user can gain access to the service contained in the profile.

Communication Profile tab — CM Endpoint Profile

Note:

The system displays these fields only if a CM Endpoint profile exists for the user.

Name/Button	Description
System	The Communication Manager on which you add the endpoint. The Communication Manager system on which you add the endpoint. You must select the system.
Profile Type	The type of the profile for the user.
Extension	The extension of the endpoint that you associate this profile with. You must select the extension.
View Endpoint	Lists the existing or available endpoints based on check box status of the **Use Existing Endpoints** field.
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. You must select the port.
Voice Mail Number	The voice mail number of the endpoint you associate with.
Preferred Handle	Numeric only handles, SIP handles,or nonSIP handles, that are administered for a user. The **Preferred Handle** field is optional. By default, the field is blank.

Table continues…

Name/Button	Description
	If SIP entity is of the Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
Enhanced Callr-Info display for 1–line phones	The option to activate the enhanced Callr-info operation on the phone. The **Enhanced Callr-Info display for 1-line phones** field on the station form is valid for the following set types: • 1603, 1608, 1616, 1408, 1416 • 2402, 2410, 2420 • 4606, 4612, 4612CL, 4624, 4602, 4602+, 4630, 4610, 4622, 4620, 4621, 4625, • 6402D, 6408D, 6408D+, 6416D+, 6424D+, 607A1 • 7506D, 7507D • 8405D+, 8410D, 8405D, 8411D • 9404, 9408, 9601, 9601+, 9610, 9620, 9621, 9608, 9611, 9630, 9640, 9641, 9650 The valid options are: • **No**: The default setting and does not change the callr-info interactions with the connected phone. • **Yes**: Activates the enhanced Callr-info operation including the application of the existing feature related system parameters. Clear Callr-Info option settings of leave-ACW, next-call and on-call-release. If the **callr-info** button is not assigned to the phone on the station form, **Enhanced Callr-Info display for 1-line phones** does not apply.
Delete Endpoint on Unassign of Endpoint from User or Delete User	The option to specify whether to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or when you delete the user.
Override Endpoint Name	Use this check box for the following two purposes: • To override the endpoint name on Communication Manager with the value you configured on the Manage Users page during synchronization. If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization.

Table continues…

Name/Button	Description
	• To override the Localized Display Name on the Manager Users page on the **Localized Display Name** field of Communication Manager. If you clear the check box, the system does not override the Localized display name in the **Localized Display Name** field.

Communication Profile tab - CS1000 Endpoint Profile

Field	Description
System	The CS1000 system of the station you view.
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	Select this check box to add this profile to the CS1K 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.
Template	The template, system-defined or user-defined, that you associate with the subscriber.
Mailbox Number	The mailbox number of the subscriber.
Password	The password for logging on to the mailbox.
Delete Subscriber on Unassign of Subscriber from User	Provides the option to specify whether to delete the subscriber mailbox from the Messaging device or Communication System Management when you remove this messaging profile or when you delete the user.

Communication Profile tab - CallPilot Messaging Profile

Field	Description
System	The CallPilot system of the mailbox to view.
Location	This field maps to the CallPilot Location field. CallPilot Manager provides the **Location** field.
Template	The mailbox template you apply. Select a template from the drop down list. The element manager maintains all the mailbox templates.
Update	Updates the mailbox information for the user. If you click **Update**, the system cuts through to the element manager for the updates.
Service Details	Displays mailbox service details from endpoint after you create the mailbox.
Mailbox Number	Mailbox number or the extension DN of the user.

Communication Profile tab — IP Office Endpoint Profile

Use this profile to assign a new or an existing user to a System Manager device in User Management.

While adding a user, if you choose to assign a CM endpoint profile and an IP Office endpoint profile to the user, then the system uses the IP Office endpoint profile as the survivability option for the CM endpoint profile. That is, the endpoint extension used in the CM endpoint profile is also used for creating an IP Office endpoint profile so that when Communication Manager is unavailable, the IP Office device can serve the extension.

Note:

If a Communication Manager endpoint profile is present while adding or editing a user, the user administration functions in the centralized mode. If a Communication Manager endpoint profile is present, the user administration functions in the distributed mode.

Commit the Communication Manager endpoint profile and the Session Manager endpoint profile before you add an IP Office endpoint profile for a centralized user.

Name/Button	Description
System	The list of IP Office device names from which you can select the IP Office device you associate with the user.
Template	The list of user templates from which you can select your preferred template to set the user configurations.
Use Existing Extension	Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint you associate.

Table continues…

Name/Button	Description
	The field lists the endpoints, existing or available, based on option you selected in the **Use Existing Endpoints** check box.
Endpoint Editor button	Starts the IP Office application, where you can edit or view the details of the IP Office endpoint. After you save the changes in IP Office manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Module-Port	The module port combination list for IP Office analog extensions. You must select **Module-Port** for centralized users with Set Type as **Analog**.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the set type is auto populated.
Delete Extension On User Delete check box	Provides the option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with **Analog** and **Digital** set types.

Communication Profile tab — Presence Profile

Name	Description
System	Selects the Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile: • Aggregate presence • Archive instant messages if the Instant Messages option is enabled
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with the AES Collector. The options are: • **System Default** • **Off** • **On** The default is **System Default**. You can change the default value. You do not require to configure AES Collector in the Presence Services server.

Communication Profile tab: Conferencing Profile

Field	Description
Select Auto-generated Code Length	The number of characters in PIN. The default is 6. The system displays this field if you select the **Auto Generate Participant and Moderator Security Code** check box.
Auto Generate Participant and Moderator Security Code	Select the check box if the system must generate the participant security code and moderator security code for this user. Clear the check box to assign a specific participant security code or moderator security code for this user.
Participant Security Code	The participant security code that you assign for this user. The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Moderator Security Code	The moderator security code that you assign for this user. The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Location	The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users. For SIP users, the system uses the location value from the **Home Location** field in the Session Manager profile.
Template	The Conferencing template that you assign to this user.

Button	Description
Get Templates	Displays the list of Conferencing templates that you can assign to this user.

Membership tab — Roles section

Name	Description
Name	The name of the role.
Description	A brief description about the role.

Membership tab — Group Membership section

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

Contacts tab — Default Contact List section

Name	Description
Description	A brief description of the contact list.

Contacts tab — Associated Contacts section

Name	Description
Last Name	The last name of the contact.
First Name	The first name of the contact.
Scope	The categorization of the contact based on whether the contact is a public or private contact.
Speed Dial	The value that specifies whether the speed dial is set for the contact.
Speed Dial Entry	The reduced number that represents the speed dial number.
Presence Buddy	The value that specifies whether you can monitor the presence information of the contact or not. **False** indicates that you cannot track the presence of the contact.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab — Private Contacts section

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

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

Table continues…

Name	Description
Contact Address	The address of the private contact.
Description	A brief description about the contact.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Edit	Opens the User Profile Edit page. Use the User Profile Edit page to modify the details of the user account.
Done	Closes the User Profile View page and takes you back to the User Management page.

Related Links

Viewing details of a user on page 119

User Delete Confirmation field descriptions

Use this page to delete an user account.

Name	Description
Last Name	Displays the last name of the user.
First Name	Displays the first name of the user.
Display Name	Displays the localized display name of a user. It is typically the localized full name.
Login Name	Displays the login name of the you want to delete.
Last login	Displays the date and time of last successful login on to System Manager.

Button	Description
Delete	Deletes a user.
Cancel	Closes the User Delete Confirmation page and takes you back to the User Management page.

Chapter 7: Session Manager routing

Session Manager routes session creation requests from one server to another server, based on the address specified in the session creation request.

The addresses, which specify the identity of the destination of a session creation request, are in the form of a SIP Uniform Resource Identifier (URI). This identifier consists of a user part and a domain part.

- The user part is an alphanumeric string or handle. Session Manager has special rules for efficiently routing and manipulating handles that consist of digits, for example, telephone numbers.
- The domain part is specified as a DNS domain.

Session Manager uses both parts of the identifier in its routing decisions.

The servers that send the session creation requests to Session Manager are called SIP entities. Session Manager routes these requests to other SIP entities, based on the administered routing rules.

Session Manager associates SIP entities with specific locations and can make different routing decisions based on the location from which a session creation request arrives.

Prerequisites for routing setup

This section assumes that the following requirements are met:

- System Manager is installed.
- All Session Manager instances are installed.

For more information on installation, see *Deploying Avaya Aura® Session Manager*.

Routing

Routing enables the system to identify which SIP entity should receive a call based on the configured dial pattern or regular expression. Administrators can use routing to administer Session Manager instances and related routing policies. Routing policies define how Session Manager

routes calls between different SIP network elements. The configuration data is distributed from the Routing database to each remote Session Manager instance.

All calls originate either from an administered user of the system or a SIP entity.

Locations are used for origination-based routing and for specifying bandwidth for call admission control.

Session Manager Routing allows administrators to define routing:

- by combining several locations.
- by combining several dial patterns and domains.
- for several ToD and rankings.
- for a single routing destination.

Call routing using routing policy data

1. Session Manager tries to match the domain to one of the authoritative domains.
2. If Session Manager is authoritative for the domain, then the Session Manager tries to match the digit pattern.
3. If a digit pattern is not matched, Session Manager tries to use the regular expression table.
4. If no regular expression match is found, Session Manager sends the request to a Session Manager-provisioned outbound proxy.
5. If no outbound proxy has been administered for the Session Manager and Session Manager is not authoritative for the domain then Session Manager routes the request to the destination in the request-URI. If the request-URI does not contain an IP address, then Session Manager uses DNS or the Local Host Name Resolution table to determine where to route the request.
6. If the hostname cannot be resolved to an IP address, the call fails.

Handling SIP responses

The following table describes how Session Manager handles SIP responses.

Table 6: Handling SIP responses

Response	Session Manager action
2xx	Session Manager completes a call.
3xx 422	Session Manager sends a response to the caller.

Table continues…

Response	Session Manager action
423 484 5xx (other than 501-504) 6xx	
408 501 to 504	Session Manager maps an alternate IP address or entity link of a SIP entity to determine an alternate route for a call.
4xx (except 408)	Session Manager does not try to map the alternate IP addresses or entity link of a SIP entity to establish a call and tries to determine an alternate route for the call with another routing policy.

IP alternate routing and Call Admission Control

When sending a request, Session Manager sets the timer B or timer F value as specified in the destination SIP entity. If a SIP entity is administered with an FQDN, the Session Manager resolves the FQDN into a list of IP addresses using DNS or the local host name resolution table. The IP address of the final destination determines the egress location. The IP address is compared with IP address patterns on the Location Details page. If a location matches, the location is identified as the destination location. If no IP address pattern matches, the location that is administered on the destination SIP entity, if any, is identified as destination location.

If call admission control is administered for the location and the current request causes the number of allowed calls to be exceeded, the request is rejected with a 488 response. If timer B or timer F expires, Session Manager generates a 408 response to the request and other IP addresses for the same SIP entity are tried. When all IP addresses have been tried, Session Manager tries the next routing policy on the prioritized list.

Related Links

Session Manager SIP Entity Monitoring on page 502
SIP Responses to an OPTIONS Request on page 297

Administering initial setup of the Session Manager

About this task

Once you have completed the initial setup, you can modify the created entities or delete them, as required.

The recommended order for the initial set up of Session Manager using the System Manager routing screens is as follows.

Procedure

1. Accept or change default settings.
2. Create domains of type SIP.
3. Create locations.

4. Create adaptations.
5. Create SIP entities, some of which are routing destinations:
   - Create SIP entities that are used as Outbound Proxies, such as a particular Gateway or SIP Trunk.
   - Create other SIP entities.
   - Assign locations, adaptations, and Outbound Proxies to the SIP entities.
6. Create entity links:
   - Between Session Managers.
   - Between Session Managers and other SIP entities.
7. Create time ranges.

   Align with the tariff information received from the Service Providers.
8. Create routing policies.

   Assign the appropriate routing destination and Time Of Day. For Time Of Day, assign the appropriate time range and define the ranking.
9. Create dial patterns and assign the appropriate locations and routing policies to the dial patterns.
10. Create regular expressions and assign them to routing policies.
11. Create Session Manager instances using the Session Manager menus on the System Manager navigation pane.

Routing import and export Overview

Overview of exporting and importing routing element data

The Routing screens allow administering of the Session Manager SIP routing rules. The management screens consist of nine configurable elements.

You can import a very large number of the above elements in System Manager by using XML files. You can also export each of the elements or the entire routing configuration to XML files.

Pre-requisites:

- Ensure that System Manager is installed and the server is running.
- Ensure that the user performing the bulk import operation has administrative privileges.
- Before you import a large amount of data, back up the System Manager database. This backup will provide an easy way to restore the original database in case you find that the information you imported is substantially incorrect. Refer to the document *Administering Avaya Aura® System Manager* for details about this operation.
- Importing a very large number of elements (thousands and above) can take a very long time and can be CPU intensive to the System Manager server. This information also needs to be

synchronized with all the Session Managers. Therefore, perform large imports at a time where there is reduced platform activity in the network (for example, at night or during a maintenance window).

- When adding subcomponents to an existing element, include all parameters associated with that element in the import XML file. In other words, when you add digit patterns to an adaptation, ensure that the adaptation import includes all patterns and not just the ones being added to the adaptation.

FEATURES:

System Manager Routing Import/Export supports:

- Routing related data:
  - Domains
  - Locations
  - Adaptations
  - SIP Entities
  - Entity Links
  - Time Ranges
  - Routing Policies
  - Dial Patterns
  - Regular Expressions
- Importing each element separately as a single XML file containing many entries.
- Compressing the XMLs using ZIP compression in order to decrease the size of the files that need to be uploaded to the System Manager server.

  Note:

  This is especially important when importing large files of size exceeding 10 MB or more.
- Importing several elements or all the elements in a single ZIP file containing many XML files.
- Exporting a single type of entity or all the entities. When exporting all the entities, the exported files are contained in a single ZIP file.
- Since routing elements depend on each other, an import operation fails if the needed elements do not already exist in the database or exist in the same import operation. For example, import of a dial pattern with domain name *avaya.com* will fail if there is no such domain in the database, or if an XML file containing this domain is not imported in the same import operation as the dial pattern.
- When importing several entities together (either as a list of XML/ZIP files or inside a single ZIP file), System Manager imports these entities in the correct order to maintain dependencies. Because of this, it is possible, for example, to import SIP entities and entity links pointing to these SIP entities in the same import operation. The import order is always:

  1. Domains

2. Locations
3. Adaptations
4. SIP Entities
5. Entity Links
6. Time Ranges
7. Routing Policies
8. Dial Patterns
9. Regular Expressions

The order is decided by analyzing the internal structure of the files. Any file name can be used as long as its extension is *xml*.

- The Import operation does not halt if one of the elements fails validation. The failed element does not get added to the database, and the operation continues to the next one.
- An audit log provides details of the failed and successful import operations.
- If an imported element already exists in the System Manager database, which means that there is an element with the same unique identifiers, then the values in the new element will overwrite the old element.
  - For example: if a domain named *avaya.com* already exists in the database, then the note, type, and default values will be overwritten by the new element.
  - Dial Pattern is an exception for this rule. It is not possible to import a dial pattern with elements such as <digitpattern>,<maxdigits>,<mindigits>,<sipdomainName> and <routingoriginationName> already present in the database. Such an attempt will fail.
- Every operation in the routing application is logged to an audit log including the import operation. A log entry is added for each element that is imported, even if the operation succeeds or fails. The log is located at the following location:**`/var/log/Avaya/mgmt/nrp/nrpaudit.log`**. The file is accessible through the System Manager command prompt.

Note:

The routing elements depend on each other. An import operation fails if the needed elements do not already exist in the database or exist in the same import operation. For example, import of a dial pattern with domain name *avaya.com* will fail if there is no such domain in the database, or if an XML file containing this domain is not imported in the same import operation as the dial pattern.

Exporting Routing element data

Procedure

1. On the System Manager console, under **Elements**, click **Routing**.
2. Click **Routing** > ***<Any Routing element>***.
3. Select a check box for the entity to be exported from the list of entities on the screen.
4. From the Routing Entity screen, click **More Actions** > **Export *<Routing Element>***.

For example, to export adaptations, select **Routing** > **Adaptations**. From the Adaptations screen, select **More Actions** > **Export Adaptations**.

To export regular expressions, select **Routing** > **Regular Expressions**. From the Regular Expressions screen, click **More Actions** > **Export Regular Expressions**.

5. To export multiple routing elements, from the routing element screen, click **More Actions** > **Export all data**.

   The system packages the XML files in a zip file. The XML files conform to the XML schema definition that supports export of the element data.

Importing Routing element data

About this task

You must import element data as a ZIP file consisting of one or more XML files.

- Do not import data from the later stages in the routing definition process without importing data from the earlier stages. For example, you must import SIP entities either before or along with the relevant entity links.
- The import operation can accept XML files of any routing element. For example, you can import **Locations** from the Domains page.
- During the export operation, the XML files contain the following version information:

```
<buildNumber>0</buildNumber>
<implementationVersion>0</implementationVersion>
<specificationVersion>0</specificationVersion>
```

Procedure

1. On System Manager Web Console, click **Elements** > **Routing**.
2. In the left navigation pane, click **<Any Routing element>**.
3. To import routing elements, click **More Actions** > **Import**.
4. On the Import Routing Data page, click **Choose File** to select files that contain Routing data.
5. Perform the following operations to schedule an import job:
   - To begin the import operation immediately, click **Run immediately**.
   - To begin the import operation at the specified start time, click **Schedule later**.
6. Perform the following import job operations:
   - To delete a scheduled import job, select the job and click **Delete Job**.
   - To stop a running import job, select the job and click **Stop Job**.

   Note:

   In the **Import Job Status** section, you can view the job status of the import operation.

   If the import job contains errors, then the **Import Job Status** table provides a link to the failed import objects.
7. Click **Import** to start the import operation.

Import Routing Data page field descriptions

File Selection

Button	Description
Select File	Allows selecting files to import **<Any Routing element>** data.

Schedule

Name	Description
Run immediately	Begins import operation immediately after you click **Import**.
Schedule later	Begins import operation at the specified start time.

Import Job Status

Button	Description
Delete Job	Deletes an import job that is scheduled to run.
Stop Job	Stops an import job that is running.

Name	Description
Start Time	The start time of the import job.
Status	The status of the import job. Values are: 1. SUCCESSFUL 2. Waiting to run 3. Manually Stopped 4. FINISHED View errors in `/var/avaya/nrp`.
Files Processed	The number of files imported out of the total number of files.
Failed Entries	The number of errors encountered during the import operation.
Last Updated	The last update time of the import job.
Job Name	The name of the import job in the System Manager scheduler.

Button	Description
Import	Starts import operation of the **<Any Routing element>** data.

Saving configuration changes

About this task

When you make any configuration changes in Session Manager and click **Commit**, System Manager saves the data to the System Manager database. System Manager then synchronizes and distributes the data to all the Session Manager instances in the network. For example, renaming an adaptation changes the data on the SIP Entities Details screen, or changing dial pattern data also changes the data in the routing policy where that dial pattern is used.

Duplicating Routing entity data

About this task

You can use the **Duplicate** button on the relevant Session Manager Routing screens to duplicate routing entities. Duplication of data is useful if you want to create entities that are similar and want to rename these entities or copy an entity and make minimal changes to the entity attributes.

For example, you can duplicate a routing policy and then add the required dial pattern to the copy.

Domains

About Domains

The Domains screen is used to create a set of domains and sub-domains to enable an enterprise to use domain-based routing. This information is used to determine if a SIP user is part of the enterprise SIP network. Domains determine if the Session Manager Dial Plan can be used to route a particular call. Sub-domains are automatically checked if not provisioned. For example, Session Manager needs to check dial patterns for *avaya.com* if a request to *123@myserver.avaya.com* comes in and *myserver.avaya.com* is not administered as a domain.

Based on the corporate requirement, the administrator can create a SIP domain and sub-domains.

- Domain name can be `<organization-name.domain>`. For example, *avaya.com* or *abc.org*.
- Sub-domain can be named based on the geographical location or any other corporate requirements such as office location. For example, *us.avaya.com* and *fr.avaya.com* can be sub-domains for Avaya offices in the US and in France, or *dr.avaya.com* and *br.avaya.com* can be sub-domains for Avaya offices in Denver and in Basking Ridge.

Creating domains

Procedure

1. On System Manager Web Console, click **Elements** > **Routing**.
2. In the left navigation pane, click **Domains**.
3. Click **New**.
4. Enter the domain name and notes for the new domain or sub-domain.
5. Select **sip** as the domain type from the drop-down list.
6. Click **Commit**.

Related Links

Domain Management field descriptions on page 256
Domain Details field descriptions on page 257

Modifying domains

Procedure

1. On System Manager Web Console, click **Elements** > **Routing**.
2. In the left navigation pane, click **Domains**.
3. To edit information for existing domains or sub-domains, select the check boxes for the domains that you want to edit and click **Edit**.
4. Make changes to the domain data as required.
5. To copy existing domain data to a new domain, select the domain and click **Duplicate**. You can edit the duplicate domain name as required.
6. Click **Commit**.

   Warning:

   SIP domain name change will cause login failure for Communication Address handles with this domain.

Related Links

Domain Management field descriptions on page 256
Domain Details field descriptions on page 257

Deleting Domains

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .

2. In the left navigation pane, click **Domains**.
3. To delete an existing domain, select the check box of the relevant domain, and click **Delete**.
4. Click **Delete** on the confirmation page.

Related Links

Domain Management field descriptions on page 256
Delete Confirmation field descriptions on page 256

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of selected domains.

Button	Description
Delete	Deletes the selected domains.
Cancel	Cancels the deletion of the domains.

Related Links

Deleting Domains on page 255

Domain Management field descriptions

Use this page to create, modify, delete, and manage domains.

Button	Description
Edit	Opens the Domains page, which you can use to modify the domain details.
New	Opens the Domains page, which you can use to create new domains.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the domain.
Duplicate	Creates a duplicate of the selected domain.
More Actions > **Import**	Opens the Import data page, which allows you to import from XML files or zip file containing one or more XML files.
More Actions > **Export Domains**	Opens the Export Domains page, which allows you to export the domains data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page, which allows you to export the routing entities data as a zipped file to a specified location.

Name	Description
Name	Name of the domain.
Type	List of the type of domains. Only Domains of type SIP can be used for routing.
Notes	Additional notes about the domain.

Related Links

Creating domains on page 255
Modifying domains on page 255
Deleting Domains on page 255

Domain Details field descriptions

Name	Description
Name	Name of the domain.
Type	List of the type of domains. Only domains of type SIP can be used for routing.
Notes	Additional notes about the domain.

Button	Description
Commit	Saves the domain and distributes it to all the instances of the Session Manager.
Cancel	Cancels the domain creation.

Related Links

Creating domains on page 255
Modifying domains on page 255

Bulk import for Domains

Follow these rules when creating an XML bulk import file:

- The domain name must be unique, and is referred to by other elements.
- It is not possible to create a domain with <domainType> of type *sip* that have <defaultDomain> containing the value *true*.
- The values in <domainType> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sipdomainFullTOList>
    <SipdomainFullTO>
        <notes>this is a test</notes>
```

```
        <defaultDomain>false</defaultDomain>
        <domainName>avaya.com</domainName>
        <domainType>sip</domainType>
        <name>avaya.com</name>
    </SipdomainFullTO>
    <SipdomainFullTO>
        <notes>this is another test</notes>
        <defaultDomain>false</defaultDomain>
        <domainName>avaya2.com</domainName>
        <domainType>sip</domainType>
        <name>avaya2.com</name>
    </SipdomainFullTO>
</sipdomainFullTOList>
```

Locations

About Locations

Use the Locations screen to configure gateway and user locations. The IP address of the device determines the physical location of the caller or the called user.

To determine the location:

1. The Session Manager tries to match the IP address of the bottom-most VIA header of the received INVITE against the IP patterns on the Locations.
2. If no IP address match is found, the Session Manager uses the assigned location on the sending SIP Entity.
3. If no assigned Location is found, the Session Manager uses the assigned location of the Session Manager SIP Entity.

If dial patterns are administered for the specific location, the Session Manager uses the originating location to determine which dial pattern is suitable for routing the call. Locations are also used to limit the number of calls originating from or terminating to a physical location. This is known as Call Admission Control (CAC) and is useful to manage the network bandwidth of locations. CAC provides a level of protection by limiting the impact of multimedia traffic over the most critical network links between enterprise locations, such as the links from branch offices to data centers in the network core. You specify CAC details using the **Overall Managed Bandwidth** and **Per-Call Bandwidth Parameters** sections on the Location Details page.

Note:

The Session Manager logs the result of each rejected multimedia CAC request to help determine the root cause when multimedia calls fail.

You can use the following wildcard characters to specify a location:

- “*” (star) specifies any number of allowed characters at the end of the string.
- “x” specifies a digit.

Note:

The pattern can also accept an IP address range. For example: 10.0.0.1-10.0.0.5

The IP address mask is also a valid pattern. For example: 135.9.0.0/16

The Locations screen can contain one or several IP addresses. Each SIP Entity has a particular IP address. Depending on the physical and geographic location of each SIP Entity, some of the SIP Entities can be grouped into a single location. For example, if there are two Communication Managers located in Denver, the Communication Managers can form one location named Denver.

The order in which the Session Manager matches the IP address is as follows:

1. Wildcard patterns (* and x)
2. Ranges
3. Netmask

Dial Plan Transparency

Dial Plan Transparency (DPT) is a business continuity feature that, during a network outage, preserves the dial plan and reroutes all calls that are generated after the detection of the outage, to the PSTN. Communication Manager and Session Manager support DPT in the Listed Directory Number (LDN)/DTMF method, as follows:

- A PSTN call routes to a single LDN at the far end.
- The PSTN call carries the identity of the calling party.
- The far end answers the call, and the calling side sends identifying DTMF digits of the called party.

For more information about the Dial Plan Transparency feature, see the Communication Manager documentation and Avaya Aura® Dial Plan Transparency White Paper on the Avaya Support website at http://support.avaya.com/.

Note:

- DPT can be triggered by a call between endpoints in different Session Manager locations. However, if a data network failure occurs within a Session Manager location, a DPT call is not supported. Administrators must accordingly plan their data network when deciding how to partition their users into different locations.
- In a mixed environment with SIP and non-SIP devices, the Session Manager DPT feature does not support DPT calls to non-SIP devices connected to a Communication Manager instance that is different from the Communication Manager instance administered in the Location screen.

Creating Locations

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Locations**.

   The Location Details screen is displayed.
3. Click **New**.
4. Enter the location name in the **Name** field.
5. Enter notes about the location, if required.
6. Enter the DPT parameters in the **Dial Plan Transparency in Survivable Mode** section.
7. Specify the parameters for the location in the **Overall Managed Bandwidth** section.
8. Specify the average bandwidth per call for the location in the **Per-Call Bandwidth Parameters** section. For more information, see CAC Administration on page 268.
9. Specify the alarm threshold percentage for audio and multimedia calls for the location in the **Alarm Threshold** section.
10. To add a location pattern, click **Add** under **Location Pattern**.
11. Enter an IP address pattern to match.
12. Enter notes about the location pattern, if required.
13. Continue clicking the **Add** button until all the required Location Pattern matching patterns have been configured.
14. Click **Commit**.

Related Links

Location field descriptions on page 262
Location Details field descriptions on page 262

Modifying Locations

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Locations**.
3. To edit a location name or location matching pattern, select a check box for the required location and click **Edit** and make the required changes to the location or location pattern for that location.
4. If required, modify the DPT parameters in the **Dial Plan Transparency in Survivable Mode** section.

5. If required, modify the parameters for the location in the **Overall Managed Bandwidth** section.
6. If required, modify the average bandwidth per call for the location in the **Per-Call Bandwidth Parameters** section.
7. If required, modify the alarm threshold percentage for audio and multimedia calls for the location in the **Alarm Threshold** section.
8. If required, add or remove a **Location Pattern**.
9. To add or remove a location pattern, click **Add** or **Remove** under **Location Pattern**.
10. Click **Commit**.

Related Links

Location field descriptions on page 262
Location Details field descriptions on page 262

Deleting Locations

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Locations**.
3. To delete an existing location or locations, select the corresponding check boxes and click **Delete**.
4. Click **Delete** on the confirmation page.

Related Links

Location field descriptions on page 262
Delete Confirmation field descriptions on page 261

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of locations.

Button	Description
Delete	Deletes the selected location.
Cancel	Cancels the deletion of the location.

Related Links

Deleting Locations on page 261

Location field descriptions

Use this page to create, modify, delete, and manage locations.

Button	Description
New	Opens the Location Details page to create new locations.
Edit	Opens the Location Details page to modify the location details.
Delete	Opens the Delete Confirmation page to confirm or cancel the deletion of the location.
Duplicate	Creates a duplicate of the selected location and assigns a new state to it.
More Actions > **Import**	Opens the Import data page to import data from XML files or compressed files that contain one or more XML files.
More Actions > **Export Locations**	Opens the Export Locations page to export the location data as an XML file to a specific location.
More Actions > **Export all data**	Opens the Export all data page to export the routing entities data as a compressed file to a specific location.

Name	Description
Name	Name of the location.
Correlation	Indicates if a Session Manager correlates with a Communication Manager network region or not (Yes, No, Unconfirmed).
Notes	Notes about the location.

Related Links

Creating Locations on page 260
Modifying Locations on page 260
Deleting Locations on page 261

Location Details field descriptions

Use this page to set up and configure locations.

General section

Name	Description
Name	Name of the location.
Notes	Notes about the location.
IP Network Region	IP Network Region that correlates with the Session Manager location.
Communication Manager	The Communication Manager that contains the IP Network Region.

Dial Plan Transparency in Survivable Mode section

Name	Description
Enabled	Enable or disable Dial Plan Transparency (DPT) in Survivable mode.
Listed Directory Number	Far end number where a DPT call gets routed. This number may only contain digits 0-9, '-', '.' or space character and may begin with a leading '+'. This number should be unique and should not match an LDN in any other Location. A Listed Directory Number is required if **Enabled** is selected.
Associated CM SIP Entity	The Communication Manager server used to originate DPT calls from this location. The Communication Manager server should ideally be located in this location to maximize the probability of being reached in the event of a network outage. A SIP Entity name must be selected if **Enabled** is selected.

Overall Managed Bandwidth section

Name	Description
Managed Bandwidth Units	Specifies the bandwidth unit for Overall Managed Bandwidth values.
Total Bandwidth	The total bandwidth available for use by any calls between this location and other locations. Any attempt to exceed this limit results in either • calls either being alternate routed or denied. • requested bandwidth of the calls may be reduced. If no value is specified, the bandwidth limit is infinite.
Multimedia Bandwidth	The bandwidth available for use by multimedia calls between this location and other locations. This is a

Table continues…

Name	Description
	subset of the Total Bandwidth value. Any attempt to exceed this limit results in either • calls either being alternate routed or denied. • requested bandwidth of the calls may be reduced. If no value is specified, the use of the limit defined for Total Bandwidth depends on the value of Audio Calls Can Take Multimedia Bandwidth. If selected, Total Bandwidth can be used for any call type. If not selected, Total Bandwidth can be used only for audio calls.
Audio Calls Can Take Multimedia Bandwidth	Specifies the use of multimedia call bandwidth for audio calls. If this check box is selected, the bandwidth reserved for multimedia calls may also be used for audio calls. If not, this bandwidth may only be used for multimedia calls.

Per-Call Bandwidth Parameters section

Name	Description
Maximum Multimedia Bandwidth (Intra-Location)	The maximum bandwidth allowed for a single multimedia call within this location. Calls requesting more bandwidth than this value are modified to use less bandwidth. Default value is 1000 Kbit/sec, range is 0-15360 Kbit/sec.
Maximum Multimedia Bandwidth (Inter-Location)	The maximum bandwidth allowed for a single multimedia call between this location and another location. Calls requesting more bandwidth than this value are modified to use less bandwidth. Default value is 1000 Kbit/sec, range is 0-15360 Kbit/sec.
Minimum Multimedia Bandwidth	The minimum bandwidth specified per multimedia media stream that Session Manager uses while reducing the bandwidth request for a call to or from this location to enforce any bandwidth restriction. If a bandwidth restriction requires Session Manager to reduce a media stream below this level, the stream is removed from the call, possibly resulting in the entire call being blocked. Media requests for bandwidth beneath this minimum is not blocked. This is solely a restriction on the ability of Session Managerto modify requests. Default value is 64 Kbit/sec and the range is 64-15360 Kbit/sec.
Default Audio Bandwidth	The audio bandwidth assumed to be used by a call originating in this location that does not explicitly specify its bandwidth needs using the Session Description Protocol (SDP). Such calls are assumed

Table continues…

Name	Description
	to be of audio type only. Default value is 80 Kbit/sec and the range is 0-15360 Kbit/sec.

Alarm Threshold section

Name	Description
Overall Alarm Threshold	Threshold percentage for the administered **Total Bandwidth** value. When audio and multimedia usage exceeds this percentage of the limit for the specified latency, an alarm will be raised. Valid range is 0% - 100% in increments of 5%. The default value is 80%. Set the value to 0% to disable the alarm.
Multimedia Alarm Threshold	Threshold percentage for the administered **Multimedia Bandwidth** value. When multimedia usage exceeds this percentage of the limit for the specified latency, an alarm will be raised. Valid range is 0% - 100% in increments of 5%. The default value is 80%. Set the value to 0% to disable the alarm.
Latency before Overall Alarm Trigger	Latency before an alarm is raised for the **Total Bandwidth** value. The units are in minutes, with a range of 0 to 30. The default value is 5 minutes.
Latency before Multimedia Alarm Trigger	Latency before an alarm is raised for the **Multimedia Bandwidth** value. The units are in minutes, with a range of 0 to 30. The default value is 5 minutes. Latency value specifies the amount of time during which a location exceeds a threshold before an alarm is raised. This specification helps to prevent excessive alarming if the network crosses back and forth over the alarm threshold value over a period of time. Alarm thresholds are sampled every 60 seconds for a given location.

Location Pattern section

Button	Description
Add	Adds an IP address pattern to match for the location.
Remove	Removes the IP address pattern to match for the location.

Name	Description
IP Address Pattern	An IP address or IP address pattern that maps IP address(es) to this location. IP addresses should uniquely map to locations. If an address matches several locations' patterns, the address gets

Table continues…

Name	Description
	assigned to the location with the most specific pattern matched. Pattern examples are, • 135.12x.121.* • 13x.1xx.* • 135.* • 135.12x.121.123 **Note:** Pattern can also accept IP address range. Example: 10.0.0.1-10.0.0.5 IP address mask is also a valid pattern. Example: 135.9.0.0/16
Notes	Additional notes.

Button	Description
Commit	Modifications made to the Location are saved.
Cancel	Modifications made to the Location are not saved.

Related Links

Creating Locations on page 260
Modifying Locations on page 260

Bulk import for Locations

Follow these rules when creating an XML bulk import file:

- Locations are referred to as routing origination in the import XML.
- The name of a location is unique and is referred to by other elements.
- Multiple Routing Origination Patterns <routingoriginationpatterns> can be configured for one Routing Origination Name.
- The values in <ManagedBandwidthUnitOfMeasurement> must appear exactly same, being case sensitive, as they appear in the System Manager user interface.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<routingoriginationFullTOList>
    <RoutingoriginationFullTO>
        <notes>this is a test</notes>
        <name>New York</name>
        <AverageBandwidthPerCall>80</AverageBandwidthPerCall>
        <AverageBandwidthPerCallUnitOfMeasurement>Kbit/sec</
AverageBandwidthPerCallUnitOfMeasurement>
        <ManagedBandwidth>500000</ManagedBandwidth>
        <ManagedBandwidthUnitOfMeasurement>Kbit/sec</ManagedBandwidthUnitOfMeasurement>
```

```
            <cac_can_audio_steal_from_video>true</cac_can_audio_steal_from_video>
        <cac_max_bwidth_video_interloc>300</cac_max_bwidth_video_interloc>
        <cac_max_bwidth_video_intraloc>384</cac_max_bwidth_video_intraloc>
        <cac_min_acceptable_bwidth_video>64</cac_min_acceptable_bwidth_video>
        <cac_normal_bwidth_video>50</cac_normal_bwidth_video>
        <routingoriginationpatterns>
            <notes>this is a test</notes>
            <ipaddresspattern>1.2.3.4-1.2.3.10</ipaddresspattern>
        </routingoriginationpatterns>
        <routingoriginationpatterns>
            <notes>this is a test</notes>
            <ipaddresspattern>1.2.4.*</ipaddresspattern>
        </routingoriginationpatterns>
        <TimeToLiveInSec>3600</TimeToLiveInSec>
    </RoutingoriginationFullTO>
    <RoutingoriginationFullTO>
        <notes>this is a test</notes>
        <name>Berlin</name>
        <AverageBandwidthPerCall>80</AverageBandwidthPerCall>
        <AverageBandwidthPerCallUnitOfMeasurement>Kbit/sec</
AverageBandwidthPerCallUnitOfMeasurement>
        <cac_can_audio_steal_from_video>true</cac_can_audio_steal_from_video>
        <cac_max_bwidth_video_interloc>384</cac_max_bwidth_video_interloc>
        <cac_max_bwidth_video_intraloc>384</cac_max_bwidth_video_intraloc>
        <cac_min_acceptable_bwidth_video>64</cac_min_acceptable_bwidth_video>
        <cac_normal_bwidth_video>40</cac_normal_bwidth_video>
            <ManagedBandwidth>900000</ManagedBandwidth>
        <ManagedBandwidthUnitOfMeasurement>Kbit/sec</ManagedBandwidthUnitOfMeasurement>
        <routingoriginationpatterns>
            <notes>this is a test</notes>
            <ipaddresspattern>3.*</ipaddresspattern>
        </routingoriginationpatterns>
        <routingoriginationpatterns>
            <notes>this is a test</notes>
            <ipaddresspattern>2.3.4.5</ipaddresspattern>
        </routingoriginationpatterns>
        <TimeToLiveInSec>3600</TimeToLiveInSec>
    </RoutingoriginationFullTO>
</routingoriginationFullTOList>
```

Call Admission Control

Audio and multimedia calls require high bandwidth and low latency for best user experience. Call Admission Control (CAC), also known as Bandwidth Management, prevents degradation of call quality by limiting the number of concurrent calls over links that have limited bandwidth. With CAC, enterprise networks can sustain the load imposed by the media traffic over the IP network.

CAC Behavior

Session Manager CAC limits bandwidth between locations. For CAC, the links between locations can have limited capacity, while calls that take place entirely within a location do not need to be limited. It also assumes that all calls entering or leaving a location use the same network link. A link for the location connects the location to the public network, from which every other location can be accessed at equal cost. Thus any media session between locations involves two links – one to and another from each location.

The association of one link to one location means that limits on links can be implemented as limits on locations. No other links are recognized or have limits enforced by CAC. Calls contained entirely within a location involve no links.

CAC enforces limits by allowing calls on a first-come, first-serve basis until a limit is about to be violated. CAC prevents limit violation by either reducing the bandwidth of calls or by denying calls. Bandwidth reduction can mean that audio or video quality is reduced, or that media streams (such as video) are removed. Only calls that would otherwise violate limits will be impacted by CAC. By preventing limits from being exceeded, CAC prevents packet loss degradation from impacting existing calls.

Calls between locations are subject to the limit enforcement of both locations, if limits have been defined for both. In cases when call parties are not mapped to locations, then CAC restrictions donot apply for those parties.

Emergency calls, as defined in the *Dial Patterns* section, are never impacted by CAC.

CAC Administration

CAC allows you to specify several types of limits on Locations. There is an overall limit (**Total Bandwidth**), which constrains the total bandwidth used for calls traversing the link of the location. There is also a multimedia sub-limit (**Multimedia Bandwidth**), which allows you to restrict calls that are not audio-only (such as video calls), to less than the full capacity of the location. This sub-limit can be used to prevent a few large video calls from exhausting the link and preventing audio calls from being made.

CAC also allows *per-call* parameters (**Maximum Multimedia Bandwidth**) to be specified at a location level, which limits the bandwidth allowed to a single call. This can proactively create room for more calls along a link by restricting video quality.

Each of these limits may be specified or left blank for any given location.

CAC operates by inspecting Session Description Protocol (SDP) contained in SIP messaging for calls. SDP identifies both the source of media (by IP address, which maps to Location) and the amount of bandwidth consumed. SDP manipulation is also used to reduce bandwidth consumption for limit enforcement. CAC allows the specification of default bandwidth assumptions for calls with unrecognized SDP, specified per Location (**Default Audio Bandwidth**). CAC also allows a per-location restriction on how much a multimedia stream can have its bandwidth reduced (**Minimum Multimedia Bandwidth**) before it should be removed entirely. This is required for maintaining a minimum level of video quality.

CAC provides alarm notifications when the bandwidth usage of a location remains above a certain threshold for a sustained period of time. Snapshots of current usage are taken every 60 seconds, and if successive snapshots remain above the threshold, the alarm is raised until usage drops below the threshold. For each location and limit type, you can administer the number of snapshots and threshold required to raise the alarm. You can monitor the real-time bandwidth usage in the Managed Bandwidth Usage page.

Finally, two additional settings can change the way Session Manager performs Call Admission Control.

1. **Audio Calls Can Take Multimedia Bandwidth**, when unchecked, specifies that only multimedia calls will fill the **Multimedia Bandwidth** bucket, while audio-only calls will be limited to the bandwidth specified by **Total Bandwidth – Multimedia Bandwidth**. When checked (default), audio-only calls can consume all of **Total Bandwidth**, and **Multimedia Bandwidth** functions as a sub-limit for calls containing non-audio media.
2. Based on the **Ignore SDP for Call Admission Control** option in the Global Settings section on the Session Manager Administration page, all Session Manager instances interpret that all calls lack SDP. This causes every call to be regarded as an audio call using bandwidth defined as **Default Audio Bandwidth** under the originating location of the call.
   - This setting can be used to transform CAC into a call count enforcer. Because each call is counted equally, the limit enforced is a limit on the number of calls allowed to or from a location. By assigning SIP entities to unique locations, you can limit the number of calls to or from an entity.
   - Session Manager 6.0 always ignores SDP. When upgrading System Manager from 6.0 to later versions, this behavior will be preserved. Otherwise, this option is disabled by default.

Adaptations

About Adaptations

You can optionally use Adaptations to modify SIP messages that are leaving a Session Manager instance (egress adaptation) and that are entering a Session Manager instance (ingress adaptation). This adaptation function is needed to convert strings containing calling and called party numbers from the local dialplan of a SIP entity to the dialplan administered on the Session Manager, and vice-versa. Adaptation is also needed when other SIP entities require special SIP protocol conventions. Each administered SIP entity may have its own unique adaptation, or one adaptation can be shared among multiple entities.

You can implement adaptations as software modules that can be created and deployed to fit the needs of the system.

Session Manager includes a module called DigitConversionAdapter, which can convert digit strings in various message headers as well as hostnames in the Request-URI and other headers. It also contains adaptation modules which do protocol conversions, such as for AT&T, Verizon and Cisco systems, as well as the digit conversion. All of these adapters allow for modification of URIs specified using unique name-value pairs for egress adaptation. For example, these can be used to replace the host name in the Request-URI with an administered host name during egress adaptation. An adaptation administered using Routing specifies the module to use as well as the

digit conversion that is to be performed on headers in the SIP messages. Different digit conversions can be specified for ingress and egress adaptation.

All the adaptation modules provided with Session Manager also convert DTMF message bodies in an INFO message between the *application/vnd.nortelnetworks.digits*, *application/dtmf-relay*, and *application/dtmf* formats. DTMF message bodies are automatically converted to *application/dtmf-relay* on ingress unless the `noidtmf` parameter is specified. DTMF message bodies are converted on egress to the format specified in the `dtmf` parameter.

Additionally, digit conversion can be specified to modify only *origination* type headers, only *destination* type headers, or both. The origination/source type URIs are:

- From: See the note 1.
- P-Asserted-Identity
- History-Info (calling portion)

The destination type URIs are:

- Request-URI: See the note 3.
- Contact in 3xx response: See the note 2.
- To: See the notes 1 and 3.
- Message Account in NOTIFY/message-summary body.
- Refer-To in REFER message: See the note 2.

Note:

1. The From and To headers are only modified by adaptation if the `fromto` module parameter is present and has the value of *true*. See *Adaptation Module Administration* below.
2. Adaptations are only applied to the Contact header in a 3xx response and the Refer-To header in a REFER message, if the host-part of the URI is either the IP address of the Session Manager or a domain for which the Session Manager is authoritative.
3. In Session Manager 6.2 and later, Request-URI and To headers are not adapted on ingress if the host part of the URI is an IP address that is different from the IP address of the Session Manager. If required, the new adaptation module parameter `adaptForeignURI` can be added to provide the earlier adaptation behavior prior to that of Session Manager 6.2 release.
4. All adaptations strip the port and transport from the Request-URI if the host-part is adapted on egress. This behavior can be overridden with the `keepPortTransport` parameter.

Related Links

Creating Adaptations on page 275

Adaptation module administration

On the Adaptation Details screen, administer the following fields:

- **Adaptation Name** : This is the name for adaptation.
- **Module Name** : Name of the module.

  The available modules are:

  - DigitConversionAdapter
  - CiscoAdapter
  - DiversionTypeAdapter
  - VerizonAdapter
  - AttAdapter
  - CS1000Adapter
  - OrangeAdapter
  - ModularMessagingAdapter
  - NortelAdapter
  - AMSAdapter

  See the section *Installed vendor adapters* for details.
- **Module Parameter Type** : The module parameter can be one of the following types:
  - No parameter
  - Single parameter. Enter the module parameter. Module parameters must not contain any white spaces.
  - Name-Value pair module parameter. Add or remove the name-value pair module parameter.

    Note:

    1. A module parameter name must not contain any white space.
    2. Enclose the value in double quotation marks if it contains the space character. Within the value field, you can include a double quotation mark by using \" .

Supported adaptation module parameters are:

- `fromto`: If set to *true*, then adaptation will modify From and To headers of the message. If omitted or set to any other value, From and To headers will not be modified.
- `multipartMIMEsupported (` can be abbreviated to `MIME)`: Is an optional parameter and is applicable to the egress processing only. If the parameter is present and set to *no* , then multipart MIME message bodies are stripped on egress from Session Manager. If the multipart MIME message contains an SDP message body, it will be inserted as the only message body in the outgoing message. If omitted or set to any other value, the message bodies will not be modified.

- `adaptForeignURI`: In Session Manager Release 6.2 and later, if the value is set to *true* then INGRESS adaptation is applied to the Request-URI (and to the header if the *fromto* parameter is set) even if the host part is an IP address that is different from the IP address of Session Manager.
- `noidtmf`: In Session Manager Release 6.3.1 and later, if the value is set to *true* then no DTMF message body conversion is done on ingress.
- `dtmf` : In Session Manager Release 6.3.1 and later, the value of this parameter determines the DTMF message body format that is desired on egress from Session Manager. If omitted, no conversion is done. Supported values are nortel, relay, and dtmf.
- `keepPortTransport` : In Session Manager Release 6.3.2 and later, if this parameter is present and set to any value, then Session Manager does not strip port and transport when the domain of the Request-URI is modified on egress.
- `noar` : In Session Manager Release 6.3.4 and later, this parameter can contain a comma-separated list of SIP response codes and is applicable to the egress adaptation only. You can use this parameter to override the default alternate routing behavior of Session Manager. Session Manager does not alternate route a request to the next SIP Entity if it gets one of the responses listed in the parameter value.

  Example

  noar = 404,486
- `sessionTimeout`: In Session Manager Release 6.3.6 and later, you can use this parameter for SIP entities that do not support the session timer (as per RFC 4028) or send periodic SIP messages to keep the session active for more than one hour. If both entities use the session timer in a call, Session Manager keeps the session active for the negotiated interval. If the entities do not use the session timer in a call, then Session Manager keeps the session active for one hour after the last SIP transaction. In such cases, you can set this parameter (in seconds) to extend the one hour interval. For example, if the session timer is not used, the parameter value of *sessionTimeout=7200* makes the session stay in memory for 7200 seconds (or 120 minutes) after the last SIP message exchange.
- `noallow`: In Session Manager Release 6.3.13 and later, this parameter requires a comma-separated list of SIP methods. The system strips the methods from the Allow header on egress. Method names are case-insensitive. For example, noallow=UPDATE and noallow=UPDATE,OPTIONS.

EGRESS Domain Modification Parameters

- `overrideDestinationDomain (` can be abbreviated to `odstd)` **:** By default, this is the first parameter. Adaptation module replaces the domain in Request-URI, To header (if administered), Refer-To header, and Notify/message-summary body with the given value for egress only. If the request is a REFER, the domain in the Refer-To header will only be modified if it is the IP address of Session Manager or a domain for which Session Manager is authoritative.
- `overrideSourceDomain (` may be abbreviated to `osrcd)` **:** Adaptation module replaces the domain in the From header (if administered), P-Asserted-Identity header and calling part of the History-Info header with the given value for egress only.

INGRESS Domain Modification Parameters:

- `ingressOverrideDestinationDomain (` can be abbreviated to `iodstd)` : Adaptation module replaces the domain in Request-URI, To header (if administered), and Notify/message-summary body with the given value for ingress only. If the request is a REFER, the domain in the Refer-To header will only be modified if it is the IP address of Session Manager or a domain for which Session Manager is authoritative.
- `ingressOverrideSourceDomain (` can be abbreviated to `iosrcd)` : Adaptation module replaces the domain in the From header (if administered), P-Asserted-Identity header and calling part of the History-Info header with the given value for ingress only.

Example:

Module Name:`CiscoAdapter`

Module Parameter:`osrcd=dr.avaya.com odstd=ny.avaya.com`

The same value in verbose form:

Module Name:`CiscoAdapter`

Module Parameter:`overrideSourceDomain=dr.avaya.com overrideDestinationDomain=ny.avaya.com`

All adaptation modules have the ability to replace the domain (also known as host name) portion of the URI with a specified value for source and destination type URIs on outgoing calls (egress) and to append parameters to the Request URI on for outgoing calls (egress). This adaptation functionality is expandable to adapt additional deployments that require further flexibility.

EGRESS Display name Modification:

`egressDisplayName` : In Session Manager Release 6.3.4 and later, if this parameter is present, then the adaptation module modifies the display name of the Contact, P-Asserted-Identity, and From/To headers (if fromto = true is specified) of the egress messages. For outgoing calls, the adaptation module applies the adaptation to the P-Asserted-Identity, Contact, and From headers in both the initial dialog-creating request sent from Session Manager and in all subsequent in-dialog requests. For incoming calls, the adaptation module applies the adaptation to the P-Asserted-Identity, Contact, and To headers. If the value of the parameter contains spaces, then the value must be enclosed in double quotes. Additionally, any double quotes that are part of the parameter value must be preceded by a backslash character.

Example:

- egressDisplayName=SomeCallingName
- egressDisplayName="My Business"
- egressDisplayName="The \"Best\" Business"

Phone Context

Phone Context is an optional field for ingress adaptation rules and in egress adaptation rules.

- During the processing of ingress messages:

If the phone-context field of an ingress adaptation module rule contains a valid value (not empty), ingress adaptation is applied only if all four trigger fields (Matching Pattern, Min, Max, and Phone-context) match the header. If the phone-context field is empty, ingress adaptation is applied based on the remaining fields (Matching Pattern, Min, and Max). The allowed format for the Phone Context string can either be an E.164 number or a domain name (which can contain only alphanumeric characters, a hyphen, and periods).

- During the processing of egress messages:

  If the phone-context field of an egress adaptation module rule contains a valid value (not empty), the adaptation module modifies the digits and inserts phone-context when the three trigger fields match the criteria, that is, Matching Pattern, Min, and Max. On the other hand, if the phone-context field is empty, the egress adaptation module does not insert phone-context.

Precedence Rules

In case a request matches the criteria of two rules (one with a valid phone-context and empty phone-context), the rule with valid phone-context string takes precedence. This is illustrated below:

Example:

Rules	Ingress Adapter Rule
1	Matching pattern: 53853 Min: 7 Max: 7 Phone-Context: Delete Digits: 3 Insert Digits: 538 Address to modify: both
2	Matching pattern: 538 Min: 7 Max: 7 Phone-Context: denver Delete Digits: 0 Insert Digits: +1303 Address to modify: both

For an adapter with the above two rules, a request with `R-URI of 5385335; phone-context=denver@avaya.com; user=phone` matches both the rules. However, Rule 2 is selected for applying adaptation because the Rule 2 matches four fields as compared with three fields in the Rule 1.

Presence of URI parameter phone-context and user=

During the ingress adaptation, when the phone-context parameter is removed, the adaptation module also removes the URI parameter `user=` if it is present.

During the egress adaptation, when the phone-context parameter is inserted, the adaptation module also inserts the URI parameter `user=phone`. However, if the URI parameter `user=phone` is already present, the adaptation module does not insert it again. The egress adaptation overwrites phone-context parameter, if it is present. If phone-context parameter is present and egress adaptation does not result in a new phone-context, the egress adaptation does not change the original phone-context parameter.

Creating Adaptations

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Adaptations**.

   System Manager displays the Adaptation page.
3. Click **New**. The Adaptation Details page is displayed.
4. Enter the Name, Adaptation Module, and any other required fields in the first section.
   a. Enter a descriptive name for the adaptation.
   b. Specify an adaptation module.
      - In the **Module Name** field, select the Adaptation module.
      - In the **Module Parameter Type** field, select the parameter type. The module parameter can be one of the following types:
        - No parameter
        - Single parameter. Enter the module parameter. Module parameter must not contain any whitespaces.
        - Name-Value pair module parameter. Add or remove the name-value pair module parameter.

          Note:

          a. A module parameter name must not contain any whitespace.

          b. Enclose the value in double quotation marks if the value contains the space character. Within the value field, you can include a double quotation mark by using \" .
   c. Enter a list of URI parameters to append to the Request-URI on egress in the **Egress URI Parameters** field.

      URI parameters can be added to the Request-URI. For example, the parameter `user=phone` can be appended for all INVITEs routing to a particular SIP entity. The egress Request-URI parameters are administered from the Adaptation Details using the Egress URI Parameters field.

      The field's format is the string that should be appended to the Request URI. The string must conform to the augmented BNF defined for the SIP Request URI in RFC3261. A

leading ';' is optional. Entry `;user=phone;custApp=1` is equivalent to `user=phone;custApp=1`.

d. Enter description about the adaptation module in the **Notes** field.

5. Click **Add** under Digit Conversion for Incoming Calls if you need to configure ingress digit conversion. Ingress adaptation is used to administer digit manipulation for calls coming into the Session Manager instance.
6. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
7. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

   The minimum value can be 1. The maximum value can be 36.
8. Add **Phone Context** as an optional parameter for the ingress adaptation rules.
9. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
10. Enter the digits that you want inserted before the number in the **Insert Digits** field.
11. From the drop-down list, select the value for **Address to modify**. A setting of both will look for adaptations on both origination and destination type headers. The digit conversion applied to a header will be taken from the entry with the longest matching pattern.
12. Enter any additional or special adaptation data in **Adaptation Data** field.

    The adaptation data can be up to 20 characters in length with valid character values including numeric characters 0-9, +, *, #, and -.
13. Continue clicking the Ingress Adaptation **Add** button until all the required ingress matching patterns have been configured.
14. To remove a matching pattern for ingress adaptations, select the check box next to that pattern and click **Remove**.
15. Click **Add** under **Digit Conversion for Outgoing Calls** if you need to configure egress digit conversion. Egress adaptation administers digit manipulation for calls going out of the Session Manager instance.
16. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
17. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

    The minimum value can be 1 or more. The maximum value can be 36.
18. Add **Phone Context** as an optional parameter for the egress adaptation rules.
19. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
20. Enter the digits that you want inserted before the number in the **Insert Digits** field.

21. From the drop-down list, select the value for **Address to modify**. A setting of both will look for adaptations on both origination and destination type headers. The digit conversion applied to a header will be taken from the entry with the longest matching pattern.
22. Enter any additional or special adaptation data in **Adaptation Data** field.

    The adaptation data can be up to 20 characters in length with valid character values including numeric characters 0-9, +, *, #, and -.

    Note:

    In the case of the Verizon Unscreened ANI feature, the data entered in the outgoing *Adaptation Data* field is verified to ensure that it complies with the required format of a Screened Telephone Number (STN).
23. Continue clicking the Egress Adaptation **Add** button until all the required egress matching patterns have been configured.
24. To remove a matching pattern for egress adaptations, select the check box next to that pattern and click **Remove**.
25. Click **Commit**.

Related Links

Adaptations field descriptions on page 288
About Adaptations on page 269
Adaptation Details field descriptions on page 289

Adaptation example

Example 1

In the following example, an adaptation for AT&T service provider is needed at least for international calls.

For incoming calls, AT&T sends the 10 digit local number. To convert this into E.164, Session Manager must add a plus sign. Specify the following values:

- Matching pattern = 1
- Min = 10
- Max = 10
- Phone-Context =
- Delete Digits = 0
- Insert Digits = +
- Address to modify = both

For outgoing calls to AT&T, Session Manager must convert the E.164 form to a format that AT&T supports, either 1+10 digits for North America calls, or 011+country code + number for international calls. For example, for calls to North America, specify the following values:

- Matching Pattern = +1

- Min = 12
- Max = 12
- Phone-Context =
- Delete Digits = 1
- Insert Digits = <None>
- Notes = Calls to North America

For calls to Germany, specify the following values:

- Matching Pattern = +49
- Min = 13
- Max = 13
- Delete Digits = 1
- Insert Digits = 011
- Address to modify = destination
- Notes = Calls to Germany

Example 2

Following is an example of how to set up adaptation with phone-context:

Ingress adaptation rule:

- Matching pattern = 53
- Min = 4
- Max = 4
- Phone-Context = site1
- Delete Digits = 0
- Insert Digits = 908
- Address to modify = both

Egress adaptation rule:

- Matching pattern = 908
- Min = 7
- Max = 7
- Phone-Context = site1
- Delete Digits = 3
- Insert Digits =
- Address to modify = both

Input (String prior to the adaptation processing)	Adaptation Processing	Output (String after the adaptation processing)
5335; phone-context = site1@avaya.com; user = phone	Ingress adaptation	9085335@avaya.com
9085335@avaya.com	Egress adaptation	5335; phone-context = site1@avaya.com; user = phone

Example 3

Session Manager supports phone-context with global number prefix (that is, a number starting with +). If the incoming request contains the phone-context parameter with a number starting with +, Session Manager prefixes the userpart with the contents of phone-context before invoking the routing lookup. The resulting string (after concatenation) is only used for routing purpose only and Session Manager does not modify the userpart. The following two examples illustrate the above point:

R-URI	Ingress Adapter Rule	Resulting R-URI	Routing Notes
8885335;phone-context= +1303@avaya.com; user=phone	Matching pattern: 888 Min: 7 Max: 7 Phone-Context: Delete Digits: 3 Insert Digits: 538 Address to modify: both **Note:** Phone-Context string is empty.	5385335;phone-context= +1303@avaya.com; user=phone	Session Manager uses the string +13035385335@avaya.com for routing purposes
5385335;phone-context= +1303@avaya.com; user=phone	Matching pattern: 538 Min: 7 Max: 7 Phone-Context: +1303 Delete Digits: 0 Insert Digits: +1303 Address to modify: both	+13035385335@avaya.com	Session Manager uses the string +13035385335@avaya.com for routing purposes

In the first example (row 1), the Phone-context is empty in the ingress adaptation rule, while the incoming INVITE contains the phone-context parameter. As the adaptation rule requires matching three fields (pattern, min and max). If phone-context field is empty, the match succeeds and the adaptation is applied. However, the adaptation does not modify the phone-context parameter. This examples also illustrate the backward compatibility case where adaptation is applied on the userpart without modifying phone-context parameter. Session Manager upon receiving this INVITE, performs routing lookup based on `+13035383535` to determine the destination. Here, Session Manager only modifies the phone number and not the phone-context parameter.

In the second example (row 2), the ingress adaptation rule contains `+1303` in the phone-context field. Also, the incoming INVITE contains the phone-context parameter with value of `+1303`. As the ingress adaptation rule requires matching all four fields, the match succeeds and the adaptation is applied, which modifies the R-URI. Session Manager, upon receiving this INVITE, performs routing lookup based on the updated R-URI.

Modifying Adaptations

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Adaptations**.

   System Manager displays the Adaptation page.
3. Select the adaptation for modification and click **Edit**
4. Edit the Name, Adaptation Module and any other required fields in the first section. Currently, there is only one adaptation module named *DigitConversionAdapter*.
   a. Enter a descriptive name for the adaptation.
   b. Specify an adaptation module.
      - In the **Module Name** field, select the Adaptation module.
      - In the **Module Parameter Type** field, select the parameter type. The module parameter can be one of the following types:
        - No parameter
        - Single parameter. Enter the module parameter. Module parameter must not contain any whitespaces.
        - Name-Value pair module parameter. Add or remove the name-value pair module parameter.

          Note:

          a. A module parameter name must not contain any whitespace.

          b. Enclose the value in double quotation marks if the value contains the space character. Within the value field, you can include a double quotation mark by using \" .
   c. Enter a list of URI parameters to append to the Request-URI on egress in the **Egress URI Parameters** field.

      URI parameters can be added to the Request-URI. For example, the parameter “user=phone” can be appended for all INVITEs routing to a particular SIP entity. The egress Request-URI parameters are administered from the Adaptation Details using the Egress URI Parameters field.

      The field's format is the string that should be appended to the Request URI. The string must conform to the augmented BNF defined for the SIP Request URI in RFC3261. A leading ';' is optional. Entry “;user=phone;custApp=1” is equivalent to “user=phone;custApp=1”.
   d. Enter description about the adaptation module in the **Notes** field.

5. Click **Add** under **Digit Conversion for Incoming Calls** if you need to configure ingress digit conversion. Ingress adaptation is used to administer digit manipulation for calls coming into the Session Manager instance.
6. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters.
7. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

   The minimum value can be 1 or more. The maximum value can be any number up to 36.
8. Add **Phone Context** as an optional parameter for the ingress adaptation rules.
9. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
10. Enter the digits that you want inserted before the number in the **Insert Digits** field.
11. From the drop-down list, select the value for **Address to modify**. A setting of both will look for adaptations on both origination and destination type headers. The digit conversion applied to a header will be taken from the entry with the longest matching pattern.
12. Enter any additional or special adaptation data in **Adaptation Data** field.

    The adaptation data can be up to 20 characters in length with valid character values including numeric characters 0-9, +, *, #, and -.
13. Continue clicking the Ingress Adaptation **Add** button until all the required ingress matching patterns have been configured.
14. To remove a matching pattern for ingress adaptations, select the check box next to that pattern and click **Remove**.
15. Click **Add** under **Digit Conversion for Outgoing Calls** if you need to configure egress digit conversion. Egress adaptation administers digit manipulation for calls going out of the Session Manager instance.
16. Enter the matching pattern and other required fields. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing valid input.
17. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

    The minimum value can be 1 or more. The maximum value can be any number up to 36. The minimum value must be less than or equal to the maximum value.
18. Add **Phone Context** as an optional parameter for the egress adaptation rules.
19. Enter the number of digits that you want deleted from left of the dialed number in the **Delete Digits** field.
20. Enter the digits that you want inserted before the number in the **Insert Digits** field.
21. From the drop-down list, select the value for **Address to modify**. A setting of both will look for adaptations on both origination and destination type headers. The digit conversion applied to a header will be taken from the entry with the longest matching pattern.

22. Enter any additional or special adaptation data in **Adaptation Data** field.

    The adaptation data can be up to 20 characters in length with valid character values including numeric characters 0-9, +, *, #, and -.

    Note:

    In the case of the Verizon Unscreened ANI feature, the data entered in the outgoing “Adaptation Data” field is verified to ensure that it complies with the required format of a Screened Telephone Number (STN).

23. Continue clicking the Egress Adaptation **Add** button until all the required egress matching patterns have been configured.
24. To remove a matching pattern for egress adaptations, select the check box next to that pattern and click **Remove**.
25. Click **Commit**.

Related Links

Adaptations field descriptions on page 288
Adaptation Details field descriptions on page 289

Deleting Adaptations

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Adaptations**.

   System Manager displays the Adaptation page.
3. To delete an Adaptation, select the corresponding check boxes and click **Delete**.
4. On the confirmation page, click **Delete**.

Related Links

Adaptations field descriptions on page 288
Delete Confirmation field descriptions on page 282

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of adaptations

Button	Description
Delete	Deletes entries of the selected adaptations from the database.
Cancel	Cancels the deletion of the selected adaptations.

Related Links

Deleting Adaptations on page 282

Installed vendor adapters

Cisco Adapter (CiscoAdapter) and DiversionTypeAdapter

Cisco Adapter provides two basic header manipulations: converting between Diversion and History-Info headers and converting between P-Asserted-Id and Remote-Party-Id headers. IETF does not accept Diversion and Remote-Party-Id headers. The Diversion and Remote-Party-Id headers are replaced by History-Info and P-Asserted-Identity respectively but are still used in the Cisco products. Cisco Adapter also performs all the conversions available by the Digit Conversion Adapter.

Note:

DiversionTypeAdapter performs the same function as the CiscoAdapter for Avaya Business Communication Manager (BCM) systems.

Diversion to History-Info Header Adaptation

Cisco requires the use of the Diversion header, rather than the History-Info header to provide information related to how and why the call arrives to a specific application or user. The following examples illustrate the adaptations.

Example 1:

Communication Manager user 66600001 forwards to Cisco user 60025.

The outgoing INVITE of Communication Managerhas this history-info:

```
History-Info: "<sip:66600001@ny.avaya.com>;index=1
History-Info: "stn 66600001" <sip:66600001@ny.avaya.com?
    Reason=SIP%3Bcause%3D302%3Btext%3D%22Moved%20Temporarily%22
    &Reason=Redirection%3Bcause%3DCFI>;index=1.1
History-Info: <sip:600025@ny.avaya.com>;index=1.2
```

In the message sent to Cisco this is converted to:

```
Diversion: "stn 66600001" <sip:66600001@ny.avaya.com>;reason=no-
answer;privacy=off;screen=no
```

Example 2:

Communication Manager user calls Cisco user 60025. This call is routed to Modular Messaging at extension 688810.

The INVITE message from the Cisco server contains the following Diversion Header:

```
Diversion: "Ken's Desk" <sip:600025@ny.avaya.com>;reason=user-
    busy;privacy=off;screen=no
```

The message is adapted and the outgoing INVITE to MM replaces the Diversion header with the following:

```
History-Info: <sip:600025@ny.avaya.com>;index=1
History-Info: "Ken's Desk" <sip:600025@ny.avaya.com?
    Reason=SIP%3Bcause%3D486%3Btext%3D%22Busy%20Here%22
    &Reason=Redirection%3Bcause%3DNORMAL%3Bavaya-cm-reason%3D%22
```

```
    cover-busy%22%3Bavaya-cm-vm-address-digits%3D81080000%3Bavaya-cm-vm-address-handle
%3Dsip:80000%40avaya.com>;index=1.1
History-Info: "MM" <sip:688810@ny.avaya.com>;index=1.2
```

Remote-Party-Id to P-Asserted-Identity Header Adaptation

Cisco requires information in the P-Asserted-Identity (PAI) header to be received in the Remote-Party-Id (RPI) header. Any incoming message containing a P-Asserted-Identity header being routed to Cisco replaces that header with the Remote-Party-Id header. Similarly, calls from Cisco containing the Remote-Party-Id header are converted to a P-Asserted-Identity header when routed to non-Cisco entities.

Example 3:

A call is placed from 12345 at Communication Manager and routed to the Cisco PBX.

The INVITE from Communication Manager contains:

```
P-Asserted-Identity: "Ryan" <sip:12345@avaya.com>
```

This header is converted to RPI when the request is sent to the Cisco PBX:

```
Remote-Party-Id: "Ryan"
<sip:12345@avaya.com>;party=called;screen=no;privacy=off
```

Example 4:

A call is placed from 23456 at Cisco PBX and routed to Communication Manager.

The INVITE from Cisco PBX contains:

```
Remote-Party-Id: "Ryan"
<sip:23456@avaya.com>;party=called;screen=no;privacy=off
```

This header is converted to PAI when the request is sent to Communication Manager:

```
P-Asserted-Identity: "Ryan" <sip:23456@avaya.com>
```

Verizon Adapter (VerizonAdapter)

The Verizon adapter requires the same History-Info to Diversion adaptations that the Cisco Adapter uses. The Verizon Adapter also performs all the conversions available by the Digit Conversion Adapter.

Verizon egress adaptor inserts a special Screened Telephone Number (STN) into the Diversion header of all outgoing calls which utilize Verizon as the Service Provider.

This enables Verizon to identify the physical location of the endpoint that is being used to make an outgoing call and to create the needed billing or tariff data as well as to provide the proper routing of E-911 emergency calls.

This feature is called the Verizon Unscreened ANI feature.

Administering Verizon ANI feature

Procedure

1. On the Adaptation Details page, administer the *Module name* field as *VerizonAdapter* so that the adaptation can be associated with the Verizon Adapter.

2. In the *Digit Conversion for Outgoing Calls from SM* section,
   a. Enter one or more *Matching Patterns* that are to be used to identify which origination numbers (PAI) are associated with a given physical location.
   b. Enter the Screened Telephone Number (STN) that corresponds with that location in the *Adaptation Data* field.

   When the Verizon Adaptor processes an egress call, the PAI number associated with the call is compared with the various *Matching Patterns* administered in the *Digit Conversion for Outgoing Calls from SM* section.

   - If there is a match, the data administered in the *Adaptation Data* field is incorporated into the Diversion header for that call and the call continues with its normal routing procedures.
   - If there is no match, the system continues to function as per design.

   Note:

   - If a match occurs on a row with STN filled-in then the History-Info to Diversion header conversion is not done by VerizonAdapter since either a STN or the converted History-Info can be inserted into the Diversion header. So effectively the STN takes precedence in such cases.
   - *Address to modify* field must be set to *origination* or *both* for STN feature to work. Session Manager does not populate STN into the Diversion header on a *destination* address match.
   - If no digit conversion is to be done (that is, matching pattern is there only to specify the STN), then the user should set *Delete Digits* field to 0 and leave *Insert Digits* field as blank.

AT&T Adapter (AttAdapter)

AT&T does not handle the History-Info header. The adaptation module removes, on egress to AT&T, any History-Info headers in a request or response. Messages from AT&T do not change. The AT&T Adapter also performs all the conversions available by the Digit Conversion Adapter.

CS1000 Adapter (CS1000Adapter)

The CS1000 adapter provides the following services:

- Translation between History-Info header formats.
- Origination routing based on the presence of `x-nt-net-feature=x-nt-home` in the Request-URI.

x-nt-home routing

The CS1000 adapter requires special origination based routing when the `x-nt-net-feature` parameter is in the Request-URI with the value of `x-nt-home`. During ingress adaptation, the CS1000 adapter looks for this parameter, value pair. If it is found, the call is routed on the URI in the P-Asserted-Identity header rather than the Request-URI.

History-Info header adaptation

Since the CS1000 adapter uses some different formatting for the History-Info header than other Avaya products, it is necessary to adapt the History-Info header values. Two primary areas of formatting differences requiring adaptation are index values and reason code values.

Index format: The CS1000 adapter increments its indices by adding a value of 1. For example: 1, 2, 3, 4. Avaya products increment its indices after the decimal dot. For example: 1, 1.1, 1.2, 1.3. The CS1000 adapter on ingress converts the values from the integer format to the decimal format. The CS1000 adapter on egress converts the values from the decimal format to the integer format.

Reason Code adaptation: Avaya uses two reason parameters in its History-Info header format. The second parameter is labeled *Redirection* and must be inserted on ingress and removed on egress by the CS1000 adapter. The *Redirection* phrase also contains a `Cause` parameter. The *Redirection Cause* is inserted to make the CS1000 History-Info look like the call forwarding History-Info sent from Communication Manager according to the following mapping:

SIP Cause	Redirection Reason
302	CFI
486	CFB
480	CFNR

Example

A conversion from Avaya format to CS1000 format:

Avaya History-Info:

```
History-Info:<sip:orig@avaya.com>;index=1
History-Info:"Original Destination"<sip:orig@avaya.com?Reason=SIP%3Bcause%3D302%3Btext%3D
%22Moved%20Temporarily%22&Reason=Redirection%3BCause%3DCFI>;index=1.1
History-Info:"Final Destination"<sip:final@avaya.com>;index=1.2
```

gets converted to:

```
CS 1000 History-Info:
History-Info:<sip:orig@avaya.com?Reason=SIP%3Bcause%3D302%3Btext%3B%22Moved%20Temporarily
%22>;index=1, <sip:final@avaya.com>;index=2
```

Example

A conversion from CS1000 format to Avaya format:

CS1000 History-Info:

```
History-Info: <sip:7521;phone-context=cdp.udp@testbed1.com;user=phone?reason=%20sip
%3bcause%3d480%3btext%3d%20%Temporarily%20Unavailable%22>; index=1,
<sip:5522;phone-context=cdp.udp@testbed1.com;user=phone>;index=2
```

gets converted to:

Avaya History-Info:

```
History-Info:<sip:canonically-adjusted-7521@testbed1.com;user=phone>;index=1
History-Info:<sip:canonically-adjusted-7521@testbed1.com;user=phone? Reason=SIP%3Bcause
%3D480%3Btext%3D%22Temporarily%20Unavailable%22&Reason=Redirection%3Bcause%3DNORMAL
%3avaya-cm-reason%3D%22cover-no-reply%22>;index=1.1
History-Info: <sip:canonically-adjusted-5522@testbed1.com;user=phone>;index=1.2
```

Multiple Diversions:

When CS1000 sends History-Info with multiple diversions, the top History-Info will have the original calling number, and the second History-Info will have the last redirect number (CS1000 can send only 2 diversion History-Infos). In Session Manager Release 6.3.2 and later, the CS1000 adapter copies the original calling number History-Info to the second-to-last History-Info during ingress adaptation. For example:

CS1000 History-Info:

```
History-Info: <sip:1001;phone-context=cdp.udp@interop.com;user=phone?reason=sip%3bcause
%3d302%3btext%3d%22Moved%20Temporarily%22>;index=1, <sip:1002;phone-
context=cdp.udp@interop.com;user=phone?reason=sip%3bcause%3d480%3btext%3d%22Temporarily
%20Unavailable%22>;index=2, <sip:1003;phone-
context=cdp.udp@interop.com;user=phone>;index=3
```

gets ingress adapted to:

```
History-Info: <sip:canonically-adjusted-1001@interop.com>;index=1
History-Info: <sip:canonically-adjusted-1001@interop.com;user=phone?
reason=SIP;cause=302;text=”Moved Temporarily”&Reason=Redirection;Cause=“CFI”>;index=1.1
History-Info:<sip:canonically-adjusted-1002@interop.com;user=phone?
reason=SIP;cause=480;text=“Temporarily
Unavailable”&Reason=Redirection;cause=“CFNR”>;index=1.2
History-Info: <sip:canonically-adjusted-1001@interop.com;user=phone?
reason=SIP;cause=302;text=”Moved Temporarily”&Reason=Redirection;Cause=“CFI”>;index=1.3
History-Info: <sip:canonically-adjusted-1003@interop.com;user=phone>;index=1.4
```

If `copyOCNHistInfo=false` is given as an adaptation module parameter, then the CS1000 adapter behaves as it did in prior Session Manager releases and does not copy the original calling number History-Info.

On egress, the CS1000 adapter removes the copied History-Info header when a call is routed from one CS 1000 to another CS 1000.

The CS1000 adapter also performs all the conversions available in the *DigitConversionAdapter*.

Orange Adapter (OrangeAdapter)

This is a module for the service provider Orange. Since it is derived from VerizonAdapter, it does the same History-Info to Diversion adaptation as the Verizon adapter and all the digit conversions available by the Digit Conversion Adapter. In addition, it looks for SDP on INGRESS only of requests and responses. If it finds SDP indicating an Orange offer or answer of G.729, such as the m= line contains the payload type 18, and if there is no fmtp:18 line containing the string 'annexb', then it adds or replaces an 'a=fmtp:18 annexb=no' line in the SDP. This is because the Orange network only supports G.729A and signals G.729B. Finally, OrangeAdapter modifies how Session Manager generates the P-Asserted-Identity header in a request or a response if it is not present on ingress from Orange. The default behavior of the Session Manager is overridden and the PAI is generated from the From header in requests and To header in responses.

Note:

This means that anything calling Orange sees what it supplied in the To header as the connected party number.

Orange does not insert PAI in 1xx/2xx responses and their contact header does not contain connected party information.

Modular Messaging Adapter (ModularMessagingAdapter)

This adaptation module is required only if you have the following elements:

- Session Manager Release 6.1.2 and later.
- Modular Messaging system with software earlier than release 5.2 Service Pack 7.
- A SIP entity that uses one of the other adaptations as listed above and that uses Modular Messaging as its voice messaging system.

You do not need this adaptation if the only entity in your network that can send calls to Modular Messaging is Communication Manager.

In Session Manager Release 6.1.2 and later, CS1000Adapter and other adaptation modules convert from Diversion to History-Info output. This History-Info format contains call forwarding diversion information instead of what looks like Communication Manager coverage history-info which can be interpreted correctly by Modular Messaging 5.2 Service Pack 7 and higher.

ModularMessagingAdapter converts this History-Info into a format that looks like it came from Communication Manager to indicate a covered call, which conforms to the History-Info format supported by earlier releases of Modular Messaging.

Avaya Media Server Adapter (AMSAdapter)

The Avaya Media Server Adapter was introduced in Session Manager Release 6.3.8.

The Avaya Media Server requires a request URI in the form **<token>@domain**. Typically, you can administer a Session Manager with a regular expression to route calls to a media server. However, regular expression routing does not support location-based routing such as dial pattern routing.

If a customer wants to perform location-based routing or domain routing to an Avaya Media Server, the customer can define a dial pattern and use the AMSAdapter on egress to the AMS to change the request-URI. The AMSAdapter does not perform any digit conversion. The AMSAdapter only converts the request-URI.

The adapter is configured with one parameter, **amsuri**. If the value of the **amsuri** parameter contains a complete URI, for example, **amsuri=user@domain**, both the user and the host parts of the URI will be replaced. If the value of the **amsuri** parameter does not contain **@**, for example, **amsuri=ce-msml**, then only the user part of the request-URI will be replaced.

Adaptations field descriptions

Use this page to create, modify, delete, and manage adaptations.

Button	Description
New	Opens the Adaptation Details page that you can use to create new adaptations.

Table continues…

Button	Description
Edit	Opens the Adaptation Details page that you can use to modify the adaptation details.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the adaptation.
Duplicate	Creates a duplicate of the selected adaptation and assigns a new state to it
More Actions > **Import**	Opens the Import data page using which you can import from XML files or zip file containing one or more XML files.
More Actions > **Export Adaptations**	Opens the Export Adaptation page using which you can export the adaptation data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page using which you can export the routing entities data as a compressed file to a specified location.
More Actions > **Manage Modules**	Provides management of custom adaptation modules. **Note:** For Avaya Professional Services use only.

Name	Description
Name	Name of the adaptation. Must be unique and be between 3 and 64 characters in length.
Module name	The module name contains only the name.
Egress URI Parameters	The terminating trunk group parameters.
Notes	Other details that you wish to add.

Related Links

Creating Adaptations on page 275
Modifying Adaptations on page 280
Deleting Adaptations on page 282

Adaptation Details field descriptions

Use this page to specify the adaptation details.

General section

Name	Description
Adaptation name	Name of the adaptation. Must be unique and from 3 to 64 characters in length.
Module Name	The module name contains only the name.
Module Parameter Type	The module parameter can be one of the following types: • No parameter. • Single parameter. Module parameter must not contain any whitespaces. • Name-Value pair module parameter. **Note:** 1. A module parameter name must not contain any whitespace. 2. Enclose the value in double quotation marks if it contains the space character. Within the value field, you can include a double quotation mark by using \" . Supported adaptation module parameters are: • `fromto`: if set to *true*, then adaptation modifies From and To headers of the message. If omitted or set to any other value, From and To headers will not be modified. • `multipartMIMEsupported (or abbr. name MIME)`: (Optional): This adaptation applies to the egress processing only. If the parameter is present and set to *no*, then multipart MIME message bodies will be stripped on egress from Session Manager. If the multipart MIME message contained an SDP message body, it will be inserted as the only message body in the outgoing message. If omitted or set to any other value, message bodies will not be modified. EGRESS Domain Modification Parameters • `overrideDestinationDomain (` can be abbreviated to `odstd)`: {parameter #1 if not named}, replaces the domain in Request-URI, To header (if administered), Refer-To header, and Notify/message-summary body with the given value for egress only. • `overrideSourceDomain (` can be abbreviated to `osrcd)`: replaces the domain in the From

Table continues…

Name	Description
	header (if administered), P-Asserted-Identity header and calling part of the History-Info header with the given value for egress only. INGRESS Domain Modification Parameters: • `ingressOverrideDestinationDomain (` can be abbreviated to `iodstd)`: replaces the domain in Request-URI, To header (if administered), and Notify/message-summary body with the given value for ingress only. • `ingressOverrideSourceDomain (` can be abbreviated to `iosrcd)`: replaces the domain in the From header (if administered), P-Asserted-Identity header and calling part of the History-Info header with the given value for ingress only.
Egress URI Parameters	The terminating trunk group parameters. URI parameters can be added to the Request-URI. For example, the parameter “user=phone” can be appended for all INVITEs routing to a particular SIP entity. The egress Request-URI parameters are administered from the Adaptation Details using the Egress URI Parameters field. The field's format is the string that should be appended to the Request URI. The string must conform to the augmented BNF defined for the SIP Request URI in RFC3261. A leading ';' is optional. Entry “;user=phone;custApp=1” is equivalent to “user=phone;custApp=1”.
Notes	Other details that you wish to add.

Digit Conversion for Incoming Calls to SM section

Button	Description
Add	Adds digit conversion for incoming calls for the adaptations.
Remove	Removes digit conversion from incoming calls for the adaptations.

Name	Description
Select check box	Use this check box to select and use the digit conversion for the incoming calls
Matching Pattern	Pattern to match for the incoming calls. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.

Table continues…

Name	Description
Min	Minimum number of digits to be matched. The minimum value can be 1 or more.
Max	Maximum number of digits to be matched. The maximum value can be any number up to 36.
Phone Context	Optional parameter for the ingress adaptation rules. If the phone-context field of an ingress adaptation module rule contains a valid value (not empty), ingress adaptation is applied only if all four trigger fields (Matching Pattern, Min, Max, and Phone-context) match the header. If the phone-context field is empty, ingress adaptation is applied based on the remaining fields (Matching Pattern, Min, and Max). The allowed format for the Phone Context string can either be an E.164 number (which can contain optional hyphens, periods, or parenthesis) or a domain name (which can contain only alphanumeric characters, a hyphen, and periods).
Delete Digits	Number of digits to be deleted from the dialed number.
Insert Digits	Number of digits to be added before the dialed number.
Address to Modify	A setting of both will look for adaptations on both origination and destination type headers. The digit conversion applied to a header will be taken from the entry with the longest matching pattern.
Adaptation Data	Any additional or special adaptation data up to 20 characters. Valid values: numeric characters 0-9, +, *, #, and -. This is a non-mandatory field.
Notes	Any other details that you wish to add.

Digit Conversion for Outgoing Calls from SM section

Button	Description
Add	Adds digit conversion for outgoing calls for the adaptations.
Remove	Removes digit conversion from outgoing calls for the adaptations.

Name	Description
Select check box	Use this check box to select and use the digit conversion for the outgoing calls.

Table continues…

Name	Description
Matching Pattern	Pattern to match for the outgoing calls. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.
Min	Minimum number of digits to be matched. The minimum value can be 1 or more.
Max	Maximum number of digits to be matched. The maximum value can be any number up to 36.
Phone Context	Optional parameter in the action fields for the egress adaptation rules. If the phone-context field of an egress adaptation module rule contains a valid value (not empty), the adaptation module modifies the digits and insert phone-context when the three trigger fields match the criteria, that is, Matching Pattern, Min, and Max. On the other hand, if the phone-context field is empty, the egress adaptation module does not insert phone-context.
Delete Digits	Number of digits to be deleted from the dialed number.
Insert Digits	Number of digits to be added before the dialed number.
Address to Modify	A setting of both will look for adaptations on both origination and destination type headers. The digit conversion applied to a header will be taken from the entry with the longest matching pattern.
Adaptation Data	Any additional or special adaptation data up can be up to 20 characters. Valid values: numeric characters 0-9, +, *, #, and -. This is a non-mandatory field. **Note:** In the case of the Verizon Unscreened ANI feature, the data entered in the outgoing **Adaptation Data** field is verified to ensure that it complies with the required format of a Screened Telephone Number (STN).
Notes	Any other details that you want to add.

Button	Description
Commit	Saves the adaptation details and distributes them to the Session Manager instances in the enterprise.
Cancel	Cancels changes to the adaptation details and returns to the Adaptations page.

Related Links

Creating Adaptations on page 275
Modifying Adaptations on page 280

Bulk import for Adaptations

Conform to the following rules while creating an XML bulk import file:

- The name of an adaptation is unique and other elements refer to it.
- The value of <adaptationmodule> is a combination of the fields *Module Name* and *Module Parameters* in the System Manager user interface. The values are separated by a single space.
- Multiple Ingress and Egress configurations <<EgressadaptationFullTO>, <IngressadaptationFullTO>> can be configured for one Adaptation name.
- The values in <addressToModify> must have the same case as they appear in the System Manager user interface.

Warning:

When you add new digit pattern or adaptation entries to an existing adaptation, you must include all patterns in the adaptation XML file. You cannot import an adaptation that includes only the new adaptation patterns. When you add new patterns to an existing adaptation, ensure that you export the current adaptation, add new patterns, and then re-import the XML file that includes the current and new patterns.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<adaptationFullTOList>
    <AdaptationFullTO>
        <notes>this is a test</notes>
        <adaptationmodule>VersionModule param1=17 param2=15</adaptationmodule>
        <egressuriparameters>uri1</egressuriparameters>
        <name>VerisonAdaptation</name>
        <EgressadaptationFullTO>
            <notes>test</notes>
            <deletedigits>1</deletedigits>
            <insertdigits>3</insertdigits>
            <matchingpattern>809</matchingpattern>
            <maxdigits>20</maxdigits>
            <mindigits>3</mindigits>
            <addressToModify>origination</addressToModify>
        </EgressadaptationFullTO>
        <EgressadaptationFullTO>
            <notes>test</notes>
            <deletedigits>1</deletedigits>
            <insertdigits>3</insertdigits>
            <matchingpattern>810</matchingpattern>
            <maxdigits>21</maxdigits>
            <mindigits>3</mindigits>
            <addressToModify>destination</addressToModify>
        </EgressadaptationFullTO>
        <EgressadaptationFullTO>
            <notes>test</notes>
```

```
            <deletedigits>1</deletedigits>
            <insertdigits>3</insertdigits>
            <matchingpattern>811</matchingpattern>
            <maxdigits>22</maxdigits>
            <mindigits>3</mindigits>
            <addressToModify>both</addressToModify>
        </EgressadaptationFullTO>
        <IngressadaptationFullTO>
            <notes>test</notes>
            <deletedigits>1</deletedigits>
            <insertdigits>2</insertdigits>
            <matchingpattern>148</matchingpattern>
            <maxdigits>25</maxdigits>
            <mindigits>3</mindigits>
            <addressToModify>origination</addressToModify>
        </IngressadaptationFullTO>
        <IngressadaptationFullTO>
            <notes>test</notes>
            <deletedigits>1</deletedigits>
            <insertdigits>2</insertdigits>
            <matchingpattern>149</matchingpattern>
            <maxdigits>26</maxdigits>
            <mindigits>3</mindigits>
            <addressToModify>destination</addressToModify>
        </IngressadaptationFullTO>
        <IngressadaptationFullTO>
            <notes>test</notes>
            <deletedigits>1</deletedigits>
            <insertdigits>2</insertdigits>
            <matchingpattern>150</matchingpattern>
            <maxdigits>27</maxdigits>
            <mindigits>3</mindigits>
            <addressToModify>both</addressToModify>
        </IngressadaptationFullTO>
    </AdaptationFullTO>
</adaptationFullTOList>
```

SIP Entities

About SIP Entities

SIP Entities are the network entities that are a part of the SIP System. Examples of SIP Entities include Session Manager instances, Communication Managers, Session Border Controllers (SBCs), and SIP trunks.

Starting with Session Manager Release 6.3.9, you can select **Endpoint Concentrator** as a SIP Entity type. With the **Endpoint Concentrator** type, you can have up to 1000 connections from a single IP address. The single IP address can be shared by multiple Windows instances running on a Virtualized server. SIP Link Monitoring is disabled for this SIP Entity type.

Authentication of trusted SIP entities

Routing uses the following information for the authentication of SIP entities by performing validation on IP/Transport Layer and TLS Layer:

- FQDN or IP Address of the SIP entity
- Credential name of the SIP entity
- Protocol of the Entity Links. This is a SIP connection transport type (TCP/TLS/UDP)
- Connection Policy of the Entity Link (This defines whether the entity link is trusted or not)

For information about administering these fields, see Creating SIP entities and Creating Entity Links.

IP and transport layer validation

When Session Manager receives a request from the network, it validates that:

- The far-end IP address matches the IP address of one of the SIP Entities configured in 'Routing' that have entity links with Session Manager. If a SIP Entity is administered with an FQDN instead of an IP address, Session Manager will resolve the FQDN to an IP address while doing the comparison.
- The transport on which the request was received matches the administered transport of one of the entity links associated with this SIP entity and the Session Manager. The Connection Policy of the entity link must be configured as trusted otherwise Session Manager challenges the request.

For SIP TLS connections, see TLS layer validation section.

TLS layer validation

Session Manager applies the following additional validations for SIP TLS connections:

1. During a TLS handshake, mutual TLS authentication is performed, that is, the Identity Certificate of the SIP entity is validated against the trusted CA certificate repository in the Session Manager for SIP TLS connections. If this verification fails, Session Manager does not accept the connection.
2. If the mutual TLS authentication is successful, further validation is performed on the SIP entity Identity Certificate as per the Credential Name or the far-end IP address.
   - If the Credential Name string is empty, the connection is accepted.
   - If the Credential Name string is not empty, the Credential Name and the IP address of the far-end is searched for in the following fields in the identity certificate provided by the SIP entity:
     - CN value from the subject.

- subjectAltName.dNSName.
- subjectAltName.uniformResourceIdentifier. For IP address comparison, IP address string is converted to SIP:W.X.Y.Z before comparison. W.X.Y.Z is the remote socket IPV4 address. Also, case insensitive search is performed in this case.

SIP Responses to an OPTIONS Request

With OPTIONS messages, Session Manager keeps track of the status of the SIP trunks and forwards calls, without any delay, onto entity links that are up or partially down. A partially down entity link indicates that one of the SIP entities is inaccessible and Session Manager must forward calls to other SIP entities that are accessible. By keeping track of the SIP entities that are inaccessible, Session Manager keeps call performance at an acceptable level and enables load balancing or fail-over configurations without the impact of delayed calls.

Sometimes, especially when interfacing with some third party entities, Session Manager receives nonstandard responses. In these situations, the Session Manager cannot determine whether the SIP entity is up or down. On the SIP Entities Details page, in the **SIP Responses to an OPTIONS Request** section, you can specify the list of specific SIP responses to OPTIONS messages for these SIP Entities so that Session Manager can track the SIP responses.

If you do not set this feature, calls can be delayed. When the Session Manager attempts to route a call over an inaccessible SIP entity, the Session Manager waits a specific time, indicated by “Timer B”, before trying for another SIP entity. If multiple SIP entities are involved, the sum of the wait times can cause substantial delays that might have an impact on service.

Related Links

Session Manager SIP Entity Monitoring on page 502
Handling SIP responses on page 247

Deny new service for entity links

This functionality enables the user to deny new service for entity links. Entity links, that deny new service, do not accept new incoming calls and Session Manager does not route outgoing calls over these links. Link monitoring continues over these links but no alarms are generated for the denied links. You can do the following operations based on the Deny new service functionality for entity links:

- Take selected SIP Entities out of service for upgrades and repair, without receiving numerous SIP Monitoring alarms.
- Test alternate routing paths by denying the primary link used on a given route.
- Deny selected links during a planned WAN outage.

SIP Call Loop elimination

Session Manager can sometimes receive identical INVITE requests within a short interval.

Session Manager sets up separate sessions for each INVITE. The identical INVITE requests can initiate SIP call loops and deplete network resources. Session Manager provides administration features to track and terminate call looping instances in the network.

Loop Administration

Session Manager rejects requests if the number of incoming requests that have the same combination of the **R-URI**, **To**, **From**, and **PAI** header values reaches the administered **Loop Count Threshold** value within the **Loop Detection Interval** time. The frequency of the call loops is a function of the latency and the number of network elements in the loop path. An administrator must set the Loop Detection parameters based on the customer network configuration. Setting improper values of **Loop Count Threshold** and **Loop Detection Interval** can result in:

- System performance overhead.
- Non-detection of call looping scenarios in the network.

For example, if the successive loop call arrives at Session Manager after 40 milliseconds (because of the propagation delay of the intermediate hops) and the administrator needs to break the loop on the fifth loop call instance, the recommended Firewall configuration must have **Loop Count Threshold** set to 5 and **Loop Detection Interval** set to 200 milliseconds. For more information on these fields, see SIP Entity Details - non Session Manager type field descriptions on page 310.

Alarm generation

The Session Manager SIP Firewall generates a minor-level alarm for a call loop detection event based on the Loop Detection parameters settings. You can administer Loop Detection alarms on the Session Manager Administration page. For more information, see Session Manager Administration page field descriptions on page 379.

When an alarm is generated for the Loop Detection event, Session Manager does not generate any more alarms for the administered **Loop Detection Alarm Threshold** interval after the event. For example, if the **Loop Detection Alarm Threshold** is set to 24 hours and a Loop Detection alarm is generated, the SIP Firewall does not generate any new Loop Detection alarms for the next 24 hours. During this interval, the SIP Firewall continues to detect and break loops without generating any new alarms, but continues to log loop detection summary events.

Creating SIP Entities

About this task

To administer minimal routing using Session Manager, you need to configure a SIP entity of type Communication Manager and a second SIP entity of type Session Manager. Use the SIP entities screen to create SIP entities.

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .

2. In the left navigation pane, click **SIP Entities**.
3. Click **New**.
4. In the **Name** field, enter the Name of the SIP entity .
5. Enter the FQDN or IP address of the SIP entity in the **FQDN** or **IP Address** field.
6. Select the type of SIP entity from the drop-down menu in the **Type** field.

   For SIP entity type *Session Manager* follow the instructions as follows and for non-Session Manager type SIP entity, see the related field description topic for details.
7. If you need to specify the location for the SIP entity, in the **Location** field, click a location.
8. If the SIP entity Type is *Session Manager* and you need to specify an Outbound Proxy for the SIP entity, click the drop-down selector for the **Outbound Proxy** field.

   In cases when Session Manager cannot associate any administered routing policies, then the request is sent to the SIP entity administered as an outbound proxy. If no outbound proxy is provisioned, then Session Manager will proxy the request on its own.
9. Enter a regular expression string in the **Credential name** field.

   The Credential name is used for TLS connection validation by searching for this string in the SIP entity identity certificate.

   - If you do not need to perform the additional validation on the SIP entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty.
   - If you need to verify that a specific string or SIP entity FQDN is present within the SIP entity identity certificate, enter that string or SIP entity FQDN using the regular expression syntax.
   - If you need to verify that the SIP entity IP address is present within the SIP entity identity certificate, enter the SIP entity IP address using the regular expression syntax.

   Note:

   IP Address is searched by default when any string is configured in the Credential Name.

   The Credential name is a regular expression string and follows Perl version 5.8 syntax. Here are some examples:

   For `www.sipentity.domain.com`, use the string `www\.sipentity\.domain\.com`.

   For `192.14.11.22`, use string `192\.14\.11\.22`. You can look for a subset of the string or you can create a wild card search. For example, to look for `domain.com` as a substring, use the string `domain\.com`.
10. For non-Session Manager type of SIP Entity, enter the Loop Detection parameters.
11. In SIP Link Monitoring, use the drop-down menu to select one of the following:

    - Use Session Manager Configuration: Use the settings in **Session Manager** > **Session Manager Administration**
    - Link Monitoring Enabled: Enables link monitoring on this SIP entity.

- Link Monitoring Disabled: Link monitoring will be turn off for this SIP entity.

12. If you need to specify the Entity Links, click **Add**.
13. In the **Name** field, enter the name.
14. From the drop-down list, enter the SIP entity 1 by selecting the required **Session Manager** SIP entity and provide the required port.

    SIP entity 1 must always be a Session Manager instance. The default port for TCP and UDP is 5060. The default port for TLS is 5061.
15. Enter the SIP entity 2 by selecting the required non-Session Manager SIP entity from the drop-down list box and provide the required port.

    The port is the port on which you have configured the remote entity to receive requests for the specified transport protocol.
16. Select the Connection Policy for the link using the **Connection Policy** drop-down list box.

    Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities. There are 3 choices:

    - Trusted.
    - Trusted HA: Connection policy for high availability clustered hosts, such as Avaya Aura® Contact Center. It is identical to the “Trusted” Connection Policy except that the TCP Keep Alive window value is 3 seconds.
    - Untrusted.
17. Select the **Deny New Service** checkbox to deny any service for the associated entity link.
18. If you need to specify the Port parameters, click **Add** in Port section.

    When Session Manager receives a request where the host-part of the request-URI is the IP address of Session Manager, it associates one of the administered domains with the port on which the request was received. Add Failover ports if the SIP entity is a failover group member. For details, see *Failover Groups* section.
19. Enter the necessary Port and Protocol parameters.
20. To remove an incorrectly added Port, select the respective **Port** check box and click **Remove**.
21. Add and remove SIP Response Codes and Reason phrases to OPTIONS requests to mark the SIP entity is up or down.
22. Click **Commit**.

Related Links

SIP Entities field descriptions on page 305
SIP Entity Details — Session Manager type field descriptions on page 306
SIP Entity Details field descriptions for other SIP Entity types on page 310

Modifying SIP entities

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **SIP Entities**.
3. Select the SIP entity for modification and click **Edit** .
4. Modify the Name, Fully Qualified Domain Name (FQDN) or IP address of the SIP entity, Type Session Manager, SBC, CM, Voice Portal, Gateway, SIP Trunk, or Other and any other required fields in the first section.
5. If you need to specify the Location for the SIP entity, click the drop-down selector for the **Location** field.
6. If the SIP entity Type is *Session Manager* and you need to specify an Outbound Proxy for the SIP entity, click the drop-down selector for the **Outbound Proxy** field.
7. From the **Time Zone** drop-down list, select the correct time zone
8. Enter or modify a regular expression string in the **Credential name** field.

   Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate.

   - If you do not need to perform the additional validation on SIP entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty.
   - If you need to verify that a specific string or SIP entity FQDN is present within the SIP entity identity certificate, enter that string or SIP entity FQDN using the regular expression syntax.
   - If you need to verify that the SIP entity IP address is present within the SIP entity identity certificate, enter the SIP entity IP address using the regular expression syntax. The system looks for the IP Address by default when any string is configured in the Credential Name.

   Note:

   The Credential name is a regular expression string and follows Perl version 5.8 syntax. Here are some of the examples:

   - For “www.sipentity.domain.com”, use the string “www\.sipentity\.domain\.com”.
   - For “192.14.11.22”, use string “192\.14\.11\.22”.
   - You can search a subset of the string or can create a wild card search. For example, for searching for “domain.com” as a substring, use the string “*domain\.com*”
9. For non-Session Manager type of SIP Entity, enter the Loop Detection parameters.
10. In SIP Link Monitoring, the following options are available from the drop-down menu:
    a. **Use Session Manager Configuration**

b. **Link Monitoring Enabled** : Enables link monitoring on this SIP entity.

c. **Link Monitoring Disabled**: Link monitoring will be turn off for this SIP entity.

11. If you need to specify the Entity Links, click **Add**.
12. Enter the name in the **Name** field.
13. Enter the SIP entity 1 by selecting the required **Session Manager** SIP entity from the drop-down list and provide the required port.

    SIP entity 1 must always be an Session Manager instance. The default port for TCP and UDP is 5060. The default port for TLS is 5061.
14. Enter the SIP entity 2 by selecting the required non-Session Manager SIP entity from the drop-down list and provide the required port.

    This port is the port on which you have configured the remote entity to receive requests for the specified transport protocol.
15. Select the connection policy for the link using the **Connection Policy** drop down list.

    Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities. There are three choices:

    - Trusted.
    - Trusted HA: connection policy for high availability clustered hosts such as Avaya Aura® Contact Center. It is identical to the “Trusted” Connection Policy except that the TCP Keep Alive window value is 3 seconds.
    - Untrusted.
16. Select the **Deny New Service** checkbox to deny any service for the associated entity link.
17. If you need to specify the Port parameters, click **Add** under Port.

    When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.
18. Enter the necessary Port and Protocol parameters.
19. To remove an incorrectly added Port, select the respective **Port** check box and click **Remove**.

    Note:

    - Changes to the protocol and port in the Port section of a Session Manager SIP entity might cause signalling issues in endpoints.
    - Changing a Failover Port on the SIP Entity affects entity links auto-generated during failover and any other entity links which are unrelated to failover but share the same Failover Port.

    When editing a Session Manager SIP entity, if the Session Manager is a member of a Failover Group then changing these port values result in automatically updating the “SIP Entity 1” port value of any Entity Links that have this Session Manager as the “SIP Entity

1". The "SIP Entity 1" port of the entity links gets updated to the new value of "TCP Failover port" if the link has transport protocol TCP or the value of "TLS Failover port" if the transport protocol is TLS. These updates ensure the correct functioning of call preservation routing behavior.

20. Add and remove SIP Response Codes and Reason phrases to OPTIONS requests to mark the SIP entity is up or down.
21. Click **Commit**.

Related Links

SIP Entities field descriptions on page 305
SIP Entity Details — Session Manager type field descriptions on page 306
SIP Entity Details field descriptions for other SIP Entity types on page 310

Deleting SIP Entities

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **SIP Entities**.
3. To delete one or multiple existing SIP entities, select the SIP entity check boxes and click **Delete**.
4. On the confirmation page, click **Delete** or **Cancel**.

Related Links

SIP Entities field descriptions on page 305
Delete Confirmation field descriptions on page 303

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of the SIP entity.

Button	Description
Delete	Deletes the selected SIP entity or entities.
Cancel	Cancels the deletion of the selected SIP entity or entities.

Related Links

Deleting SIP Entities on page 303

Accept new service for all entity links

About this task

Enables the user to accept new service for all entity links of the selected SIP entity.

Procedure

1. On the System Manager console, in **Elements**, click **Routing**.
2. Click **Routing** > **SIP Entities**.
3. On the SIP Entities page, select the sip entities and click **More Actions** > **Accept New Service** to accept any service for all entity links of the selected sip entities.
4. On the Accept New Service Confirmation page, click **Commit**.

Accept New Service Confirmation field descriptions

Use this page to accept new service for all entity links of the selected SIP Entities.

Button	Description
Commit	Accepts new service for all entity links of the selected SIP Entities.
Cancel	Cancels the Accept New Service confirmation.

Deny new service for all Entity Links

About this task

Enables the user to deny new service for all entity links of the selected SIP entity.

Procedure

1. On the System Manager console, in **Elements**, click **Routing**.
2. Click **Routing** > **SIP Entities**.
3. On the SIP Entities page, select the sip entities and click **More Actions** > **Deny new service for all Entity Links** to deny any service for all entity links of the selected sip entities.
4. On the Deny New Service Confirmation page, click **Commit**.

Deny New Service Confirmation field descriptions

Use this page to deny new service for all entity links of the selected SIP Entities.

Button	Description
Commit	Denies new service for all entity links of the selected SIP Entities.
Cancel	Cancels the Deny New Service confirmation.

SIP Entities field descriptions

Use this page to create, modify, delete, and manage SIP entities.

Button	Description
New	Opens the SIP Entity Details page that you can use to create new SIP entities.
Edit	Opens the SIP Entity Details page that you can use to modify the SIP entity.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the SIP entity.
Duplicate	Creates a duplicate of the selected SIP entity and assigns a new state to it.
More Actions > **Display SIP Entity References**	Opens the Overview of References to SIP Entities page which displays the routing policies, adaptations, and locations that correspond to the SIP entity.
More Actions > **Import**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.
More Actions > **Export SIP Entities**	Opens the Export SIP Entities page that allows you to export the SIP entity data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export data for all routing entities as a zipped file to a specified location.
More Actions > **Deny new service for all Entity Links**	Opens the Deny New Service Confirmation page to confirm deny new service for all entity links associated with the selected SIP entities (busyout condition).
More Actions > **Accept new service for all Entity Links**	Opens the Accept New Service Confirmation page to confirm accept new service for all entity links associated with the selected SIP entities (released condition).

Name	Description
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the SIP entity.
Type	SIP entity type, such as a Session Manager, Communication Manager, SIP trunk, or a gateway. **Note:** You can select the SIP entity type as **ELIN Server**. This is used by third party E911 services, which determines a user's location based on IP address, to send the new ELIN to Session Manager in case of emergency call. The SIP Entity selected as the ELIN server should be resolved through local host name resolution to use either the primary or secondary IP address.
Notes	Additional notes about the SIP entity.

Related Links

Creating SIP Entities on page 298
Modifying SIP entities on page 301
Deleting SIP Entities on page 303

SIP Entity Details — Session Manager type field descriptions

Use this page to specify SIP entity details for Session Manager type SIP entity.

General

Name	Description
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the SIP entity.
Type	Session Manager type SIP entity.
Notes	Additional notes about the SIP entity.
Location	SIP entity location. Select from previously defined locations.
Outbound Proxy	Outbound proxy if the entity type is Session Manager, and you wish to specify a proxy.

Table continues…

Name	Description
	Note: In cases when Session Manager cannot associate any administered routing policies, then the request is sent to the SIP entity administered as an outbound proxy. If no outbound proxy is provisioned, then Session Manager will proxy the request on its own.
Time Zone	Default time zone to be used for the entity.
Credential name	The Credential name is used for TLS connection validation by searching for this string in the SIP entity identity certificate. • If you do not want to perform the additional validation on the SIP entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty. • If you want to verify that a specific string or SIP entity FQDN is present within the SIP entity identity certificate, enter that string or SIP entity FQDN using the regular expression syntax. • If you want to verify that the SIP entity IP address is present within the SIP entity identity certificate, enter the SIP entity IP address using the regular expression syntax. **Note:** IP Address is searched by default when any string is configured in the Credential Name. The Credential name is a regular expression string and follows Perl version 5.8 syntax. Here are some examples: For `www.sipentity.domain.com`, use the string `www\.sipentity\.domain\.com`. For `192.14.11.22`, use string `192\.14\.11\.22`. You can look for a subset of the string or you can create a wild card search. For example, to look for `domain.com` as a substring, use the string `domain\.com`

SIP Link Monitoring

Name	Description
SIP Link Monitoring	Select the process for SIP Link monitoring.

Table continues…

Name	Description
Proactive Monitoring Interval (in seconds)	This value is used for polling the administered SIP entities by the added Session Manager. Monitoring ensures that the entities are still reachable. Proactive monitoring occurs as long as no outages are detected. A value between 1 and 9000 is required. The default is 900 seconds.
Reactive Monitoring Interval (in seconds)	This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. A value between 1 and 900 is required. The default is 120 seconds.
Number of Retries	This value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable. A value between 0 and 15 is required. The default is 1.

Entity Links

Button	Description
Add	Adds the selected entity link.
Remove	Removes the selected entity link.

Name	Description
SIP Entity 1	Select a SIP entity from the drop-down list box. This entity must always be a Session Manager instance.
Protocol	Protocol to be used for the entity link.
Port	Port to be used for SIP entity 1. The default port for TCP and UDP is 5060. The default port for TLS is 5061.
SIP Entity 2	Select a SIP entity from the drop-down list box. This entity need not be a Session Manager entity.
Port	Port to be used for SIP entity 2.
Connection Policy	Specifies the policy to use for the entity link. There are 3 choices: • Trusted • Trusted HA — connection policy for high availability clustered hosts such as Avaya Aura® Contact Center. It is identical to the *Trusted* Connection Policy except that the TCP Keep Alive window value is 3 seconds.

Table continues…

Name	Description
	• Untrusted
Deny New Service	Select to deny any service for the associated entity link.

Port

Button	Description
Add	Adds the selected port.
Remove	Removes the selected port.

Name	Description
TCP Failover port	SIP entity TCP failover port.
TLS Failover port	SIP entity TLS failover port. **Note:** • Each Session Manager instance that becomes a failover group member, must designate one failover port per transport type that it supports. Far-end Session Manager instance and failover group peers use this port to forward all call preservation traffic to the Session Manager instance over the transport type. • If the Session Manager is a member of a Failover Group, then changing these port values results in automatically updating the “SIP Entity 1” port value of any Entity Links that have this Session Manager as the “SIP Entity 1”. The update ensures that the “SIP Entity 1” port of the entity links matches the new value of “TCP Failover port” if the link has transport protocol TCP or the value of “TLS Failover port” if the transport protocol is TLS. These updates ensure the correct functioning of call preservation routing behavior.
Port	Add a listening port for the SIP entity.
Protocol	Protocol that the SIP entity uses.
Default Domain	The domain of the SIP entity.
Notes	Additional notes about the port and port parameters.

SIP Responses to an OPTIONS Request

Button	Description
Add	Adds SIP responses that signifies the SIP entity is up or down.
Remove	Removes the selected SIP response.

Name	Description
Response Code & Reason Phrase	Three digit SIP response code and optional reason code signifying that the SIP entity is up or down.
Mark Entity Up/Down	Mark the SIP entity up or down when it responds to an OPTIONS request as per the administered Response Code & Reason Phrase.
Notes	Additional notes about the responses.

Button	Description
Commit	Saves the SIP entity and distributes it to the Session Managers in the enterprise.
Cancel	Cancels the creation or modification of the SIP entity.

Related Links

Creating SIP Entities on page 298
Modifying SIP entities on page 301

SIP Entity Details field descriptions for other SIP Entity types

The following tables contain the SIP Entity field descriptions for a SIP Entity that is not of **Type** Session Manager.

Note:

Not all of the fields are applicable to all SIP Entity types.

General

Name	Description
Name	SIP Entity name. The name must be unique and have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the SIP Entity.
Type	Non-Session Manager type SIP Entity, such as Communication Manager, SIP trunk, or a gateway.

Table continues…

Name	Description
	Note: • You can select the SIP Entity type as **ELIN Server**. This is used by third party E911 services, which determines a user's location based on IP address, to send the new ELIN to the Session Manager for an emergency call. The SIP Entity selected as the ELIN server should be resolved through local host name resolution to use either the primary or secondary IP address. • You can select SIP Entity type as **Survivability Server** for a B5800 Branch Gateway (or Advanced Gateway / Secure Routers and other non-PPM capable devices) for providing local 96xx / 96x1 SIP survivability.
Notes	Notes about the SIP Entity.
Adaptation	Assigned adaptation.
Location	The SIP Entity location. Select from previously defined locations.
Time Zone	Default time zone to be used for the entity.
SIP Timer B/F (in seconds)	Amount of time the Session Manager waits for the response from the SIP Entity. The range is 1–32. The default value is 4 seconds.
Credential name	The Credential name is used for TLS connection validation by searching for this string in the SIP Entity identity certificate. • If you do not want to perform the additional validation on the SIP Entity identity certificate or are not using SIP TLS for connecting to the SIP Entity, leave this field blank. • To verify that a specific string or SIP Entity FQDN is present within the SIP Entity identity certificate, enter the string or SIP Entity FQDN using the regular expression syntax. • To verify that the SIP Entity IP address is present within the SIP Entity identity certificate, enter the SIP Entity IP address using the regular expression syntax. **Note:** The IP Address is searched by default when any string is configured in the Credential Name.

Table continues…

Name	Description
	The Credential name is a regular expression string and follows Perl version 5.8 syntax. Some examples are: For “www.sipentity.domain.com”, use the string “www\.sipentity\.domain\.com”. For “192.14.11.22”, use string “192\.14\.11\.22”. You can look for a subset of the string or you can create a wild card search. For example, to look for “domain.com” as a substring, use the string “domain\.com”
Call Detail Recording	Call Detail Recording (CDR) settings. If CDR is enabled on a Session Manager, a CDR record is generated for a call originating from a SIP Entity depending on the following settings: • none: CDR is not generated for the calls involving the entity. • ingress: CDR is generated only for calls from the entity. • egress: CDR is generated only for calls to the entity. • both: CDR is generated for call either to or from the entity. If two entities are involved in a call, the CDR settings are combined to determine whether a record should be generated. For instance, if the Session Manager routes a call from entity1 to entity2, and the CDR setting of entity1 is “none” but the CDR setting of entity2 is “ingress” or “both” then a record is generated.
CommProfile Type Preference	This field is visible for the SIP Entity type *Other* only and displays list of all of the administered **CommProfile** types that can be used with this SIP Entity type.

Loop Detection

Name	Description
Loop Detection Mode	The default value is **Off**. The **On** option activates Loop Detection monitoring for all the Entity Links associated with the SIP Entity.

Table continues…

Name	Description
	The **Test Only** option allows the administrator to test and change the settings without rejecting the live calls.
Loop Count Threshold	The default value is 5. The allowed range is 2 to 10,000.
Loop Detection Interval (in msec)	The default value is 200 msec. The allowed range is 10ms to 10,000ms.

SIP Link Monitoring

Name	Description
SIP Link Monitoring	Select the process for SIP Link monitoring.
Proactive Monitoring Interval (in seconds)	This value is used for polling the administered SIP Entities by the added Session Manager. Monitoring ensures that the entities are still reachable. Proactive monitoring occurs as long as no outages are detected. A value between 1 and 9000 is required. The default value is 900 seconds.
Reactive Monitoring Interval (in seconds)	This value is used when proactive monitoring detects that an administered SIP Entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP Entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. A value between 1 and 900 is required. The default value is 120 seconds.
Number of Retries	This value specifies the number of times the Session Manager polls a SIP Entity before the SIP Entity is considered unreachable. A value between 0 and 15 is required. The default value is 1.
Supports Call Admission Control	Enable or disable CAC management for the SIP Entity. If enabled, the Session Manager does not perform CAC on outgoing calls.
Shared Bandwidth Manager	Enable or disable Shared Bandwidth attribute for this SIP Entity. If this option is checked, you must further specify one or two Session Manager instances that supports the PUBLISH API to this SIP Entity.
Primary Session Manager Bandwidth Association	Primary Session Manager instances that supports the PUBLISH API to this SIP Entity.
Backup Session Manager Bandwidth Association	Backup Session Manager instances that supports the PUBLISH API to this SIP Entity, in case the primary fails.

Entity Links

Name	Description
Override Port & Transport with DNS SRV	Select the check box to override Local Host Name Resolution or DNS routing. • If you select this option, the transport and port information is determined using DNS information. You must administer entity links for each transport protocol used to connect to or from the remote entity. • If you do not select this option, the transport and port information is determined using the data administered in the Entity Link table. However, FQDNs are resolved to IP addresses using a DNS server and the Local Hostname Resolution table entries, and only the port and transport data is derived from the Entity Link table.

Button	Description
Add	Adds the selected entity link.
Remove	Removes the selected entity link.

Name	Description
SIP Entity 1	Select a SIP Enity from the drop-down list.
Protocol	Protocol to be used for the entity link.
Port	Port to be used for SIP Entity 1. Range is 1 to 65535.
SIP Entity 2	Select a SIP Entity from the drop-down list.
Port	Port to be used for SIP Entity 2. Range is 1 to 65535. **Note:** If you select the **Override Port & Transport with DNS SRV** check box, this field is disabled and the port identified in the DNS SRV or LHNR is used.
Connection Policy	Specifies the policy to use for the entity link. • Trusted. • Trusted HA — connection policy for high availability clustered hosts such as Avaya Aura® Contact Center. This policy is identical to the *Trusted* Connection Policy except that the TCP Keep Alive window value is 3 seconds. • Untrusted.

Table continues…

Name	Description
	• endpt conc — connection policy for the SIP Entities hosting endpoint concentrators.
Deny New Service	Select the check box to deny any service for the associated entity link.

SIP Responses to an OPTIONS Request

Button	Description
Add	Adds SIP responses that signify if the SIP Entity is up or down.
Remove	Removes the selected SIP response.

Name	Description
Response Code & Reason Phrase	Three digit SIP response code and optional reason code signifying that the SIP Entity is up or down.
Mark Entity Up/Down	Mark the SIP Entity as up or down when it responds to an OPTIONS request according to the administered Response Code & Reason Phrase.
Notes	Notes about the responses.

Button	Description
Commit	Saves the SIP Entity and distributes the information to the Session Managers in the enterprise.
Cancel	Cancels the creation or modification of the SIP Entity.

Related Links

Creating SIP Entities on page 298
Modifying SIP entities on page 301

Bulk import for SIP Entities

Follow these rules when creating an XML bulk import file:

- The name of a SIP Entity is unique and is referred to by other elements.
- <adaptationName> must either be empty or refer to an existing adaptation with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the SIP Entity. SIP Entity of type *ASM* <Avaya Session Manager> cannot contain an adaptation entry.
- <adaptationName> contains the adaptation module name and parameters separated by spaces <examples below>.
- Listen ports (<listenports>) are only relevant for SIP Entity of type *ASM*. Do not include these entries for any other type of SIP Entity.

- Multiple listen ports entries (<listenports>) can be configured for one ASM SIP Entity.
  - <sipdomainName> must refer to an existing domain with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the SIP Entity.
  - The values in <transportprotocol> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.
- The values of <timezoneName> should be same (being case sensitive) as that of the field *Time Zone* in the SIP Entity user interface in System Manager.
- The field <userfc3263> corresponds to the *Override Port & Transport with DNS SRV* check box in the SIP entity form.
- The value of <entitytype> must contain one of the following values, being case sensitive, must exactly appear as follows:
  - CM: Communication Manager in the user interface.
  - ASM: Session Manager in the user interface.
  - Modular Messaging: Session Manager in the user interface.
  - VP: Voice Portal in the user interface.
  - Gateway: Gateway in the user interface.
  - SIP Trunk: SIP Trunk in the user interface.
  - OTHER: Other in the user interface.
- The values in <cdrSetting> must appear exactly same being case sensitive, as they appear in the System Manager user interface.
- The field <do_monitoring> corresponds to the field *SIP Link Monitoring* in the SIP Entity details form. The relation is as follows:
  - In order to enable SIP Link monitoring, <do_monitoring> value must be *yes*.
  - In order to disable SIP Link monitoring, <do_monitoring> value must be *no*.
  - In order to use the Session Manager configuration, the <do_monitoring> tag must be completely omitted.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sipentityFullTOList>
    <SipentityFullTO>
        <notes>this is a test</notes>
        <entitytype>CM</entitytype>
        <fqdnoripaddr>9.8.7.6</fqdnoripaddr>
        <name>BerlinCM</name>
        <adaptationName>VerisonAdaptation param1=12 param2=14</adaptationName>
        <cdrSetting>egress</cdrSetting>
        <credentialname>credential test</credentialname>
        <do_monitoring>yes</do_monitoring>
        <monitor_proactive_secs>900</monitor_proactive_secs>
        <monitor_reactive_secs>120</monitor_reactive_secs>
        <monitor_retries>1</monitor_retries>
        <routingoriginationName>Berlin</routingoriginationName>
```

```
        <timer_bf_secs>4</timer_bf_secs>
        <timezoneName>Europe/Berlin</timezoneName>
        <userfc3263>false</userfc3263>
    </SipentityFullTO>
    <SipentityFullTO>
        <notes>this is a test</notes>
        <entitytype>CM</entitytype>
        <fqdnoripaddr>9.8.7.5</fqdnoripaddr>
        <name>NewYorkCM</name>
        <adaptationName>VerisonAdaptation param1=7 param2=8</adaptationName>
        <cdrSetting>egress</cdrSetting>
        <credentialname>credential test</credentialname>
        <do_monitoring>yes</do_monitoring>
        <monitor_proactive_secs>900</monitor_proactive_secs>
        <monitor_reactive_secs>120</monitor_reactive_secs>
        <monitor_retries>1</monitor_retries>
        <routingoriginationName>New York</routingoriginationName>
        <timer_bf_secs>4</timer_bf_secs>
        <timezoneName>America/New_York</timezoneName>
        <userfc3263>false</userfc3263>
    </SipentityFullTO>
    <SipentityFullTO>
        <notes>this is a test</notes>
        <entitytype>ASM</entitytype>
        <fqdnoripaddr>4.5.6.7</fqdnoripaddr>
        <name>SessionManager1</name>
        <cdrSetting>egress</cdrSetting>
        <credentialname>credential test</credentialname>
        <do_monitoring>use-instance</do_monitoring>
        <listenports>
            <notes>this is a test</notes>
            <portnumber>5067</portnumber>
            <sipdomainName>avaya.com</sipdomainName>
            <transportprotocol>TLS</transportprotocol>
        </listenports>
        <monitor_proactive_secs>900</monitor_proactive_secs>
        <monitor_reactive_secs>120</monitor_reactive_secs>
        <monitor_retries>1</monitor_retries>
        <routingoriginationName>New York</routingoriginationName>
        <timer_bf_secs>4</timer_bf_secs>
        <timezoneName>America/New_York</timezoneName>
        <userfc3263>false</userfc3263>
    </SipentityFullTO>
</sipentityFullTOList>
```

SIP Entity References

About SIP Entity References

Using Session Manager, you can see all references to a SIP entity, such as its location, the routing policy that is created for the SIP entity, and adaptations, if any. If a single SIP entity has more than one combination of these references, Session Manager displays each of the combinations on a separate row.

Displaying SIP Entity References

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **SIP Entities**.
3. From the SIP Entity menu, select the check box for a SIP entity whose references you need to see.
4. From the **More Actions** drop-down list, select **Display SIP Entity References**.

   Session Manager displays the overview of SIP entity references such as the entity location, name of the routing policy attached to the entity, and adaptations, if any.
5. Click **Back** to navigate to the SIP entities.

Related Links

Overview of References to SIP Entities field descriptions on page 318

Overview of References to SIP Entities field descriptions

Use this page to view information about the SIP entity references associated with the selected SIP entity.

Name	Description
SIP Entity Name	Lists the names of the SIP entities.
Location Name	Lists the location associated with the specified SIP entity.
Routing Policy Name	Lists the routing policy associated with the specified SIP entity.
Adaptation Name	Lists the name of the adaptation associated with the SIP entity.

Button	Description
Back	Returns to the **SIP Entities** page.

Related Links

Displaying SIP Entity References on page 318

Entity Links

Entity Links

You must configure an entity link between Session Manager and any administered SIP entity for Session Manager to send or receive messages directly from the entity.

To communicate with other SIP entities in the network, each Session Manager instance must identify the port and the transport protocol of its entity link to the SIP entities. The Session Manager listens on the local port for connections from the remote entity using the given transport protocol. If the **Override Port & Transport** check box is selected for the SIP entity, the port that connects to the remote entity is taken from local host name resolution or DNS.

Routing entity links connect two SIP entities through the Session Manager to define the network topology for SIP routing.

- Entity Links are configured to connect two SIP entities.
- Trusted Hosts are indicated by assigning the *Trust State* to the link that connects the entities.

Deny new service for entity links

This functionality enables the user to deny new service for entity links. Entity links, that deny new service, do not accept new incoming calls and Session Manager does not route outgoing calls over these links. Link monitoring continues over these links but no alarms are generated for the denied links. You can do the following operations based on the Deny new service functionality for entity links:

- Take selected SIP Entities out of service for upgrades and repair, without receiving numerous SIP Monitoring alarms.
- Test alternate routing paths by denying the primary link used on a given route.
- Deny selected links during a planned WAN outage.

Creating Entity Links

Procedure

1. On the System Manager Web Console, under **Elements**, click **Routing** > **Entity Links**.
2. Click **New**.
3. Enter the name in the **Name** field.
4. Enter the SIP entity 1 by selecting the required **Session Manager** SIP entity from the drop-down list and provide the required port.

   SIP entity 1 must always be a Session Manager instance.

Comments on this document? infodev@avaya.com

The default port for TCP and UDP is 5060. The default port for TLS is 5061.

5. Enter the SIP entity 2 by selecting the required non-Session Manager SIP entity from the drop-down list and provide the required port.

   The port is the port on which you have configured the remote entity to receive requests for the specified transport protocol.

6. From the **Connection Policy** drop-down menu, select **Trusted**.

   Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.

7. Click **Commit**.

Related Links

Entity Links field descriptions on page 322

Modifying Entity Links

Procedure

1. On the System Manager Web Console, under **Elements**, click **Routing** > **Entity Links**.
2. Select an entity link for modification and click **Edit**.
3. Modify the name in the **Name** field if required.
4. If required, modify the SIP entity 1 by selecting the required **Session Manager** SIP entity 1 from the drop-down list and provide the required port.

   SIP entity 1 must always be a Session Manager instance.

5. If required, modify the SIP entity 2 by selecting the required SIP entity from the drop-down list and provide the required port.
6. From the **Connection Policy** drop-down menu, select **Trusted**.
7. Click **Commit**.

Related Links

Entity Links field descriptions on page 322

Deleting Entity Links

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Entity Links**.
3. To delete an existing link or links, select the respective check boxes and click **Delete**.
4. On the confirmation page, click **Delete**.

Related Links

Delete Confirmation field descriptions on page 321
Entity Links field descriptions on page 322

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of SIP entity links.

Button	Description
Delete	Deletes the SIP entity link entries from the database.
Cancel	Cancels the deletion of SIP entity links and returns to the SIP entity Links page.

Related Links

Deleting Entity Links on page 320

Accept new service for the selected Entity Links

About this task

Enables the user to accept new service for the selected Entity Links.

Procedure

1. On the System Manager console, in **Elements**, click **Routing**.
2. Click **Routing** > **Entity Links**.
3. On the Entity Links page, select the Entity Links and click **More Actions** > **Accept new service for selected Entity Links** to accept any service for the selected entity links.
4. On the Accept New Service Confirmation page, click **Commit**.

Accept New Service Confirmation field descriptions

Use this page to accept new service for selected Entity Links.

Button	Description
Commit	Accepts new service for the selected Entity Links.
Cancel	Cancels the Accept New Service confirmation.

Deny new service for selected Entity Links

About this task

Enables the user to deny new service for selected entity links.

Procedure

1. On the System Manager console, in **Elements**, click **Routing**.
2. Click **Routing** > **Entity Links**.
3. On the Entity Links page, select the Entity Links and click **More Actions** > **Deny new service for selected Entity Links** to deny any service for selected entity links.
4. On the Deny New Service Confirmation page, click **Commit**.

Deny New Service Confirmation field descriptions

Use this page to deny new service for selected entity links.

Button	Description
Commit	Denies new service for the selected SIP entity links.
Cancel	Cancels the Deny New Service confirmation.

Entity Links field descriptions

Use this page to create, modify, delete, and manage entity links.

Button	Description
New	Opens the Entity Links page that you can use to create new entity links.
Edit	Opens the Entity Links page that you can use to modify the entity link details.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the entity link.
Duplicate	Creates a duplicate of the selected entity link and assigns a new state to it.
More Actions > **Import**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.

Table continues…

Button	Description
More Actions > **Export Entity Links**	Opens the Export Entity Links page that allows you to export the entity links data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export the data for all routing elements as a zipped file to a specified location.
More Actions > **Deny new service for selected Entity Links**	Opens the Deny New Service Confirmation page to confirm deny new service for selected entity links.
More Actions > **Accept new service for selected Entity Links**	Opens the Accept New Service Confirmation page to confirm accept new service for selected entity links.

Name	Description
Name	Name of the SIP entity link. This name must be unique and can have 3 to 64 characters.
SIP Entity 1	Name of the SIP entity 1. These are SIP entities of type Session Manager.
Protocol	Protocol to be used for the entity link.
Port	Port to be used for SIP entity 1. The default port for TCP and UDP is 5060. The default port for TLS is 5061.
SIP Entity 2	Name of the SIP entity 2. These are the non-Session Manager type SIP entities.
DNS Override	Indicates that the **Override Port & Transport with DNS SRV** checkbox is selected on the *SIP Entity Details* page.
Port	Port to be used for SIP entity 2.
Connection Policy	Specifies the policy to use for the entity link. There are 3 choices: • Trusted • Trusted HA — connection policy for high availability clustered hosts such as AACC. It is identical to the “Trusted” Connection Policy except that the TCP Keep Alive window value is 3 seconds. • Untrusted
Deny New Service	Select to deny any service for the associated entity links.
Notes	Any details or notes that you wish to add.

Related Links

Creating Entity Links on page 319
Modifying Entity Links on page 320

Deleting Entity Links on page 320

Bulk import for Entity Links

Conform to the following rules while creating an XML bulk import file:

- The name of an Entity Link must be unique.
- <entityName1> , <entityName2> must refer to an existing SIP Entity with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Entity Link.
- The values in <transportProtocol> must appear exactly same, being case sensitive, as they appear in the System Manager user interface.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<entitylinkFullTOList>
    <EntitylinkFullTO>
        <notes></notes>
        <listenPortEntity1>5061</listenPortEntity1>
        <listenPortEntity2>5061</listenPortEntity2>
        <name>SessionManager1_BerlinCM_5061_TLS</name>
        <transportProtocol>TLS</transportProtocol>
        <trusted>true</trusted>
        <entityName1>SessionManager1</entityName1>
        <entityName2>BerlinCM</entityName2>
    </EntitylinkFullTO>
    <EntitylinkFullTO>
        <notes></notes>
        <listenPortEntity1>5061</listenPortEntity1>
        <listenPortEntity2>5061</listenPortEntity2>
        <name>NewYorkCM-SessionManager1-TLS</name>
        <transportProtocol>TLS</transportProtocol>
        <trusted>true</trusted>
        <entityName1>SessionManager1</entityName1>
        <entityName2>NewYorkCM</entityName2>
    </EntitylinkFullTO>
</entitylinkFullTOList>
```

Time Ranges

About Time Ranges

Time Ranges indicate the time values for the time of day, Time Range, related routing for Routing Policies. Time Ranges can be interpreted as the UTC offset of the particular time zone.

You must specify as many Time Ranges as necessary to cover all hours and days in a week for each administered Routing Policy.

For example, Routing Policy A can be in effect on all weekdays from 9:00 a.m. to 5:59 p.m., Routing Policy B can be in effect on all weekdays from 6:00 p.m. to 9 a.m., and Routing Policy C time ranges can be in effect on weekends. These three Time Ranges together cover how calls should be routed throughout the week.

Routing Policies that a Session Manager server selects can be prioritized based on time-of-day routing information. Based on this selection, Session Manager:

- determines the current time at the destination entity. The current time on Session Manager is converted to the time at the destination SIP Entity using the administered time zone.
- finds the Time Range that you administered. The Time Range contains the time at the destination.
- finds the rank that you administered on the Routing Policy for the selected Time Range.

After the selection, Session Manager orders the Routing Policies in ascending order and tries one route in each priority as per the administered order.

Note:

Priorities must not overlap, but if the priorities overlap, the order of routing policies that have the same priorities will be random.

Creating Time Ranges

About this task

You can use the Time Ranges screen to administer time ranges with start and end times.

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Time Ranges**.
3. Click **New**.
4. Enter the name, select the required days by entering the start and end times and notes for the new time range. Start times start with the first second of the hour:minute. End Times go through the last second of the end hour:minute.
5. Click **Commit**.

Related Links

Time Ranges field descriptions on page 326
Time Range List field descriptions on page 327

Modifying Time Ranges

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .

2. In the left navigation pane, click **Time Ranges**.
3. Select a time range for modification and click **Edit**.
4. If required, modify the name.
5. If required, modify the days by modifying the start and end times and notes. Start times start with the first second of the start hour:minute. End Times go through the last second of the end hour:minute.
6. Click **Commit**.

Related Links

Time Ranges field descriptions on page 326
Time Range List field descriptions on page 327

Deleting Time Ranges

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Time Ranges**.
3. To delete an existing time range or ranges, select the respective check boxes and click **Delete**.
4. Click **Delete** on the confirmation page.

Related Links

Time Ranges field descriptions on page 326
Delete Confirmation field descriptions on page 326

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of time ranges.

Button	Description
Delete	Deletes the selected time ranges from the database.
Cancel	Cancels the deletion of the selected time ranges.

Related Links

Deleting Time Ranges on page 326

Time Ranges field descriptions

Use the Time Ranges page to create, modify, delete, and manage time ranges.

Button	Description
New	Opens the Time Ranges page where you can create new time ranges.
Edit	Opens the Time Ranges page where you can modify the time range details.
Delete	Opens the Delete Confirmation page for confirming or canceling the deletion of the time range.
Duplicate	Creates a duplicate of the selected time range and assigns a new state to it.
More Actions > **Import**	Opens the Import data page where you can import the time ranges from XML files or zip file containing one or more XML files.
More Actions > **Export Time Ranges**	Opens the Export Time Ranges page where you can export the time ranges data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page where you can export data for all the routing entities as a zipped file to a specified location.

Field	Description
Name	Name for the time range.
Days (Mo to Su)	Days of the week for which the time range is defined.
Start Time	Start time for the time range. Use 24-hour time format.
End Time	End time for the time range. Use 24-hour time format.
Notes	Additional notes.

Related Links

Creating Time Ranges on page 325
Modifying Time Ranges on page 325
Deleting Time Ranges on page 326

Time Range List field descriptions

Use this page to define or modify a Time Range.

Name	Description
Name	Name for the Time Range. It can have between three and 64 characters. The name cannot contain the following characters:

Table continues…

Name	Description
	<, >, ^, %, $, @, #, *
Mon to Sun	Selected check box indicates the days of the week applicable for the Time Range.
Start Time	Start time for the Time Range. For a 24–hour Time Range, the start time is 0.00.
End Time	End time for the Time Range. For a 24–hour Time Range, the end time is 23:59.
Notes	Additional notes about the Time Range.

Button	Description
Select	Selected Time Range is assigned to the Routing Policy.
Cancel	Cancels the changes to the Time Range.

Related Links

Creating Time Ranges on page 325
Modifying Time Ranges on page 325

Bulk import for Time Ranges

Conform to the following rules while creating an XML bulk import file:

- The name of a Time Range must be unique and is referred to by other elements.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<timerangeFullTOList>
    <TimerangeFullTO>
        <notes>this is a test</notes>
        <includesFriday>true</includesFriday>
        <includesMonday>true</includesMonday>
        <includesSaturday>false</includesSaturday>
        <includesSunday>false</includesSunday>
        <includesThursday>true</includesThursday>
        <includesTuesday>true</includesTuesday>
        <includesWednesday>true</includesWednesday>
        <name>regularweek</name>
        <startTime>00:00:00</startTime>
        <stopTime>23:59:00</stopTime>
    </TimerangeFullTO>
    <TimerangeFullTO>
        <notes></notes>
        <includesFriday>false</includesFriday>
        <includesMonday>false</includesMonday>
        <includesSaturday>true</includesSaturday>
        <includesSunday>true</includesSunday>
        <includesThursday>false</includesThursday>
        <includesTuesday>false</includesTuesday>
        <includesWednesday>false</includesWednesday>
        <name>weekend</name>
```

```
        <startTime>00:00:00</startTime>
        <stopTime>23:59:00</stopTime>
    </TimerangeFullTO>
    <TimerangeFullTO>
        <notes>Time Range 24/7</notes>
        <includesFriday>true</includesFriday>
        <includesMonday>true</includesMonday>
        <includesSaturday>true</includesSaturday>
        <includesSunday>true</includesSunday>
        <includesThursday>true</includesThursday>
        <includesTuesday>true</includesTuesday>
        <includesWednesday>true</includesWednesday>
        <name>24/7</name>
        <startTime>00:00:00</startTime>
        <stopTime>23:59:00</stopTime>
    </TimerangeFullTO>
</timerangeFullTOList>
```

Routing Policies

About Routing Policies

All *Routing Policies* together form the *enterprise wide dial plan*.

Routing Policies can include the *Origination of the caller*, the *dialed digits* of the called party, the *domain* of the called party and the actual time the call occurs.

Optionally, you can define a *regular expression* instead of the *dialed digits* of the called party and the *domain* of the called party.

Session Manager determines the destination of the call depending on one or more inputs as mentioned above.

If you qualify the destination using *deny*, then Session Manager does not routes the call.

Session Manager uses the data configured in the routing policy to find the best match against the number or address of the called party.

Note:

If Session Manager cannot match any dial patterns, then Session Manager attempts to find a matching regular expression. Session Manager examines each regular expression in the administered Rank Order and determines if it matches the request-URI. During this comparison, user parameters are not stripped, however, the request-URI is compared against each regular expression twice. The first time, the entire request-URI is compared. The second time, if there is no match, only user@host is compared, that is the URI scheme, sip:, sips:, tel:, and any URI parameters appearing after the host-part of the request-URI are stripped. If there is a match, then Session Manager selects routing policies as per the administered regular expressions.

Use the Routing Policies page to create and modify routing policies.

Creating Routing Policies

Procedure

1. On the System Manager Web Console, under **Elements**, click **Routing** > **Routing Policies**.
2. To add a new routing policy, click **New**.
3. Under the **General** section, enter a routing policy name and notes in the relevant fields.
4. In the **Retries** field, enter the number of retries for the destination SIP entity.

   Note:

   The default value in **Retries** field is zero. The valid values are 0-5.
5. Select the **Disabled** check box to disable the routing policy.
6. Under the **SIP Entities as Destination** section, click **Select** to select the destination SIP entity for this routing policy.
7. Select the required destination and click **Select**.
8. Under the **Time of Day** section, click **Add** to associate the Time of Day routing parameters with this Routing Policy.
9. Select the Time of Day patterns that you want to associate with this routing pattern and click **Select**.

   If there are gaps in the selected Time of Day coverage pattern, the Session Manager displays a warning message. If such gaps exist in the Time of the Day coverage, randomness in routing selections may be observed.
10. Enter the relative Rankings that you want to associate with each Time Range. Lower ranking values indicate higher priority.
11. Under the Dial Patterns and Regular Expressions sections, click **Add** to associate existing Dial Patterns and Regular Expressions with the Routing Policy.
12. Select a dial pattern from the pattern list or a regular expression from the regular expression list, and click **Select**.

    Note:

    This field can be left blank. The routing policy can be added to the dial pattern or regular expression when you add it.
13. Under the Dial Patterns and Regular Expressions sections, click **Remove** to dissociate existing Dial Patterns and Regular Expressions with the Routing Policy.
14. Select a dial pattern from the pattern list or a regular expression from the regular expression list, and click **Select**.
15. Click **Commit**.

Related Links

Routing Policies field descriptions on page 333
Routing Policy Details field descriptions on page 334
SIP Entity List field descriptions on page 336
Pattern List field descriptions on page 337
Regular Expression List field descriptions on page 338

Modifying Routing Policies

Procedure

1. On the System Manager Web Console, under **Elements**, click **Routing** > **Routing Policies** .
2. Select a routing policy for modification and click **Edit**.
3. In the **General** section, modify a routing policy name and add notes in the relevant fields if required.
4. In the **Retries** field, enter the number of retries for the destination SIP entity.

   Note:

   The default value in **Retries** field is zero. The valid values are 0-5.
5. Select the **Disabled** check box to disable the routing policy.
6. In the **SIP Entities as Destination** section, click **Select** to select another destination SIP entity for this routing policy if required.
7. Select the required destination and click **Select**.
8. In the **Time of Day** section, click **Add** to associate another Time of Day routing parameters with this Routing Policy, if required.
9. Select the Time of Day patterns that you want to associate with this routing pattern and click **Select**.

   If there are gaps in the selected **Time of Day** coverage pattern, the Session Manager displays a warning message. If such gaps exist in the Time of the Day coverage, randomness in routing selections may be observed.
10. Enter the relative rankings that you want to associate with each Time Range. Lower ranking values indicate higher priority.
11. If you need to dissociate the Time of Day routing parameters from this Routing Policy, click **Remove** from the Time of Day section.
12. In Dial Patterns or Regular Expressions, click **Add** to associate existing Dial Patterns and Regular Expressions with the Routing Policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**.

If you have not specified the dial patterns or regular expressions, you can add the routing policy to the dial pattern or regular expression when you add them later.

13. In **Dial Patterns or Regular Expressions**, click **Remove** to dissociate existing Dial Patterns and Regular Expressions with the Routing Policy.
14. Select another dial pattern, if required, from the pattern list or a regular expression from the regular expression list and click **Select**.
15. Click **Commit**.

Related Links

Routing Policies field descriptions on page 333
Routing Policy Details field descriptions on page 334
SIP Entity List field descriptions on page 336
Pattern List field descriptions on page 337
Regular Expression List field descriptions on page 338

Deleting Routing Policies

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Routing Policies**.
3. To delete an existing routing policy or routing policies, select the respective check boxes and click **Delete**.
4. Click **Delete** on the confirmation page.

Note:

If you delete a routing policy, all dial patterns and regular expressions that are linked only to the routing policy, you are going to delete, are also deleted.

Related Links

Routing Policies field descriptions on page 333
Delete Confirmation field descriptions on page 332

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of the routing policy.

Button	Description
Delete	Deletes the selected routing policy as well as any dial patterns and regular expressions that are associated *only* with this routing policy.
Cancel	Cancels the deletion of the routing policy.

Related Links

Deleting Routing Policies on page 332

Routing Policies field descriptions

Use this page to create, modify, delete, and manage routing policies.

Button	Description
New	Opens the Routing Policy Details page that you can use to create a new routing policy.
Edit	Opens the Routing Policy Details page that you can use to modify the routing policy.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the routing policy.
Duplicate	Creates a duplicate of the selected routing policy and assigns a new state to it.
More Actions > **Import**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.
More Actions > **Export Routing Policies**	Opens the Export Routing Policies page that allows you to export the routing policy data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export data for all the routing entities as a zipped file to a specified location.

Name	Description
Name	Name of the routing policy.
Disabled	Specifies that the routing policy is to be disabled and should not be used.
Retries	Number of retries for the destination SIP entity. The default value is zero, but the valid values are 0-5.
Destination	SIP Entity as Destination.
Notes	Additional notes about the routing policy.

Related Links

Creating Routing Policies on page 330
Modifying Routing Policies on page 331
Deleting Routing Policies on page 332

Routing Policy Details field descriptions

Use this page to specify the details for creating or modifying a routing policy.

General section

Name	Description
Name	Name of the routing policy.
Disabled	Selecting this check box specifies that the routing policy is to be disabled and should not be used.
Retries	
Notes	Additional notes about the routing policy.

SIP Entity as Destination section

Button	Description
Select	Opens the SIP entity List page. You can use this page to select a SIP entity as a destination and associate it to the selected routing policy.

Name	Description
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the SIP entity.
Type	SIP entity type, such as a Session Manager , Communication Manager, SIP trunk, or a gateway.
Notes	Additional notes about the SIP entity.

Time of Day section

Button	Description
Add	Adds a new time of the day to the selected routing policy.
Remove	Removes the selected time of day entry from the selected routing policy.
View Gaps/Overlaps	Selecting a time of day entry and selecting **View Gaps/Overlaps** generates a Duration Lists report and displays if there are any gaps or overlaps in the time of day entries for each day of the week.

Name	Description
Ranking	Ranking of the assigned Time Ranges.

Table continues…

Name	Description
Name	Name of the Time Ranges.
Days (Mo to Su)	Days of the week specified for the time range.
Start Time	Start Time of the Time Range.
End Time	End Time of the Time Range.
Notes	Additional notes.

Dial Patterns section

Button	Description
Add	Adds a new dial pattern to the selected routing policy.
Remove	Removes the selected dial pattern from the selected routing policy.

Name	Description
Pattern	Dial pattern to match. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.
Emergency Call	Indicate if it is an emergency call.
SIP Domain	Domain for which you want to restrict the dial pattern.
Originating Location	Origination Location Name.
Notes	Additional Notes.

Regular Expressions section

Button	Description
Add	Adds a new regular expression to the selected routing policy.
Remove	Removes the selected regular expression from the selected routing policy.

Name	Description
Pattern	Regular expression pattern that Session Manager tries to match.
Rank Order	Priority of the pattern. A lower rank order means higher priority.
Deny	Denies routing for a matched regular expression pattern.
Notes	Additional Notes.

Button	Description
Commit	Saves the routing policy changes and distributes the changes to the Session Manager instances in the enterprise.
Cancel	Cancels modifications to the routing policy.

Related Links

Creating Routing Policies on page 330
Modifying Routing Policies on page 331

SIP Entity List field descriptions

Use this page to select and associate SIP entities to a routing policy.

Name	Description
Name	Select a SIP entity name check box from the list to associate it to the selected routing policy.
FQDN or IP Address	Displays the fully qualified domain name or IP address of the SIP entity.
Type	Displays the type of the SIP entity such as Session Manager, Session Border Controller, Communication Manager, Voice Portal, Gateway, SIP Trunk, or Other entities.
Notes	Additional notes.

Button	Description
Select	Confirm selection of the SIP entity for associating to the routing policy.
Cancel	Cancel the selection of the SIP entity.

Time Range List field descriptions

Use this page to define or modify a Time Range.

Name	Description
Name	Name for the Time Range. It can have between three and 64 characters. The name cannot contain the following characters: <, >, ^, %, $, @, #, *
Mon to Sun	Selected check box indicates the days of the week applicable for the Time Range.

Table continues…

Name	Description
Start Time	Start time for the Time Range. For a 24–hour Time Range, the start time is 0.00.
End Time	End time for the Time Range. For a 24–hour Time Range, the end time is 23:59.
Notes	Additional notes about the Time Range.

Button	Description
Select	Selected Time Range is assigned to the Routing Policy.
Cancel	Cancels the changes to the Time Range.

Related Links

Creating Time Ranges on page 325
Modifying Time Ranges on page 325

Pattern List field descriptions

Use this page to view the Dial Pattern details for associating with the Routing Policy

Name	Description
Pattern	Dial pattern to match. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.
Emergency Call	Indicate if it is an emergency call. **Note:** Some of the important constraints on the use of this feature are as follows • Up to 100 emergency numbers can be assigned for each location. • This emergency dial number must match the emergency dial number in the 96xx settings file for all SIP phones in the identified location. Failure to follow this guideline can result in users being unable to dial emergency numbers.
SIP Domain	Domain for which you want to restrict the Dial Pattern.

Table continues…

Name	Description
Originating Location	Name of the location associated with the Dial Pattern.
Notes	Other details that you wish to add.

Button	Description
Select	Associate the selected pattern to the Routing Policy.
Cancel	Cancel the association of the selected pattern to the Routing Policy.

Regular Expression List field descriptions

Use this page to view the regular expression associated with the selected routing policy.

Name	Description
Regular Expression	Displays the regular expression to be used for the selected routing policy.
Rank Order	Priority of the regular expression. Lower rank order means a higher priority.
Deny	Denies routing for a matched regular expression.
Notes	Additional notes for the regular expression.

Button	Description
Select	Associates the selected regular expression to a routing policy or dissociates it based on the Add or Remove option selected earlier.
Cancel	Cancels the association or dissociation of the regular expression.

Related Links

[Creating Routing Policies](#) on page 330
[Modifying Routing Policies](#) on page 331

Bulk import for Routing Policies

Conform to the following rules while creating an XML bulk import file:

- The name of a routing policy <referred to as routing policy> is unique and is referred to by other elements.
- <sipentityName> must refer to an existing SIP element with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Routing Policy.

- Multiple time of day entries, <timeofdayNames>, can be configured for one Routing Policy.
  - <timerangeName> must refer to an existing Time Range with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Routing Policy.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<routingpolicyFullTOList>
    <RoutingpolicyFullTO>
        <notes>this is a test</notes>
        <disabled>false</disabled>
        <name>toBerlin</name>
        <sipentityName>BerlinCM</sipentityName>
        <timeofdayNames>
            <rank>1</rank>
            <timerangeName>regularweek</timerangeName>
        </timeofdayNames>
        <timeofdayNames>
            <rank>0</rank>
            <timerangeName>24/7</timerangeName>
        </timeofdayNames>
    </RoutingpolicyFullTO>
</routingpolicyFullTOList>
```

Dial Patterns

About Dial Patterns

A dial pattern specifies routing policies to route a call based on the digits dialed by a user. The system matches a dial pattern and then routes the call based on the dial pattern. Session Manager matches the dialed digits after applying any administered ingress adaptation.

The system also uses the following to determine how to route the call:

- the originating location of the call.
- the domain in the request-URI.
- the Global Settings option of the **Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location** on the Session Manager Administration page.

The following sections describe the dial pattern look-up method with respect to the Global Setting option.

If the Global Settings option is not selected:

1. Session Manager compares the user-part of the Request-URI with all dial patterns valid for the originating location where the domain matches the domain in the Request-URI. A Dial Pattern is valid for a particular location if :
   - the location in the dial pattern matches the originating location.

- the dial pattern is for “ALL” locations.

2. Dial patterns that match the originating location are considered before dial patterns for “ALL” locations. If a dial pattern for the originating location matches the digits, dial patterns for “ALL” locations are ignored.
3. If no matching dial patterns are found, then the domain in the Request-URI is modified to remove one level of subdomain until only a top-level domain is left. For example, if “dr.avaya.com” does not match, then “avaya.com” is tried. If “avaya.com” does not match, then Session Manager tries “.com”, which fails.
4. If more than one Dial Pattern matches, Session Manager selects the Dial Pattern with the longest matching pattern.

If the Global Settings option is selected:

1. Session Manager compares the user-part of the Request-URI with all dial patterns valid for the originating location where the domain matches the domain in the Request-URI. Only dial patterns matching the location are considered.
2. If no matching dial patterns are found, then the domain in the Request-URI is modified to remove one level of subdomain until only a top-level domain is left. For example, if “dr.avaya.com” does not match, then “avaya.com” is tried. If “avaya.com” does not match, then Session Manager tries “.com” , which fails.
3. If more than one dial pattern matches,Session Manager selects the dial pattern with the longest matching pattern.
4. Similarly, dial patterns administered for “ALL” locations are also compared.
5. The comparison may result in two matching dial patterns, one for “ALL” locations and one for the specific location. The longest matching pattern is then chosen. A longer pattern administered for “ALL” locations overrides a location-specific pattern. If both matching patterns are of the same length, then both patterns are examined for wildcard characters. If one pattern contains a wildcard and the other does not, then the pattern without a wildcard is selected. If both patterns contain a wildcard, then the location-specific pattern is selected.

Examples - Global Settings option is selected:

Location Specific Pattern	“ALL” Locations Pattern	Chosen Pattern
1303538	1303538	Location-Specific
130353	1303538	ALL Locations
1303538	130353	Location-Specific
130353x	1303538	ALL Locations
1303538	130353x	Location-Specific
1x	1303538	ALL Locations
13035xx	130xxxx	Location-Specific
1303xxxxx	1303538xx	ALL Locations

The pattern matching algorithm works as follows:

- Valid digits are 0-9.

- Valid characters for the leading position are,+, *, and #. Any other characters are not matched.
- x , lowercase, is a wildcard character that matches a character from the allowed characters above. Spaces are not allowed.
- Longer matches have a higher priority over shorter matches. For example, +1601555 has a higher priority as compared to +1601.
- For matches of equal length, exact matches have a higher priority over wildcard matches. For example, +1601555 has a higher priority as compared to +1xxx555.
- For both routing policies and adaptations, the pattern matching rules work in the same manner.

Note:

If multiple Routing Policies:

- have the same destination SIP Entity, and
- are assigned to the same Dial Pattern,

the Session Manager behaves as if the Route Policy **Retries** field is set. The value is equal to the number of administered Routing Policies. The Route Policy **Retries** value specifies the number of times the Session Manager polls a SIP Entity before timing out.

Emergency Numbers

Session Manager supports administering of up to 100 emergency numbers for each unique location. Emergency Numbers can be administered in the Dial Patterns pages of System Manager. The IP address of the endpoint determines the emergency numbers that are downloaded to that endpoint. Only those emergency numbers from the Dial Patterns page where **Originating Locations and Routing Policies** and **Denied Originating Locations** are consistent with the location administered for the user, are sent to the endpoint. Both location specific emergency numbers and the general emergency numbers are sent to the endpoint. If the general emergency number is same as that of the local emergency number, the local number description takes precedence over the general emergency number description. Prior to user login, the emergency number related information is downloaded to the endpoint devices upon connection to the network. Emergency numbers are again sent to the endpoint when a user logs in.

A priority number can be assigned or the first number administered is assigned as the priority number, so that the endpoint can associate an emergency number with the emergency softkey of the endpoint.

Emergency Number dialing for unregistered endpoints

If multiple locations have been defined in System Manager, there must be at least one emergency call dial pattern entered with originating location = ALL. Alternatively, every location with a location specific emergency number dial pattern, must be defined with an associated IP address pattern. If these criteria are not met, then unregistered endpoints cannot make emergency calls.

Note:

- The SIP endpoints administered with more than one emergency number should have software that supports multiple emergency number downloads from Session Manager. For an Avaya endpoint that does not support multiple emergency numbers, only the first administered emergency number gets routed properly by Session Manager.
- You should assign only one priority number to one emergency number and which should be unique.
- Maximum of 300 dial plan entries are send to the endpoints. Take this fact into consideration while specifying the number of emergency numbers.
- Emergency numbers are not supported for dial pattern ranges.

Dial Plan Ranges

Note:

Before enabling the Dial Plan Range feature in an enterprise system, ensure that all Session Manager installations are of version 6.3.4.

With Dial Plan Range, you can specify number ranges in the Session Manager Dial Plan.

A valid range has the following characteristics:

- Two integers separated by a colon (:)
- (Optional) A plus sign (+) can precede the numbers. If one number begins with a (+) sign, then the other number must also begin with a (+) sign.
- The number to the left of the colon must be numerically less than the number to the right. These numbers cannot be equal.
- The numbers on the left and right of the colon must be of the same length.

Note:

The Global Settings **Dial Plan Ranges** must be enabled in the Session Manager Administration page.

The valid pattern format is [+0-9][0-9]{0,23}[:][+0-9][0-9]{0,23}. For example, +493420479242000:+493420479242999.

You can enter a range that is a subset or superset of an existing range or pattern. The smaller range is a sub-range. Sub-ranges have the following limitations within the same location and domain:

- Two sub-ranges must not match each other.
- A sub-range must not match a pattern.
- A sub-range must not cross the starting or end of another range.

Example

If the specified range is 5000:5499, you can specify the sub-ranges as:

- 5002:5011
- 5000:5499 and 5492:5499, where the end of sub-range and range match.
- 5000 (single entry) and 5000:5009, where the beginning of sub-range and range match.

The sub-range 5300:5555 is not valid because the sub-range crosses the end of the range.

Note:

When routing, Session Manager prefers a smaller range over a larger range or pattern.

Multilocation Dial Plan

The Communication Manager location of a user is determined from the Communication Manager station form or from the *ip-address* of the endpoint if this address is administered on the Communication Manager *ip-network-map* form. If a user has a specific location other than the administered global location, then both the global and location specific dial plan entries are sent to the endpoint. If the user is not administered with a Communication Manager location, then only the global dial plan entries are sent to the endpoint. This information is used by the endpoint to determine the permitted dial sequences for a user.

Note:

For Session Manager releases earlier than 6.2, upon user login, endpoints receive all the administered Communication Manager (CM) dial plan entries.

Creating Dial Patterns

About this task

The Dial Patterns screen is used to create Dial Patterns and associate the Dial Patterns to a Routing Policy and Locations.

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Dial Patterns**.
3. Click **New**.

   The Dial Pattern Details screen is displayed.
4. Enter the Dial Pattern General information in the General section.

   You can specify Domain to restrict the Dial Pattern to the specified Domain.
5. Click **Add** under the Originating Locations and Routing Policies section.

6. Select all the required Locations and Routing Policies that you want associated with the Dial Pattern by selecting the check box in front of each item.
7. Click **Select** to indicate that you have completed your selections.
8. To specify that calls from the specified locations will be denied, click **Add** under the Denied Locations section.
9. Select all the Locations that are to be denied and click **Select** to indicate that you have completed your selections.
10. Click **Commit**.

Note:

You cannot save a dial pattern unless you add at least a routing policy or a denied location.

Related Links

Dial Pattern Details field descriptions on page 347
Dial Patterns field descriptions on page 346

Modifying Dial Patterns

Procedure

1. On System Manager Web Console, click **Elements** > **Routing**.
2. In the left navigation pane, click **Dial Patterns**.
3. Select a dial pattern for modification and click **Edit**.

   The Dial Pattern Details screen is displayed.
4. Enter the Dial Pattern General information in the General section.

   You can specify Domain to restrict the Dial Pattern to the specified Domain.
5. Click **Add** under the Locations and Routing Policies sections one after the other.
6. Select all the required Locations and Routing Policies that you want associated with the Dial Pattern by selecting the check box in front of each item.
7. Click **Select** to indicate that you have completed your selections.
8. Similarly, to remove locations, click **Remove**, select the locations to remove, and click **Select**.
9. To specify that calls from the specified locations will be denied, click **Add** in the Denied Locations section.
10. Select all the Locations that are to be denied and click **Select** to indicate that you have completed your selections.
11. To remove locations from the denied list, click **Remove**, select the locations to remove, and click **Select**.

12. Click **Commit**.

Note:

You cannot save a dial pattern unless the dial pattern has at least one routing policy or a denied location associated to the dial pattern.

Related Links

Dial Pattern Details field descriptions on page 347
Dial Patterns field descriptions on page 346

Deleting Dial Patterns

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Dial Patterns**.
3. To delete an existing dial pattern or patterns, select the respective check boxes and click **Delete**.
4. Click **Delete** on the confirmation page.

Note:

When you delete a Dial Pattern, the Dial Pattern is also deleted from all the Routing Policies that the Dial Pattern is associated to.

Related Links

Dial Patterns field descriptions on page 346
Delete Confirmation field descriptions on page 345

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of selected dial patterns.

Button	Description
Delete	Deletes entries for the selected dial patterns from the database.
Cancel	Cancels the deletion of the selected dial patterns.

Related Links

Deleting Dial Patterns on page 345

Dial Patterns field descriptions

Use this page to create, modify, delete, and manage dial patterns.

Button	Description
New	Opens the Dial Pattern Details page that you can use to create new dial patterns.
Edit	Opens the Dial Pattern Details page that you can use to modify the dial pattern details.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the dial pattern.
Duplicate	Creates a duplicate of the selected dial pattern and assigns a new state to it.
More Actions > **Dial Pattern Report**	Displays Dial Patterns and the corresponding Locations, Routing Policies and Domains.
More Actions > **Import**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.
More Actions > **Export Dial Patterns**	Opens the Export Dial Patterns page that allows you to export the dial patterns data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export data for all the routing entities as a zipped file to a specified location.

Name	Description
Pattern	The dial pattern to match. The pattern can have 1 to 49 characters.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.
Emergency Call	Call that is an emergency call.
Emergency Type	Type of emergency number. For example, medical, fire.
Emergency Priority	Priority of the emergency number.
SIP Domain	Domain for which you want to restrict the dial pattern.
Notes	Other details that you wish to add.

Related Links

Creating Dial Patterns on page 343
Modifying Dial Patterns on page 344
Deleting Dial Patterns on page 345

Dial Pattern Details field descriptions

Use this page to specify the dial pattern details.

General section

Name	Description
Pattern	The dial pattern to match. The pattern can have 1 to 49 characters. The valid pattern format for different pattern types are as follows: 1. For regular patterns, [+*#0-9x][0-9x]{0,35} 2. For pattern ranges, [+0-9][0-9]{0,23}[:][+0-9][0-9]{0,23} 3. For patterns with Emergency number, [0-9]{0,35} **Note:** If you specify Dial Pattern Range, the system disables the **Min**, **Max** and **Emergency Call** fields. For more information about pattern ranges, see the topic *Dial Plan Ranges*.
Min	The minimum number of digits to match.
Max	The maximum number of digits to match.
Emergency Call	Indicate if the call is an emergency call. **Note:** Some of the important constraints of this feature are as follows: • Each location can have upto 100 emergency numbers assigned. • This emergency dial number must match the emergency dial number in the 96xx settings file for all SIP phones in the identified location. Failure to follow this guideline can result in users being unable to dial emergency numbers.
Emergency Priority	Based on the IP address of the endpoint, up to 100 emergency numbers get downloaded to the endpoint, with each number assigned with a separate priority.

Table continues…

Name	Description
	Note: • PPM sends the emergency number, type, and priority/default to the endpoint. The first number in the list of emergency numbers, sent to the endpoint device, gets assigned with the Emergency soft key on the device. • Do not assign the same priority number for more than one emergency number of a location.
Emergency Type	The Type of emergency number. For example, medical, fire.
SIP Domain	The Domain for which you want to restrict the dial pattern.
Notes	Other details that you want to add.

Originating Locations and Routing Policies section

Button	Description
Add	Adds locations, routing policies for the dial patterns.
Remove	Removes locations, routing policies for the dial patterns.

Name	Description
Select check box	Use this check box to select and use the digit conversion for the incoming calls.
Originating Location Name	The name of the location to be associated to the Dial Pattern.
Originating Location Notes	Notes about the selected location.
Routing Policy Name	The name of the Routing Policy to be associated to the Dial Pattern.
Rank	The rank order.
Routing Policy Disabled	The name of the Routing Policy that should not be used for the Dial Pattern.
Routing Policy Destination	The destination of the Routing Policy.
Routing Policy Notes	Any other notes about the Routing Policy that you want to add.

Denied Originating Locations section

Button	Description
Add	Adds denied locations for the dial patterns.
Remove	Removes denied locations for the dial patterns.

Name	Description
Select check box	Select this check box to select denied locations for the Dial Pattern match.
Originating Location	The name of the location to be associated to the Dial Pattern.
Notes	Notes about the selected location.

Button	Description
Commit	Saves the Dial Pattern details.
Cancel	Cancels changes to the Dial Pattern details and returns to the Dial Patterns page.

Related Links

Creating Dial Patterns on page 343
Modifying Dial Patterns on page 344

Denied Originating Location List field descriptions

Use this page to specify denied locations for the selected dial pattern

Button	Description
Select	Selects the location as a denied location for the Dial Pattern.
Cancel	Cancels the selection of the denied location.

Name	Description
Apply to All Originating Locations	Select to associate all the locations to the Dial Pattern.
Select check box	Select this check box to select denied locations for the Dial Pattern match.
Name	Name of the location to be associated to the Dial Pattern.
Notes	Notes about the selected location.

Bulk Import for Dial Patterns

Conform to the following rules when creating an XML bulk import file:

- A dial pattern is identified by a combination of 5 elements below. This combination must be unique for each dial pattern.
  - <digitpattern>

- <maxdigits>
- <mindigits>
- <sipdomainName>
- <routingoriginationName>

- <sipdomainName> must refer to an existing domain with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the dial pattern.
- <routingpolicyNames> must refer to existing Routing Policies with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Dial pattern.
- <routingpolicyNames> must exist if <deny> is false.
- <routingpolicyNames> must exist if <deny> is true.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<digitmapFullTOList>
    <DigitmapFullTO>
        <notes>this is a test</notes>
        <deny>true</deny>
        <digitpattern>123</digitpattern>
        <maxdigits>36</maxdigits>
        <mindigits>3</mindigits>
        <routingoriginationName>New York</routingoriginationName>
        <routingpolicyNames>toBerlin</routingpolicyNames>
        <sipdomainName>avaya.com</sipdomainName>
        <treatasemergency>true</treatasemergency>
    </DigitmapFullTO>
    <DigitmapFullTO>
        <notes>this is a test</notes>
        <deny>false</deny>
        <digitpattern>123</digitpattern>
        <maxdigits>36</maxdigits>
        <mindigits>3</mindigits>
        <routingoriginationName>Berlin</routingoriginationName>
        <routingpolicyNames>toBerlin</routingpolicyNames>
        <sipdomainName>avaya.com</sipdomainName>
        <treatasemergency>true</treatasemergency>
    </DigitmapFullTO>
</digitmapFullTOList>
```

Regular Expressions

About Regular Expressions

You can configure routing in Session Manager by creating regular expressions and associating them with a routing policy.

Regular expression syntax is based on Java syntax. Some of the syntax related rules are:

- The asterisk character "*" matches any character string.
- The dot character "." matches one character.
- The backslash character "\ " makes a character lose its special meaning, if any

Some examples are:

- For “www.sipentity.domain.com”, use the string “www\.sipentity\.domain\.com”
- For “192.14.11.22”, use string “192\.14\.11\.22”.
- The routing policy with a regular expression .*@.*\.de routes all calls requesting a domain in Germany (for example, name@company.de) to a Frankfurt Gateway.

Related Links

Regular Expression constructs on page 351

Regular Expression constructs

Construct	*Matches*
Characters	
x	The character x
\\	The backslash character
Character classes	
[abc]	a, b, or c (simple class)
[^abc]	Any character except a, b, or c (negation)
[a-zA-Z]	a through z or A through Z, inclusive (rang
[a-d[m-p]]	a through d, or m through p: [a-dm-p] (uni
[a-z&&[def]]	d, e, or f (intersection)
[a-z&&[^bc]]	a through z, except for b and c: [ad-z] (su
[a-z&&[^m-p]]	a through z, and not m through p: [a-lq-z](
Predefined character classes	
.	Any character (may or may not match line
\d	A digit: [0-9]
\D	A non-digit: [^0-9]
\s	A whitespace character: [\t\n\x0B\f\r]
\S	A non-whitespace character: [^\s]
\w	A word character: [a-zA-Z_0-9]
\W	A non-word character: [^\w]
java.lang.Character classes (simple java character type)	
\p{javaLowerCase}	Equivalent to java.lang.Character.isLower

\p{javaUpperCase}	Equivalent to java.lang.Character.isUpper
\p{javaWhitespace}	Equivalent to java.lang.Character.isWhite
\p{javaMirrored}	Equivalent to java.lang.Character.isMirror
Classes for Unicode blocks and categories	
\p{InGreek}	A character in the Greek block (simple blo
\p{Lu}	An uppercase letter (simple category)
\p{Sc}	A currency symbol
\P{InGreek}	Any character except one in the Greek blo
[\p{L}&&[^\p{Lu}]]	Any letter except an uppercase letter (sub
Boundary matchers	
^	The beginning of a line
$	The end of a line
Greedy quantifiers	
X?	X, once or not at all
X*	X, zero or more times
X+	X, one or more times
X{n}	X, exactly n times
X{n,}	X, at least n times
X{n,m}	X, at least n but not more than m times
Logical operators	
XY	X followed by Y
X|Y	Either X or Y

Note:

Refer to the full documentation at http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html for details.

Creating Regular Expressions

About this task

Use the Regular Expressions screen to create regular expressions and associate them with routing policies. You cannot save a regular expression unless the regular expression has a routing policy associated with the regular expression.

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Regular Expressions**.
3. Click **New**. The Regular Expression Details screen is displayed.

4. Enter the regular expression pattern in the **Pattern** field.
5. Specify a rank order for the regular expression. A lower rank order indicates a higher priority.
6. To deny routing for a matched regular expression pattern, select the **Deny** check box.
7. To associate a routing policy for the matched pattern, click **Add** under the Routing Policy section.
8. Select the required routing policies that you want associated with the Regular Expression by selecting the respective check boxes.
9. Click **Select** to indicate that you have completed your selections.
10. To remove an associated routing policy, select the routing policy and click **Remove**.
11. Click **Commit**.

Related Links

Regular Expression Details field descriptions on page 355
Regular Expressions field descriptions on page 354

Modifying Regular Expressions

About this task

Use the Regular Expressions screen to modify regular expressions and associate the regular expressions with routing policies.

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Regular Expressions**.
3. Select a regular expression from the list and click **Edit**. The Regular Expression Details screen is displayed.
4. Modify the regular expression pattern in the **Pattern** field, if required.
5. If required, modify the rank order for the regular expression. A lower rank order indicates a higher priority.
6. To allow or deny routing for a matched regular expression pattern, select or clear the **Deny** check box.
7. To associate a routing policy for the matched pattern, click **Add** under the Routing Policy section.
8. Select the required routing policies that you want associated with the Regular Expression by selecting the respective check boxes.
9. Click **Select** to indicate that you have completed your selections.
10. To remove an associated routing policy, select the routing policy and click **Remove**.
11. Click **Commit**.

Note:

You cannot save a regular expression unless the regular expression has a routing policy associated to the regular expression.

Related Links

Regular Expression Details field descriptions on page 355
Regular Expressions field descriptions on page 354

Deleting Regular Expressions

About this task

Deleting a regular expression deletes it from all of the routing policies that it is associated with.

Procedure

1. On System Manager Web Console, click **Elements** > **Routing** .
2. In the left navigation pane, click **Regular Expressions**.
3. To delete existing regular expressions, select the respective check boxes and click **Delete**.
4. On the confirmation page, click **Delete**

Related Links

Regular Expressions field descriptions on page 354
Delete Confirmation field descriptions on page 354

Delete Confirmation field descriptions

Use this page to confirm or cancel the deletion of the regular expression.

Button	Description
Delete	Confirms the deletion of the regular expression and also deletes the regular expression from the routing policy that it is associated to.
Cancel	Cancels the deletion of the regular expression.

Related Links

Deleting Regular Expressions on page 354

Regular Expressions field descriptions

Use this page to create, modify, delete, and manage regular expressions.

Button	Description
New	Opens the Regular Expression Details page that you can use to create new regular expressions.
Edit	Opens the Regular Expression Details page that you can use to modify the regular expressions.
Delete	Opens the Delete Confirmation page on which you can confirm or cancel the deletion of the regular expression.
Duplicate	Creates a duplicate of the selected regular expression and assigns a new state to it.
More Actions > **Import**	Opens the Import data page that allows you to import from XML files or zip file containing one or more XML files.
More Actions > **Export Regular Expressions**	Opens the Export Regular Expressions page that allows you to export the regular expressions data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page that allows you to export data for all entities as a zipped file to a specified location.

Name	Description
Pattern	Regular expression pattern that Session Manager tries to match.
Rank Order	Priority of the pattern. A lower rank order means higher priority.
Deny	Denies routing for a matched regular expression pattern.
Notes	Additional notes about the regular expression pattern.

Related Links

Creating Regular Expressions on page 352
Modifying Regular Expressions on page 353
Deleting Regular Expressions on page 354

Regular Expression Details field descriptions

Use this page to specify the regular expression details.

General

Name	Description
Pattern	Regular expression pattern that Session Manager tries to match. Refer to the “Appendix B: Regular Expression constructs” for details.
Rank Order	Priority of the pattern. A lower rank order means higher priority.
Deny	Denies routing for a matched regular expression pattern.
Notes	Additional notes about the regular expression pattern.

Routing Policy

Button	Description
Add	Associates a routing policy for the matched pattern.
Remove	Dissociates a routing policy from the matched pattern.

Name	Description
Name	Name of the routing policy.
Disabled	Specifies that the routing policy is to be disabled and should not be used.
Destination	SIP Entity as Destination.
Notes	Additional notes about the routing policy.

Button	Description
Commit	Saves the regular expression and distributes it to the Session Managers in the enterprise.
Cancel	Cancels the creation or modification of the regular expression.

Related Links

[Creating Regular Expressions](#) on page 352
[Modifying Regular Expressions](#) on page 353

Routing Policy List field descriptions

Use this page to select a routing policy that the regular expression should be associated with.

Name	Description
Name	Name of the routing policy to be associated with the selected regular expression.
Disabled	Denotes that the associated routing policy is to be disabled for the selected regular expression.
Destination	Destination SIP entity for the routing policy.
Notes	Additional notes about the routing policy.

Button	Description
Select	Confirms the selection of the routing policy for associating it with the regular expression.
Cancel	Cancels the selection of the routing policy.

Bulk import for Regular Expressions

Conform to the following rules when creating an XML bulk import file:

- The pattern of a Regular Expression, referred to as <regexpmap> must be unique.
- <routingpolicyNames> must refer to an existing Routing Policy with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Regular Expression.
- Multiple Routing Policy entries (<routingpolicyNames>) can be configured for one Regular Expression.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<regexpmapFullTOList>
    <RegexpmapFullTO>
        <notes>this is a test</notes>
        <deny>false</deny>
        <pattern>*.com</pattern>
        <rankorder>0</rankorder>
        <routingpolicyNames>toBerlin</routingpolicyNames>
    </RegexpmapFullTO>
</regexpmapFullTOList>
```

Defaults

Modifying the default settings

You can use the Defaults screen to change the default values or ranges for parameters that are used by the other Routing menu options

About this task

These values are used as defaults values of admin personal settings when creating new Routing entities. Modifying these values does not change the values of already created entities .

Procedure

1. On the System Manager console, under **Elements**, click **Routing**.
2. Click **Routing** > **Defaults**. The Personal Settings screen is displayed.
3. In **Adaptations**, specify the minimum and maximum number of characters for pattern matching. The default minimum and maximum values are 1 and 36 respectively.
4. In **Dial Patterns**, specify the minimum and maximum length for dial pattern. These values are used by the **Dial Patterns** option. The default minimum and maximum values are 1 and 36 respectively.
5. In **Entity Links**, specify the port number to be used as a listen port. The default port is 5060.
6. In **Domain Management**, specify a domain suffix.
7. In **SIP Entities**, specify the following:
    a. Select the default SIP entity type from the **Type** drop-down menu. The default type is Session Manager.
    b. Select the default time zone from the **Time Zone** pull-down menu. The default time zone is America/Denver.
    c. Select the default transport protocol for ports. The default protocol is TLS.
    d. With entity links from both the Session Manager instances, checking the Override Port & Transport with DNS SRV check box on the SIP entity form indicates that both the Port and Protocol (Transport) on the SIP entity form are ignored.
        - If you select the check box, the port and transport administered in the local host name resolution table is used, which could override the entity link.
        - If the FQDN is not in the local table and DNS is consulted, if you have not selected the check box, only an A-Record lookup is done in DNS to resolve the host name to an IP address. Transport and port specified in the entity link are used. If you selected the check box, a full DNS lookup (as described in RFC 3263) is done, and the transport and port specified in the entity link could be overridden.
8. In **Time Ranges**, specify the default start time and end time for the time range. The default is to use a 24-hour time range, that is, the start time is 00:00 hours and the end time is 23:59 hours.
9. In **Application Settings**, select the **Show warning message** check box to get a warning message if you try to navigate to another page when a page has unsaved data or when data import is in progress.
10. Click **Apply** to save the changes.

Related Links

Default Settings field descriptions on page 359

Default Settings field descriptions

Use this page to specify default settings for all the Routing menus on the right-hand side pane and to save them as your default personal settings.

Adaptations

Name	Description
Matching Pattern Min Length	Minimum length of pattern matched for adaptations. The minimum value can be 1.
Matching Pattern Max Length	Maximum length of pattern matched for adaptations. The maximum value can be 36.

Dial Patterns

Name	Description
Dial Pattern Min Length	Minimum length of dial pattern to be matched. The minimum value can be 1.
Dial Pattern Max Length	Maximum length of dial pattern to be matched. The maximum value can be 36.

Entity Links

Name	Description
Listen Port	Number of the port to be used for entity links. The default port is 5060.
Default Transport Protocol for Entity Links	The default transport protocol that the entity links use, such as TLS, TCP, or UDP. The default is TLS.

Domain Management

Name	Description
Suffix	The default suffix to be used for the domain name.

SIP Entities

Name	Description
Type	Type of the SIP entity, such as ASM, CM, Trunk, Gateway, and so on. The default is ASM.
Time Zone	Default time zone to be used for the entity link.
Default Transport Protocol for Ports	Default transport protocol to be used by the ports. The default is TLS.
Override Port & Transport with DNS SRV	Select check box to override DNS routing.

Time Ranges

Name	Description
Time Range Start Time	Start time for the time range. Default is 00:00.
Time Range End Time	End time for the time range. Default is 23:59.

Application Settings

Name	Description
Show warning message	Displays a warning message if you try to navigate to another page when the displayed page has unsaved data or if a data import is on progress.

Button	Description
Restore Defaults	Restores vendor defaults.
Revert	Reverts to settings before the last applied settings.
Apply	Saves and applies the modified default settings.

Related Links

Modifying the default settings on page 357

Chapter 8: Configuring and monitoring Session Manager instances

Session Manager Dashboard

The Session Manager Dashboard displays a snapshot summary view of the system status of the administered Session Manager instances. The Dashboard also provides the following Session Manager maintenance operations:

- **Deny New Service**
- **Accept New Service**
- **Shutdown System**
- **Reboot System**

Session Manager Dashboard field descriptions

The **As of (time)** message indicates the time the information on the screen was last updated.

Button	Description
Service State > Deny New Service	Block incoming calls for the selected Session Manager or Session Managers but leave active calls connected.
Service State > Accept New Service	Accept incoming calls for the selected Session Managers.
Shutdown System > Shutdown	Shut down the selected Session Manager server.
Shutdown System > Reboot	Reboot the selected Session Manager server.

Name	Description
Session Manager	Displays the name of administered Session Manager instance. Click the link to go to the Session Manager Administration page.
Type	Displays the type of Session Manager instance. The type can be Core or Branch Session Manager.

Table continues…

Name	Description
Tests Pass	Displays the current results for periodic maintenance tests. Green indicates the tests passed. Red indicates at least one test failed Click the link to display the Maintenance Tests page.
Alarms	Displays the number of active Major/Minor/Warning alarms. Click the link to go to the Alarming page.
Security Module	Displays the state of the Security Module. The state can be Up, Down, and --- (unknown). Click the link to go to the detailed summary page of the selected security module.
Service State	Displays the current service state of Session Manager. The service state can be: • Accept New Service • Deny New Service
Entity Monitoring	Displays the monitoring status of the selected Session Manager. The page shows the number of down links and number of total links. Click the link to display the Session Manager Entity Link Connection Status page. **Note:** Entity Monitoring does not apply to a Session Manager that is administered as a BSM. The monitoring status of a BSM is always unknown (---).
Active Call Count	Displays the current number of active calls for the Session Manager instance.
Registrations	Displays the current registration summary and the maximum registrations in the last 24 hours. Click the link to display the Registration Summary page.
Data Replication	Displays the replication status for the replica node. Green indicates synchronized and red indicates not synchronized. Click the link to display the Replica Groups page.
User Data Storage Status	A green check indicates the User Data Storage Sanity Test passed. A red check indicates the test failed. Click the check mark to display the User Data Storage Status page for the detailed status report.

Table continues…

Name	Description
	Note: The **User Data Storage Status** appears as **– –** for: • Branch Session Managers. • Session Managers running a release earlier than 6.3.8.
Version	Displays the installed version of the Session Manager. The version has the following format: <major release number>.<minor release number>.<service pack number>.<patch number>.<build number>. Click a version string link to display the Session Manager Version Inventory information for a particular software version.

Session Manager Administration

About Session Manager Administration

Session Manager administration functionality enables adding a SIP entity as a Session Manager instance. Once you add Session Manager instances, these instances form a link with Session Manager Element Manager and can be used for obtaining and monitoring the status of the instance.

Data replication and monitoring operations are possible only after these Session Manager instances are added and configured.

In addition to creating new Session Manager instances, the Session Manager administration page also enables you to view, edit, or delete Session Manager instances that you have created.

You can also administer Session Manager and Branch Session Manager instances using **Inventory** > **Manage Elements** pages in the System Manager Web Console. This creates an application system in the element inventory managed by System Manager.

About E911 Services

Using the E911 service you can identify the physical location of a registered user in the event of an emergency call. The location is determined through the IP address and port level discovery as per E911 administration. Session Manager interacts with E911 service upon user registrations to obtain an Emergency Location Identification Number (ELIN). Each Session Manager synchronizes with the E911 services server, stores ELIN records for its registered users, and sends the ELIN to

Communication Manager when an emergency call is made. Session Manager synchronizes with the E911 services server when any of the following events occurs:

- You can add the server to Session Manager in order to initialize or synchronize databases
- The connection between Session Manager and the server is lost and later restored
- User registration and un-registration results in Session Manager to synchronize with the E911 service.

E911 services operate in a primary and secondary server mode, in which one server is active and the other is operating in a standby mode.

NIC bonding

NIC bonding is method to increase available bandwidth. When bonded, 2 NICs appear to have the same physical device and the MAC address.

NIC bonding provides backup if the primary Security Module interface fails or if the port is switched off.

Before attempting NIC bonding, verify the integrity and functionality of each NIC individually. The cable or either of the ports the cable plugs into can fail.

For NIC bonding, the Security Module uses Eth2 as the primary interface and Eth3 as the secondary backup interface. A logical interface, called bond0, connects the two interfaces and has the IP address of the Security Module.

To administer NIC bonding, make sure both the Eth 2 and Eth3 ports have network cables connected to the network.

The system generates alarms when one of the interfaces (Eth2 or Eth3) is out of service. If both of the interfaces are out of service, the system generates an alarm indicating that the bond0 interface is out of service.

The system displays the NIC bonding status for a Session Manager on the **Security Module Status** page.

The following is the mapping of the physical Ethernet interfaces:

- Eth0 : Management
- Eth1: Services
- Eth2: Security Module (SIP or PPM) – Physical port 3
- Eth3: Backup interface for NIC bonding – Physical port 4

Adding a SIP entity as Session Manager Instance

Before you begin

Before starting this procedure, make sure that the SIP entity that you want to add has been created. For Session Manager SIP Entity type, you must administer the listen ports on the SIP Entity page.

The endpoints use these listen ports to connect to Session Manager and to map different ports to different domains.

About this task

You can administer Session Manager either using:

- Session Manager pages.
- Manager Elements pages that creates an application system in the element inventory managed by System Manager.

Using Session Manager pages

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Session Manager Administration**.
3. On the Session Manager Administration page under Session Manager Instances, click **New**.
4. In the **General** section, enter the following information:
   a. From the drop-down list, select the **SIP Entity Name** .
   b. In the **Description** field, add a description for this entity.
   c. In the **Management Access Point Host Name/IP** field, enter the IP address of the management interface, eth0 , of the Session Manager server.
   d. From the drop-down list, select the **Direct Routing to Endpoints** .
   e. Select the **VMware Virtual Machine** check box to suggest that the Session Manager is hosted on the VMware platform.
   f. For **Adaptation for Trunk Gateway**, from the drop-down list, select **None** .
5. In the **Security Module** section, enter the following information to configure Security Module:
   a. In the **Network Mask** field, enter the value for the network mask associated with the network. The Security Module network interface is connected to this network.
   b. In the **Default Gateway** field, add the IP address of the default gateway.
   c. In the **Call Control PHB** field, select the default value of 46 (forward with highest priority).
   d. In the **QOS Priority** field, enter a 802.1q priority value. The default value is 6.
   e. In the **Speed & Duplex** field, select a value from the drop-down menu to configure the security module interface speed and duplex values.
   f. In the **VLAN ID** field, enter an integer value. The entered value is the VLAN that Session Manager is to be associated with. Leave this field blank if VLAN is not in use.
   g. Select the associated SIP Firewall Configuration with the Session Manager instance.

   SIP Entity IP Address field is populated as per the IP address of the SIP entity.
6. In the **NIC Bonding** section, enable or disable NIC bonding by selecting or clearing the **Enable Bonding** check box.

7. In the **NIC Bonding** section, select a monitoring mode for NIC bonding from the drop-down menu for **Device Monitoring Mode**
8. If you selected **ARP Monitoring** for **Device Monitoring Mode**, enter the following information:
    a. ARP Interval (msecs) : Specifies the ARP link monitoring frequency. The range is 50 to 1000. The default value is 100.
    b. ARP Target IP: Specifies the IP target of the ARP request that is sent to determine the health of the link to the targets. You can configure up to 3 IP addresses for ARP monitoring.

    Note:

    Due to a Red Hat Linux kernel limitation, do not monitor virtual IP addresses when using ARP monitoring. This affects the Session Manager ARP table updates causing the virtual IP entity link to be marked as down. However, you can monitor virtual IP addresses using MII mode.
9. If you selected **MII Monitoring** for **Device Monitoring Mode**, enter the following information:
    a. Link Monitoring Frequency (msecs) : Specifies the sampling period. The range is 50 to 500. The default value is 100.
    b. Down Delay (msecs): Specifies the wait time for disabling a slave if a link failure is detected. The range is 50 to 1000. The default value is 200.
    c. Up Delay (msecs): Specifies the wait time for enabling a slave if a link recovery is detected. The range is 50 to 1000. The default value is 200.
10. In the **Monitoring** section, enter the following information to configure how this Session Manager instance should monitor SIP entities:
    a. Select or clear the **Enable Monitoring** check box to enable or disable monitoring of the SIP entities by this Session Manage instance.
    b. In the **Proactive cycle time (secs)** field, enter a value in seconds. The default is 900 seconds. Session Manager uses this value for monitoring and polling an administered SIP entity at this interval until that entity is reachable.
    c. In the **Reactive cycle time (secs)** field, enter a value in seconds. The default is 120 seconds.
    d. In the **Number of Retries** field, enter an integer value. This value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable. The default value is 1.
11. In the **CDR** section, enter the following information:
    a. Select the **Enable CDR** check box to enable Call Detail Recording at the system level for the Session Manager instance. You can then use the **Call Detail Recording** drop-down menu to individually control call detail recording for specific SIP entities.
    b. To gain access to the CDR record, enter and then re-enter the password for confirmation. The password that you enter here becomes the default password for the **CDR_USER** user ID.

c. In the **Data File Format** field, click the format for the CDR data file.

d. Select the respective checkboxes to include the CDR records for user-to-user calls and incomplete calls.

To enable the **Include User to User Calls** or **Include Incomplete Calls** checkbox, in the **Data File Format** field, click **Enhanced Flat File** or **Enhanced XML File**.

Note:

For more information about Call Detail Recording, see the chapter *Call Detail Recording (CDR)* in the book *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

12. In the **Personal Profile Manager (PPM) - Connection Settings** section, enter the following information:

a. Select the **Limited PPM Client Connection** check box to enable the **Maximum Connection per PPM client** field. The default value is enabled.

b. Specify the value of **Maximum Connection per PPM client**. Valid values are integers between 1 and 10. The default value is 3.

c. Select the **PPM Packet Rate Limiting** check box to enable the **PPM Packet Rate Limiting Threshold** field. The default value is enabled.

d. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. The range is 1-500. The default value is 50.

13. Under the **Event Server** section, select **Yes** or **No** for **Clear Subscription on Notification Failure**.

14. Click **Commit**.

Using Manage Elements pages

Procedure

1. On System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On New Elements page, select an application type **Session Manager**.
5. Select **Core Session Manager** and click **Continue**.

Add Session Manager page opens.

6. In the **General** section, enter the following information:

a. From the drop-down list, select the **SIP Entity Name** .

b. In the **Description** field, add a description for this entity.

c. In the **Management Access Point Host Name/IP** field, enter the IP address of the management interface, eth0 , of Session Manager server.

d. From the drop-down list, select the **Direct Routing to Endpoints** .

e. Select the **VMware Virtual Machine** check box to suggest that the Session Manager is hosted on the VMware platform.

f. For **Adaptation for Trunk Gateway**, from the drop-down list, select **None** .

7. In the **Security Module** section, enter the following information to configure the Security Module:

   a. In the **Network Mask** field, enter the value for the network mask associated with the network. The Security Module network interface is connected to this network.

   b. In the **Default Gateway** field, add the IP address of the default gateway.

   c. In the **Call Control PHB** field, select the default value of 46 (forward with highest priority).

   d. In the **QOS Priority** field, enter a 802.1q priority value. The default value is 6.

   e. In the **Speed & Duplex** field, select a value from the drop-down menu to configure the security module interface speed and duplex values.

   f. In the **VLAN ID** field, enter an integer value. The entered value is the VLAN that Session Manager is to be associated with. Leave this field blank if VLAN is not in use.

   g. Select the associated SIP Firewall Configuration with the Session Manager instance.

   SIP Entity IP Address field is populated as per the IP address of the SIP entity.

8. In the **NIC Bonding** section, enable or disable NIC bonding by selecting or clearing the **Enable Bonding** check box.

9. In the **NIC Bonding** section, select a monitoring mode for NIC bonding from the drop-down menu for **Device Monitoring Mode**

10. If you selected **ARP Monitoring** for **Device Monitoring Mode**, enter the following information:

    a. ARP Interval (msecs) : Specifies the ARP link monitoring frequency. The range is 50 to 1000. The default value is 100.

    b. ARP Target IP: Specifies the IP target of the ARP request that is sent to determine the health of the link to the targets. You can configure up to 3 IP addresses for ARP monitoring.

    Note:

    Due to a Red Hat Linux kernel limitation, do not monitor virtual IP addresses when using ARP monitoring. This affects Session Manager ARP table updates causing the virtual IP entity link to be marked as down. However, you can monitor virtual IP addresses using MII mode.

11. If you selected **MII Monitoring** for **Device Monitoring Mode**, enter the following information:

    a. Link Monitoring Frequency (msecs) : Specifies the sampling period. The range is 50 to 500. The default value is 100.

    b. Down Delay (msecs): Specifies the wait time for disabling a slave if a link failure is detected. The range is 50 to 1000. The default value is 200.

c. Up Delay (msecs): Specifies the wait time for enabling a slave if a link recovery is detected. The range is 50 to 1000. The default value is 200.

12. In the **Monitoring** section, enter the following information to configure how this Session Manager instance should monitor SIP entities:
    a. Select or clear the **Enable Monitoring** check box to enable or disable monitoring of the SIP entities by this Session Manage instance.
    b. In the **Proactive cycle time (secs)** field, enter a value in seconds. The default is 900 seconds. Session Manager uses this value for monitoring and polling an administered SIP entity at this interval until that entity is reachable.
    c. In the **Reactive cycle time (secs)** field, enter a value in seconds. The default is 120 seconds.
    d. In the **Number of Retries** field, enter an integer value. This value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable. The default value is 1.
13. In the **CDR** section, enter the following information:
    a. Select the **Enable CDR** check box to enable Call Detail Recording at the system level for the Session Manager instance. You can then use the **Call Detail Recording** drop-down menu to individually control call detail recording for specific SIP entities.
    b. To gain access to the CDR record, enter and then re-enter the password for confirmation. The password that you enter here becomes the default password for the **CDR_USER** user ID.
    c. In the **Data File Format** field, click the format for the CDR data file.
    d. Select the respective checkboxes to include the CDR records for user-to-user calls and incomplete calls.

       To enable the **Include User to User Calls** or **Include Incomplete Calls** checkbox, in the **Data File Format** field, click **Enhanced Flat File** or **Enhanced XML File**.

Note:

For more information about Call Detail Recording, see the chapter *Call Detail Recording (CDR)* in the book *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

14. In the **Personal Profile Manager (PPM) - Connection Settings** section, enter the following information:
    a. Select the **Limited PPM Client Connection** check box to enable the **Maximum Connection per PPM client** field. The default value is enabled.
    b. Specify the value of **Maximum Connection per PPM client**. Valid values are integers between 1 and 10. The default value is 3.
    c. Select the **PPM Packet Rate Limiting** check box to enable the **PPM Packet Rate Limiting Threshold** field. The default value is enabled.
    d. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. The range is 1-500. The default value is 50.

15. Under the **Event Server** section, select **Yes** or **No** for **Clear Subscription on Notification Failure**.
16. Click **Commit**.

Viewing Session Manager administration settings

About this task

You can view Session Manager using:

- Session Manager pages.
- Manage Elements pages.

Using Session Manager pages

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Session Manager Administration**.
3. Select Session Manager from Session Manager Instances list and click **View**. The View Session Manager page displays information about the selected Session Manager instance.
4. After you have viewed the information, click **Return**.

Using Manager Elements pages

Procedure

1. On System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Select a Session Manager instance and click **View**. The View Session Manager page displays information about the selected Session Manager instance.
4. After you have viewed the information, click **Return**.

Modifying the Session Manager administration settings

About this task

You can use this option to modify the configuration settings for an already configured Session Manager.

You can modify an existing Session Manager using:

- Session Manager pages.
- Manage Elements pages.

Using Session Manager pages

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Session Manager Administration**.
3. Select a Session Manager instance from the list and click **Edit**.
4. In the **General** section, change the following information, if required:
   - Add a comment in the Description field for the Session Manager SIP entity.
   - Change the IP address of the host on which Session Manager is installed in the **Management Access Point Host Name/IP** field. This is the IP address of the domain name of the server that hosts the Session Manager application. Session Manager passes the address to the Security Module agent to allow the agent to query the server for the required information. To be a part of Session Manager instances network of an enterprise, a Session Manager instance must first be administered as a management access point.
   - Select the **Direct Routing to Endpoints** from the drop-down list.
   - Select the **VMware Virtual Machine** check box to suggest that the Session Manager is hosted on the VMware platform.
5. In the **Security Module** section, change the following information, if required
   - Modify the network mask in the **Network Mask** field. Session Manager passes this network mask to the Security Module agent. The agent configures the network mask to define the subnet that the Security Module is to be associated with.
   - Modify the IP address in the **Default Gateway** field.
   - Modify the value for **Call Control PHB**. The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from the Security Module as it travels through the IP network. All packets containing SIP signaling that leave the Security Module have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence--they must either support this by default or be specially configured to do so.

     Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Session Manager uses a default DSCP value of 46 that indicate forwarding with the highest priority.
   - Select the **Speed & Duplex** value to configure the Security Module interface speed and duplex values.
   - Modify the **QOS Priority** value. This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Session Manager for any SIP traffic. The default value is 6. Range of the QOS priority value is 0-7. This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, the lower the QOS priority number.
   - Modify the value for **VLAN ID**. Session Manager associates with this VLAN value. Call traffic segregation could be based on the VLAN that Session Manager is associated with.

- Modify the associated SIP Firewall Configuration with the Session Manager instance.

6. In **NIC Bonding** section, change the following information if required:
   - To enable or disable NIC bonding, select or clear the **Enable Bonding** check box. NIC bonding slaves interfaces eth2 and eth3 in a bond of interfaces. This makes all the Network firewall rules related to Security Module agent public IP Address to be applied on the NIC bonding interface.
   - Select one of the following modes of NIC bonding as supported by NIC bonding driver from the drop-down menu **Device Monitoring Mode**:
     - ARP Monitoring
     - MII Monitoring
   - Modify the following details related to ARP monitoring:
     - ARP Interval (msecs) : Specifies the ARP link monitoring frequency and range is from 50 to 1000. The default value is 100.
     - ARP Target IP : Specifies the IP target of the ARP request that is sent to determine the health of the link to the targets. You can configure up to 3 IP Addresses for ARP monitoring

       Note:

       Due to a Red Hat Linux kernel limitation, do not monitor virtual IP addresses when using ARP monitoring. This affects the Session Manager ARP table updates causing the virtual IP entity link to be marked as down. However, you can monitor virtual IP addresses using MII mode.
   - Modify the following details related to MII monitoring:
     - Link Monitoring Frequency (msecs) : Specifies the sampling period with range from 50 to 500. The default value is 100.
     - Down Delay (msecs) : Specifies the wait time for disabling of a slave in case of detection of a link failure. The value is a multiple of link monitoring frequency value and range is from 50 to 1000. The default value is 200.
     - Up Delay (msecs) : Specifies the wait time for enabling of a slave in case of detection of a link recovery. The value is a multiple of link monitoring frequency value and range is from 50 to 1000. The default value is 200.
7. In the **Monitoring** section, modify the following information as required to configure how Session Manager instance should monitor SIP entities:
   - To enable or disable monitoring of the SIP entities by Session Manager instance, select or clear the **Enable Monitoring** check box.
   - Type a required value in seconds for **Proactive cycle time (secs)**. The default value is 900 seconds.
   - Session Manager uses this value for monitoring and polling an administered SIP entity at this interval till that entity is reachable.
   - Type a required value in seconds for **Reactive cycle time (secs)**. The default value is 120 seconds. This value is used when proactive monitoring detects that an administered

SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default is 120 seconds.

Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP Entities screen for a specific entity.

- Type an integer value in **Number of Retries**. The default value is 1. This value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable.

8. In the **CDR** section, enter the following information:
   a. Select the **Enable CDR** check box to enable Call Detail Recording at the system level for the Session Manager instance. You can then use the **Call Detail Recording** drop-down menu to individually control call detail recording for specific SIP entities.
   b. To gain access to the CDR record, enter and then re-enter the password for confirmation. The password that you enter here becomes the default password for the **CDR_USER** user ID.
   c. In the **Data File Format** field, click the format for the CDR data file.
   d. Select the respective checkboxes to include the CDR records for user-to-user calls and incomplete calls.

      To enable the **Include User to User Calls** or **Include Incomplete Calls** checkbox, in the **Data File Format** field, click **Enhanced Flat File** or **Enhanced XML File**.

Note:

For more information about Call Detail Recording, see the chapter *Call Detail Recording (CDR)* in the book *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

9. **Personal Profile Manager (PPM) - Connection Settings** section specifies the global parameters that apply to all Session Manager instances. Under the **Personal Profile Manager (PPM) - Connection Settings** section, specify related information:
   a. Select the **Limited PPM client connection** check box to enable selecting **Maximum Connection per PPM client**. Default value is enabled.
   b. Specify the value of **Maximum Connection per PPM client**. Valid values are integers between 1 and 10. Default value is 3.
   c. Select the **PPM Packet Rate Limiting** check box to enable selecting **PPM Packet Rate Limiting Threshold**. Default value is enabled.
   d. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. Value Range: 1-500, default value is 50.

   Event Server section specifies the option to clear Subscription on Notification Failure.

10. Click **Commit**.

Using Manage Elements pages

Procedure

1. On System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Select a Session Manager instance from the list and click **Edit**.
4. In the **General** section, change the following information, if required:
   - Add a comment in the Description field for the Session Manager SIP entity.
   - Change the IP address of the host on which Session Manager is installed in the **Management Access Point Host Name/IP** field. This is the IP address of the domain name of the server that hosts the Session Manager application. Session Manager passes the address to the Security Module agent to allow the agent to query the server for the required information. To be a part of Session Manager instances network of an enterprise, a Session Manager instance must first be administered as a management access point.
   - Select the **Direct Routing to Endpoints** from the drop-down list.
   - Select the **VMware Virtual Machine** check box to suggest that the Session Manager is hosted on the VMware platform.
5. In the **Security Module** section, change the following information, if required
   - Modify the network mask in the **Network Mask** field. Session Manager passes this network mask to the Security Module agent. The agent configures the network mask to define the subnet that the Security Module card is to be associated with.
   - Modify the IP address in the **Default Gateway** field.
   - Modify the value for **Call Control PHB**. The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from Security Module that you may expect as it travels through the IP network. All packets containing SIP signaling that leave the Security Module have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence--they must either support this by default or be specially configured to do so.

     Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Session Manager uses a default DSCP value of 46 that indicate forwarding with the highest priority.
   - Select the **Speed & Duplex** value to configure the Security Module interface speed and duplex values.
   - Modify the **QOS Priority** value. This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Session Manager for any SIP traffic. The default value is 6. Range of the QOS priority value is 0-7. This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, the lower the QOS priority number.

- Modify the value for **VLAN ID**. Session Manager associates with this VLAN value. Call traffic segregation could be based on the VLAN that Session Manager is associated with.
- Modify the associated SIP Firewall Configuration with the Session Manager instance.

6. In **NIC Bonding** section, change the following information if required:
   - To enable or disable NIC bonding, select or clear the **Enable Bonding** check box. NIC bonding slaves interfaces eth2 and eth3 in a bond of interfaces. This makes all the Network firewall rules related to Security Module agent public IP Address to be applied on the NIC bonding interface.
   - Select one of the following modes of NIC bonding as supported by NIC bonding driver from the drop-down menu **Device Monitoring Mode**:
     - ARP Monitoring
     - MII Monitoring
   - Modify the following details related to ARP monitoring:
     - ARP Interval (msecs) : Specifies the ARP link monitoring frequency and range is from 50 to 1000. The default value is 100.
     - ARP Target IP : Specifies the IP target of the ARP request that is sent to determine the health of the link to the targets. You can configure up to 3 IP Addresses for ARP monitoring

       Note:

       Due to a Red Hat Linux kernel limitation, do not monitor virtual IP addresses when using ARP monitoring. This affects the Session Manager ARP table updates causing the virtual IP entity link to be marked as down. However, you can monitor virtual IP addresses using MII mode.
   - Modify the following details related to MII monitoring:
     - Link Monitoring Frequency (msecs) : Specifies the sampling period with range from 50 to 500. The default value is 100.
     - Down Delay (msecs) : Specifies the wait time for disabling of a slave in case of detection of a link failure. The value is a multiple of link monitoring frequency value and range is from 50 to 1000. The default value is 200.
     - Up Delay (msecs) : Specifies the wait time for enabling of a slave in case of detection of a link recovery. The value is a multiple of link monitoring frequency value and range is from 50 to 1000. The default value is 200.
7. In the **Monitoring** section, modify the following information as required to configure how Session Manager instance should monitor SIP entities:
   - To enable or disable monitoring of the SIP entities by Session Manager instance, select or clear the **Enable Monitoring** check box.
   - Type a required value in seconds for **Proactive cycle time (secs)**. The default value is 900 seconds.

- Session Manager uses this value for monitoring and polling an administered SIP entity at this interval till that entity is reachable.
- Type a required value in seconds for **Reactive cycle time (secs)**. The default value is 120 seconds. This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default is 120 seconds.

  Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP Entities screen for a specific entity.
- Type an integer value in **Number of Retries**. The default value is 1. This value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable.

8. In the **CDR** section, enter the following information:
   a. Select the **Enable CDR** check box to enable Call Detail Recording at the system level for the Session Manager instance. You can then use the **Call Detail Recording** drop-down menu to individually control call detail recording for specific SIP entities.
   b. To gain access to the CDR record, enter and then re-enter the password for confirmation. The password that you enter here becomes the default password for the **CDR_USER** user ID.
   c. In the **Data File Format** field, click the format for the CDR data file.
   d. Select the respective checkboxes to include the CDR records for user-to-user calls and incomplete calls.

      To enable the **Include User to User Calls** or **Include Incomplete Calls** checkbox, in the **Data File Format** field, click **Enhanced Flat File** or **Enhanced XML File**.

   Note:

   For more information about Call Detail Recording, see the chapter *Call Detail Recording (CDR)* in the book *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

9. **Personal Profile Manager (PPM) - Connection Settings** section specifies the global parameters that apply to all Session Manager instances. Under the **Personal Profile Manager (PPM) - Connection Settings** section, specify related information:
   a. Select the **Limited PPM client connection** check box to enable selecting **Maximum Connection per PPM client**. Default value is enabled.
   b. Specify the value of **Maximum Connection per PPM client**. Valid values are integers between 1 and 10. Default value is 3.
   c. Select the **PPM Packet Rate Limiting** check box to enable selecting **PPM Packet Rate Limiting Threshold**. Default value is enabled.
   d. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. Value Range: 1-500, default value is 50.

Event Server section specifies the option to clear Subscription on Notification Failure.

10. Click **Commit**.

Deleting a Session Manager instance

About this task

You can delete Session Manager instances using:

- Session Manager pages.
- Manage Elements pages.

Using Session pages

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Session Manager Administration**.
3. Select a Session Manager instance from the list and click **Delete**.
4. On the **Delete Confirmation** screen, click **Delete** to delete the Session Manager instance.

   Note:

   Before you delete a Session Manager instance, you should first dissociate the Session Manager instance from all the related Communication Profiles or delete the associated users.

Using Manage Elements pages

Procedure

1. On System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Select a Session Manager instance from the list and click **Delete**.
4. On the **Delete Confirmation** screen, click **Delete** to delete the Session Manager instance.

   Note:

   Before you delete a Session Manager instance, you should first dissociate the Session Manager instance from all the related Communication Profiles or delete the associated users.

Administering ELIN Server

About this task

This section provides the basic steps of ELIN Server administration.

Procedure

1. In Local Host Name Resolution (LHNR) page, administer the FQDN for the ELIN Server to have two IP address, that is one primary, one backup, with different priorities.
2. Add a SIP Entity of type ELIN Server using the administered FQDN.
3. In the Session Manager Administration page in the **Global Settings** section, select the administered ELIN Server for *ELIN SIP Entity* field.
4. Create the Entity Links from ELIN Server to all Session Manager SIP Entities.
5. Import certificates, using TLS link between Session Manager and ELIN server. This is required only if the entity link is of *TLS* type.

   Note:

   OPTIONS monitoring is enabled between Session Manager and ELIN Server. This applies to all entity links and you should not disable it.

Saving Global Session Manager Settings

Procedure

1. On the System Manager web console, under **Elements**, click **Session Manager** > **Session Manager Administration**.
2. On the Session Manager Administration screen in the Global Settings section, click **Save Global Settings** to the configure global settings of all the configured Session Manager instances.
3. Select **Allow Unauthenticated Emergency Calls** to enable unauthenticated users to make emergency calls, based on the dial pattern.
4. Select **Allow Unsecured PPM Traffic** to enable PPM traffic over HTTP to continue to process phone login, download button labels, contact lists, and other services.
5. Select **Failback Policy** to specify manual and scheduled failback support for terminals.
6. Select **ELIN SIP Entity** to specify the ELIN server for E911 services.
7. Select **Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location** to specify how to route the call based on the Dial Pattern settings. .
8. Select **Ignore SDP for Call Admission Control** to specify whether call admission control (CAC) uses SDP in SIP messages to determine the bandwidth used by a call.
9. Select **Disable Call Admission Control Threshold Alarms** to disable the alarms that are generated when Call Admission Control alarm thresholds are crossed.
10. Select **Disable Loop Detection Alarms** to disable the generation of loop detection alarms.
11. In the **Loop Detection Alarms Threshold (hours)** field, for a loop detection event, enter the interval after which an alarm needs to be generated.

The default value is 24 hours. The allowed range is 1 hour to 168 hours. This field is disabled when the **Disable Loop Detection Alarms** check box is selected. For details, see *SIP Call Looping.*

12. Select **Enable TLS Endpoint Certificate Validation** to validate an endpoint certificate when the connection type is TLS (outbound SIP connection to the endpoint).

    This setting is applicable for all Session Manager and Branch Session Manager instances in the managed network.

    Note:

    This setting is not applicable for Session Manager releases earlier than 6.3.2.

13. Select **Enable Dial Plan Ranges** to enable specification of dial plan ranges in the Dial Pattern Details page.

    Warning:

    Before specifying a dial plan range, ensure that all Session Manager instances and Branch Session Manager instances are 6.3.4 release or later.

14. Select **Enable Implicit Users Applications for SIP users** to enable implicit application sequencing.

    Note:

    This setting is not applicable for Session Manager releases earlier than 6.3.8.

Delete Confirmation page field descriptions

Button	Description
Delete	Deletes the selected Session Manager instance.
Cancel	Cancels the deletion of the selected Session Manager instance

Session Manager Administration page field descriptions

Global Settings

Name	Description
Save Global Settings	Configures global settings of all the configured Session Manager instances.
Allow Unauthenticated Emergency Calls	Specifies whether to allow unauthenticated users to make emergency calls.

Table continues…

Name	Description
Allow Unsecured PPM Traffic	Enables PPM traffic over HTTP so that it can continue to process phone login, download button labels, contact lists, and other services.
Failback Policy	Specifies manual and scheduled failback support for terminals.
ELIN SIP Entity	Determines a user's location based on IP address, to send the new ELIN to Session Manager in case of emergency call. This entity is used by third party E911 services. The SIP Entity selected as the ELIN server should be resolved through local host name resolution to use either the primary or secondary IP address.
Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location	Specifies how the call gets routed as per Dial Pattern settings. For details, see About Dial Patterns on page 339.
Ignore SDP for Call Admission Control	Determines whether call admission control (CAC) uses the SDP in SIP messages to determine the bandwidth used by a call.
Disable Call Admission Control Threshold Alarms	When this flag is set, alarms that are generated when Call Admission Control alarm thresholds are crossed get disabled. Alarms will still be generated by call denials due to crossing of bandwidth limits.
Disable Loop Detection Alarms	When this flag is set, generation of Loop Detection alarms is disabled.
Loop Detection Alarms Threshold (hours)	Specifies the interval after which the Session Manager generates an alarm for a Loop Detection event. By default, the value is 24 hours. The allowed range is 1 hour to 168 hours. For details, see SIP Call Looping on page 298.
Enable TLS Endpoint Certificate Validation	Enables validation of an endpoint certificate on a TLS connection (outbound SIP connection to the endpoint). By default, this field is disabled. This setting is applicable for all Session Managers and s in the managed network. **Note:** This selection does not apply for Session Manager releases earlier than 6.3.2.
Enable Dial Plan Ranges	Enables specification of dial plan ranges in the Dial Pattern Details page.

Table continues…

Name	Description
	Warning: Before specifying a dial plan range, ensure that all Session Managers and s are 6.3.4 release or later.
Enable Implicit User Applications for the SIP users	Enable or disable Implicit User sequenced applications for SIP users.

Session Manager Instances

Button	Description
New	Opens the Add Session Manager page, using which you can add a SIP entity as a new Session Manager instance.
View	Opens the View Session Manager page, which you can use to view an already added Session Manager instance.
Edit	Opens the Edit Session Manager page, which you can use to edit the properties of a Session Manager instance.
Delete	Opens the Delete Confirmation page, which you can use to delete a SIP entity that is added as a Session Manager instance.

Name	Description
Name	Name of administered Session Manager.
Primary Communication Profiles	The number of Communication Profiles that use this Session Manager as the primary SIP controller.
Secondary Communication Profiles	The total number of Communication Profiles that use this Session Manager as the secondary SIP controller.
Maximum Active Communication Profiles	The maximum number of active Communication Profiles supported by this Session Manager instance.
Description	Details of the Session Manager instance added.
VMware	Specifies whether the Session Manager is hosted on the VMware platform.

Branch Session Manager Instances

Button	Description
New	Opens the Add Branch Session Manager page that you can use to add a SIP entity as a new instance.

Table continues…

Button	Description
View	Opens the View Branch Session Manager page that you can use to view an already added instance.
Edit	Opens the Edit Branch Session Manager page that you can use to edit the properties of an already added instance.
Delete	Opens the Delete Confirmation page that you can use to delete a SIP entity that is added as a instance.

Name	Description
Name	Name of administered .
Main CM for LSP	Main Communication Manager for the Local Survivable Processor (LSP) associated with this .
SIP Communication Profiles	The number of Communication Profiles assigned to this .
Description	Details of the instance added.

Session Manager page field descriptions

General

Name	Description
SIP Entity Name	Name of the SIP entity that you must add as a Session Manager instance. The entity must be of type Session Manager and it must be in Sync state.
Description	Description of the entity added. This field is optional.
Management Access Point Host Name / IP	IP address of the host on which the management agent is running, that is, the host on which Session Manager is installed.
Direct Routing to Endpoints	Provides the option to enable or disable direct routing to endpoints.
VMware Virtual Machine	Specify whether the Session Manager is hosted on the VMware platform.

Security Module

Name	Description
SIP Entity IP Address	IP address of Session Manager as specified in the SIP Entity Details screen.

Table continues…

Name	Description
Network Mask	Specify the value of the Network mask. The security module configures the network mask and defines the subnet associated with the security module.
Default Gateway	IP address of the default gateway.
Call Control PHB	Specifies the type of service and priority for SIP traffic from the security module. All packets containing SIP signaling that leave the security module have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers might or might not treat packets with this value with a different level of precedence. These routers must either support this by default or be specially configured to do so. Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Session Manager uses a default DSCP value of 46 that indicates forwarding with the highest priority.
QOS Priority	Specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, lower the QOS priority number. This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Session Manager for any SIP traffic. The default value is 6. Range of this value is 0-7.
Speed & Duplex	Enables the configuring of the security module interface speed and duplex values. The recommended value is `Auto`.
VLAN ID	The VLAN that Session Manager should be associated with. Call traffic segregation could be based on the VLAN that Session Manager is associated with.
SIP Firewall Configuration	Shows the associated SIP Firewall Configuration with the Session Manager instance.

NIC Bonding

Name	Description
Enable Bonding	Enables or disables NIC bonding. NIC bonding slaves interfaces eth2 and eth3 in a bond of interfaces. This makes all the Network firewall rules related to SM100 agent public IP Address to be applied on the NIC bonding interface.

Table continues…

Name	Description
Driver Monitoring Mode	Allows you to select ARP Monitoring or MII Monitoring as the modes of NIC bonding as supported by NIC bonding driver.
ARP Interval (msecs)	Specifies the ARP link monitoring frequency and range is from 50 to 1000. The default value is 100.
ARP Target IP	Specifies the IP target of the ARP request that is sent to determine the health of the link to the targets. You can configure up to 3 IP Addresses for ARP monitoring.
Link Monitoring Frequency (msecs)	Specifies the sampling period with range from 50 to 500. The default value is 100.
Down Delay (msecs)	Specifies the wait time for disabling of a slave in case of detection of a link failure. The value is a multiple of link monitoring frequency value and range is from 50 to 1000. The default value is 200.
Up Delay (msecs)	Specifies the wait time for enabling of a slave in case of detection of a link recovery. The value is a multiple of link monitoring frequency value and range is from 50 to 1000. the default value is 200.

Monitoring

Button	Description
Enable Monitoring	Select to enable monitoring of the administered SIP entities by the added Session Manager instance. Clear the check box to disable monitoring.
Proactive cycle time (secs)	Specifies a value in seconds for polling the administered SIP entities by the added Session Manager. Monitoring ensures that the entities are still reachable. Proactive monitoring occurs as long as no outages are detected. The default is 900 seconds. These default values are used for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP Entities page for a specific entity.
Reactive cycle time (secs)	Specifies a value in seconds used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default value is 120 seconds.

Table continues…

Button	Description
	Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP Entities page for a specific entity.
Number of Retries	Only integers are valid values. This value specifies the number of times Session Manager polls a SIP entity before it is deemed unreachable. The default value is 1. Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP Entities page for a specific entity.

CDR

Name	Description
Enable CDR	Enables CDR at the system level for the Session Manager instance. You can then use the **Call Detail Recording** drop-down menu to individually control call detail recording for specific SIP entities.
User	User login name for CDR access.
Password	Password for CDR access. An external CDR processing adjunct uses this password for connecting to Session Manager and to transfer the generated CDR files. Normally, the adjunct logs in as *CDR_User* user ID, with a default password. The password that you specify here becomes the default password.
Confirm Password	Same password for confirmation.
Data File Format	Specifies the format for the CDR data file. Valid choices are: • Standard Flat File (default) This selection is applicable for releases earlier than Session Manager 6.3.4. • Enhanced Flat File This selection is applicable for Session Manager 6.3.4 release and later. • Enhanced XML File This selection is applicable for Session Manager 6.3.4 release and later.

Table continues…

Name	Description
Include User to User Calls	Select to include CDR records for user-to-user calls. User-to-user calls are SIP calls that originate and terminate at Session Managers, which are managed by the same System Manager.
Include Incomplete Calls	Select to include CDR records for one of the following types of incomplete calls: • Incoming or outgoing calls that are not answered. • Incoming or outgoing calls that do not have enough media resources to complete. • Other incoming and outgoing calls that are not completed for other reasons. • When, at a SIP level, the call receives any non 2xx response to the initial INVITE associated with that call.

Personal Profile Manager (PPM) - Connection Settings

Name	Description
Limited PPM client connection	Enables selecting **Maximum Connection per PPM client**. Default value is Enabled.
Maximum Connection per PPM client	Valid values are integers between 1 and 10. Default value is 3.
PPM Packet Rate Limiting	Enables selecting **PPM Packet Rate Limiting Threshold**. Default value is Enabled.
PPM Packet Rate Limiting Threshold	This value is applied per PPM client. Value Range: 1-500. The default value is 200.

Event Server

Name	Description
Clear Subscription on Notification Failure	Specifies the option to clear Subscription on Notification Failure.

Button	Description
Cancel	Cancels Session Manager addition operation.
Commit	Saves the added SIP entity as a Session Manager instance with the selected configuration options.

Branch Session Manager Administration

Branch Session Manager

Branch Session Manager, also known as Survivable Remote Session Manager, provides a SIP-enabled branch survivability solution. A Branch Session Manager handles emergency calls similarly to that of the core Session Manager.

A typical branch setup contains the following components:

- A Branch Session Manager provides service to SIP users if a WAN failure occurs between the branch and core.
- A Media Gateway connects the branch to the PSTN and provides media services such as conferencing, tones, and announcements.
- A Survivable Remote Server (also called as an LSP) is a survivable processor for the branch Media Gateways. The Survivable Remote Server (SRS) provides telephony features to SIP users using application sequencing. The SRS becomes active when a Media Gateway loses connectivity to the main Communication Manager C-LAN or PE and then registers to the SRS.
- End user devices register with the primary Session Manager as a primary controller, but use Branch Session Manager as a secondary or tertiary controller in case of a WAN failure.

A Branch Session Manager provides service when the branch loses WAN connectivity. When a WAN failure occurs,

- The Branch Media Gateway loses connectivity with the main Communication Manager (procr or C-LAN), and registers with the Branch Communication Manager SRS. As the result, the SRS starts providing service.
- The SIP phones detect connectivity is lost with the core Session Manager and subscribe to the Branch Session Manager.

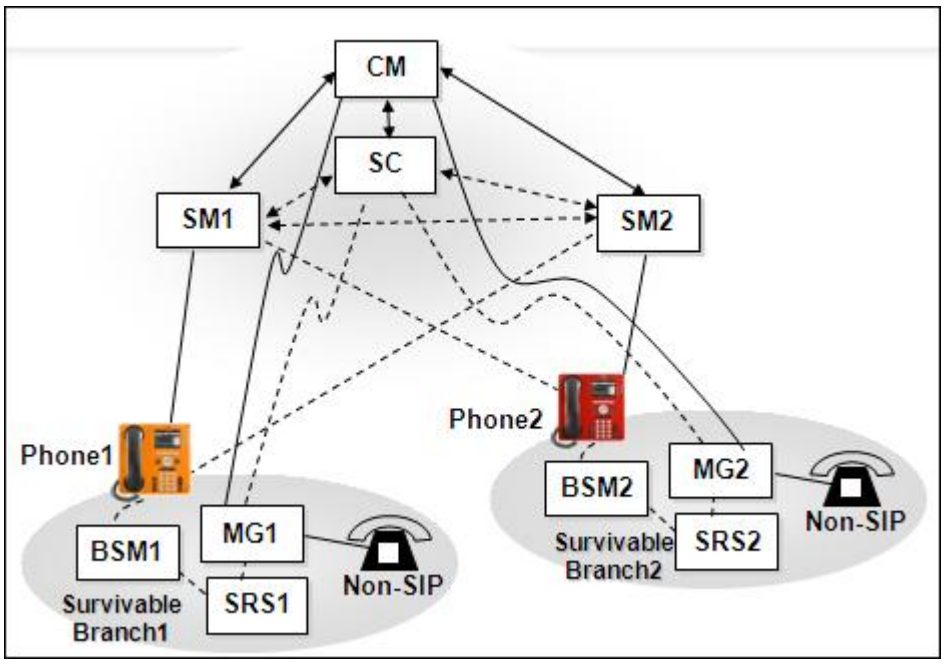
Configure each Branch Session Manager to support no more than two core Session Managers. You can configure either Session Manager as the primary or the secondary server for a branch user.

Important:

When a WAN outage occurs, the Branch Session Manager supports the SIP endpoints, possible PSTN access, and the ISDN trunks off the media gateways. The Branch Session Manager does not have access to other adjuncts due to the same WAN outage that caused the Media Gateways to register to the LSP.

For SIP trunks configured with adjuncts, the far-end node name ip-address field displays the Branch Session Manager IP address for the active Survivable Remote server (LSP).

Survivable Branch Configuration



Legend

- BSM: Branch Session Manager (also called as Survivable Remote Session Manager)
- CM: Communications Manager (Feature Server and Evolution Server)
- SRS : Survivable Remote Server (also called as LSP)
- SC: Survivable Core Server
- MG: Media Gateway
- SM: Session Manager

Configuration details

- Phone1 has SM1 as primary, SM2 as secondary, and BSM1 as the local Survivability Server.
- Phone2 has SM2 as primary, SM1 as secondary, and BSM2 as the local Survivability Server.
- Phone1 is served by CM (primary), SC (backup), and SRS (survivable condition).
- Phone2 is served by CM (primary), SC (backup), and SRS (survivable condition).
- MG1 is configured with CM, SC, and SRS1 as reprioritized list of controllers.
- MG2 is configured with CM, SC, and SRS2 as reprioritized list of controllers.

System Behavior

- Phones simultaneously register with multiple SMs in the core and BSM in the branch.
- Gateways connect with the highest priority controller that is reachable.

- If SM1 fails
  - Phone1 registers with SM2 as the active controller
  - MG1 is served by CM
  - Phone1 is still served by CM
- If Branch1 loses WAN connectivity
  - MG1 cannot connect with CM or SC. It registers with the SRS1 as the controller.
  - Phone1 cannot connect with SM1 or SM2. It re-registers with the BSM as the active controller.
  - Phones in the branch are served by survivable elements
    - SIP endpoints are served by SRS1 using BSM1.
    - Non-SIP endpoints are served by SRS1 using MG1.
- If CM fails
  - Media Gateways registers with the SC as the controller.
  - SIP phones are served by SC using SMs in the core.
  - Non-SIP phones are served by SC using Media Gateways.

Survivable Public Remote SIP Trunking

With Public SIP Trunks in a branch location, an enterprise can build network topologies to route SIP traffic to external networks using the branch locations. The network topologies can include the following:

- Intra-enterprise calls such as SIP to SIP, SIP to Non-SIP, Non-SIP to SIP, Non-SIP to Non-SIP.
- Enterprise-bound call from the PSTN (destinations are SIP and non-SIP endpoints).
- Enterprise-originated calls towards the PSTN (SIP and non-SIP originations).

BSM connects with the SIP Service Provider and supports incoming and outgoing SIP Service Provider traffic, irrespective of network connectivity to the data center. For a survivable remote configuration, the following section shows the different branch connectivity scenarios and the associated call flows:

1. Normal Scenario: All provisioned entity link connections between the BSM and the core are in service. The Media Gateway is in contact with the primary controller, that is, the core CM. No error is reported on any of the BSM SM links.
2. Failure Scenarios: All provisioned entity link connections between the BSM and the core are out of service. When the Media Gateway loses contact with the core CM, the Media Gateway attempts to re-register with the SRS. The BSM is in complete survivable mode, as there is a full WAN outage of the branch. All the components in the branch, such as phones, Media Gateway, BSM, have lost connectivity with all the components in the core, such as SM and CM.

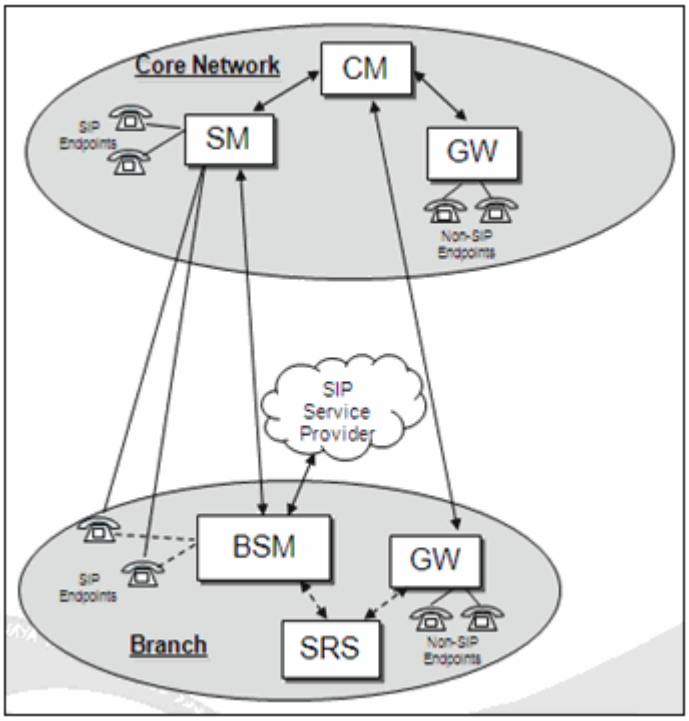
Related Links

Call Scenarios on page 390

Branch SIP Trunk administration on page 393

Call Scenarios

Normal Scenarios



- SIP phones in the branch locations are simultaneously registered with core SMs and BSM.
- SIP phones are registered with one of the core SMs as the active controller.
- Media Gateways are registered with CM, in the core.
- BSM has direct connectivity with SIP Service Provider (SP).
- BSM and SM have direct connectivity.

Following are some example call scenarios to illustrate the behavior of the feature. The scenarios listed here are not intended to be a complete list of all possible configurations and call scenarios.

Case 1: Calls incoming from the SP branch SIP trunk to a branch SIP user

1. Request arrives at BSM from SIP SP interface.
2. BSM perform ingress adaptation and routes the request to primary core SM of the called party.
3. SM invokes core CM as the sequenced application and completes sequenced application invocation.
4. SM performs contact resolution and routes the call to the SIP endpoint at the branch.

Case 2: Calls going to the SP branch SIP trunk from a branch SIP user

1. Branch SIP user initiates a call to an external number.
2. Core SM invokes core CM as a sequence application and completes sequenced application invocation.
3. Based on dial patterns, SM routes the request to the SIP SP connected with the BSM.

4. SM performs egress adaptation and Call Admission Control (CAC).
5. SM routes the request to BSM with route-through to SIP SP. Based on route-header, BSM routes the request to SIP SP.

Case 3: Calls incoming from the SP branch SIP trunk to a branch non-SIP user

1. Request arrives at BSM from SIP SP interface.
2. BSM perform ingress adaptation and then routes the request to one of the core SM instances.
3. Based on the dial pattern, SM routes the request to core CM.

   Note:

   CM-ES does CAC for this call.
4. CM processes the request and terminates the request at the branch non-SIP endpoint.

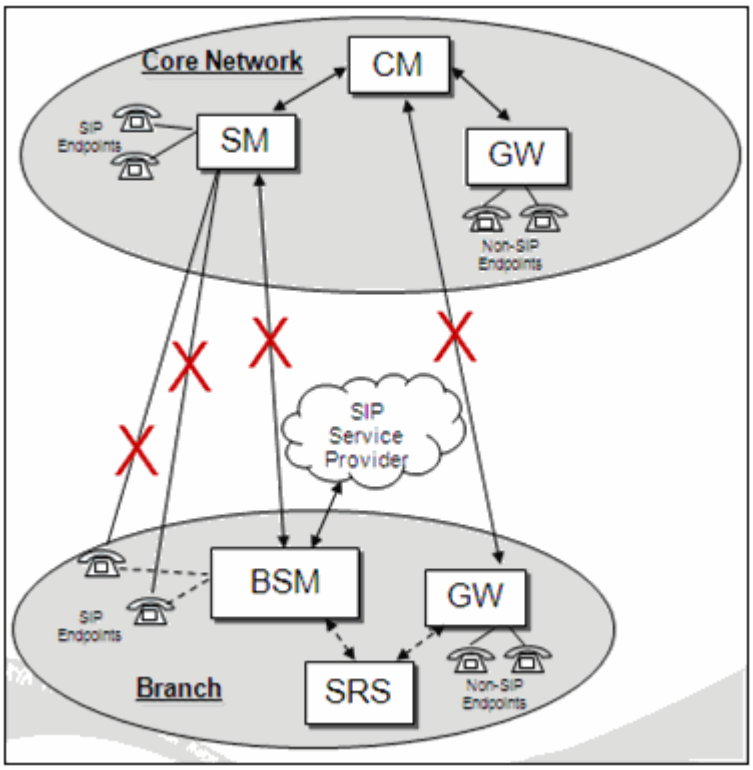
Case 4: Calls going to the SP branch SIP trunk from a branch non-SIP user

1. Branch non-SIP endpoint initiates a call to an external number.
2. CM performs call processing and routes the request to SM.
3. Based on dial patterns, the SM determines the request should be routed to SIP SP connected with BSM. SM performs egress adaptation and CAC. Finally, SM routes the request to BSM with route-through to SIP SP.
4. Based on the Route header, BSM routes the request to SIP SP.

Case 5: Calls incoming from the SP branch SIP trunk for a non-branch SIP user

1. Request arrives at BSM from SIP SP interface.
2. BSM performs ingress adaptation and then routes the request to one of the core SMs.
3. The authoritative SM performs CAC and invokes core CM as the sequenced application and completes sequenced invocation.
4. SM performs contact resolution and routes the call to the non-branch SIP user.

Failure Scenarios



- Branch users are provisioned with one core SM (SM-1) and the BSM. There is no secondary SM.
- Branch SIP phones, after losing connectivity with SM-1, mark BSM as the active controller.
- Media Gateways in the branch detect outage and connect with SRS as the controller.
- SRS activates the link with BSM.
- Branch loses connectivity with all the core networks.

Following are some example call scenarios to illustrate the behavior of the feature. The scenarios listed are not intended to be a complete list of all possible configurations and call scenarios.

Case 1: Calls incoming from the SP branch SIP trunk to a branch SIP user

1. Incoming request from the SIP SP arrives at BSM.
2. BSM performs ingress adaptation.
3. BSM detects the outage of the primary controller of the branch SIP user.
4. BSM invokes SRS as the sequenced application and completes application sequencing.
5. BSM terminates the call at the locally registered SIP endpoint.

Case 2: Calls going to the SP branch SIP trunk from a branch SIP user and entire core is unreachable

1. A call originates from branch SIP user.
2. BSM detects the outage of the primary controller of the branch SIP user.
3. BSM invokes SRS as the sequenced application and completes application sequencing.

4. BSM cannot connect with any core SM.
5. BSM performs routing based on partial routing data.
6. Before forwarding the request to SIP SP, BSM performs egress adaptation. No CAC is performed at this step.

Related Links

Survivable Branch Configuration on page 388

Branch SIP Trunk administration

About this task

When using Branch SIP Trunking, you must first administer the service providers interface as the new SIP entity of type **Service Provider**. You must also create SIP entity links between:

1. The associated BSM and one or more core SMs.
2. The service provider SIP entity and the associated BSM.

Following are the high level administration steps for the branch SIP trunk administration. See the book *Administering Avaya Aura® Session Manager* for details related to the individual steps:

Procedure

1. Add a new SIP Entity with type **Service Provider** and the IP address of the service provider equipment. See the topic *Creating SIP Entities* for details.
2. Modify Adaptation as needed. See the topics on *Adaptations* for details.
3. Add SIP Entity link between the new **Service Provider** and the BSM. See the topic *Creating Entity Links* for details.
4. Add Entity Links between the BSM and the core SMs. See the topic *Creating Entity Links* for details.

   Note:

   Links must be available between BSM and any core SMs that are controllers for users on the branch. For call routing, at least one link must be available between BSM and a core SM to make calls to the core.

5. Administer SIP Monitoring for all Branch SIP Trunks. See the topics on *SIP Entities* and *SIP Entity Monitoring*.

Related Links

Survivable Branch Configuration on page 388

Administering Branch Session Manager

Before you begin

The main Communication Manager Feature Server or Evolution Server (CM-FS/ES) is added as an Inventory element and all appropriate configurations are done for CM-FS/ES in System Manager. For details, see *Administering Avaya Aura® Communication Manager Server Options, 03-603479*.

About this task

This section provides the basic steps of Branch Session Manager (BSM) administration.

Procedure

1. Add a SIP Entity for the BSM using the IP address of the BSM Security Module.
2. Administer a BSM Instance using **Session Manager Administration** module in *System Manager web console*.
3. Create Entity Links from the BSM to the main CM server (CM-FS/ES) as per the following information:
   a. In case of BSM with CM Feature Server or Trunk Gateway (CM FS/TG):
      - Entity Link 1: BSM to core CM Feature Server
      - Entity Link 2: BSM to core CM Trunk Gateway
   b. In case of BSM with CM Evolution Server (CM-ES):

      A CM-ES can be configured using just one entity link. That entity and entity link is used for both application sequencing and trunk gateway routing.

      Each entity link must use the same port and transport as the corresponding link to the primary Session Manager in the core. The ports between the CM and SM entities must be unique.

   The BSM uses its administered entity link to the main CM to internally generate an entity and entity link connection to the SRS used for survivability mode.
4. If required, create a sequence of applications (application sequence). The CM application selected should be the same as specified on the BSM administration page.
5. Administer SIP user profiles with the BSM as the survivability server.

Adding a SIP entity as a Branch Session Manager instance

Before you begin

Ensure that the SIP entity that you want to add was created. For a Session Manager type SIP entity, the customer has to administer the listen ports on the SIP entity form. These listen ports are used by endpoints to connect to Branch Session Manager and they can be used to map different ports to different domains.

About this task

You can administer Branch Session Manager either using:

- Session Manager pages.
- Manage Elements pages that create an application system in the element inventory managed by System Manager.

Using Session Manager pages

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Session Manager Administration**.
3. Click **New** on the Branch Session Manager Instances section of Session Manager Administration screen. The system displays the Add Branch Session Manager screen.
4. In the **General** section, enter the following information:
   - From the drop-down list, select the **SIP Entity Name**.
   - In the **Description** field for this entity, add a comment if required.
   - In the **Management Access Point Host Name/IP** field, add the IP address of the host on which the management agent is running; that is, the host on which the Branch Session Manager is installed.
   - From the drop-down list, select the **Main CM for LSP**. Click the **View / Add CM Entities** link to add new CM applications.
   - From the drop-down list, select the **Direct Routing to Endpoints**.
   - From the drop-down list, select the **Adaptation for Trunk Gateway**. This selected adaptation is used by the Branch Session Manager for routing calls to or from the Communication Manager LSP trunk gateway.

     Note:

     In case of Communication Manager Feature Server (CM-FS) or Communication Manager Trunk Gateway (CM-TG), the adaptation from the core CM-TG is used by default. This field adaptation selection overrides the default CM-TG adaptation and is applied to all calls routed on the trunk gateway entity to the LSP. For Communication Manager Evolution Server (CM-ES), the default adaptation is taken from the core Communication Manager entity. The adaptation is applied either to calls that are routed through the gateway to the LSP and also to calls that are application sequenced.

   Note:

   To be a part of the Branch Session Manager instances network of an enterprise, a Branch Session Manager instance must first be administered as a management access point. This is the network mask of the domain name of the server that hosts the Branch Session Manager application. The address is passed to the security module for the agent to query the server for the required information.
5. Under the **Security Module** section, enter the following information to configure the security module:
   - In the **Network Mask** field, enter the value for the network mask. The network mask is passed to the security module. The agent configures the network mask to define the subnet that the security module is to be associated with.
   - In the **Default Gateway** field, add the correct IP address.

- In the **Call Control PHB** field, enter a value.

  The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from security module that you may expect as it travels through the IP network. All packets containing SIP signaling that leave the security module have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence—they must either support this by default or be specially configured to do so.

  Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Branch Session Manager uses a default DSCP value of 46 that indicates forwarding with the highest priority.

- In the **Speed & Duplex** field, you can configure the security module interface speed and duplex values. The drop-down menu contains a list of the valid values.
- In the **QOS Priority** field, enter the 802.1q priority value.

  This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Branch Session Manager for any SIP traffic. The default is 6. Range of this value is 0-7. This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, the lower the QOS priority number.

- In the **VLAN ID** field, enter an integer value. This is the VLAN that the Branch Session Manager is to be associated with. Call traffic segregation could be based on the VLAN associated with the Branch Session Manager.
- Select the associated SIP Firewall Configuration with the Branch Session Manager instance.

SIP Entity IP Address field is populated as per the IP address of the SIP entity.

6. In the **Monitoring** section, enter the following information to configure how this Branch Session Manager instance should monitor SIP entities:

   - To enable or disable monitoring of the SIP entities by this Branch Session Manager instance, select or clear the **Enable Monitoring** check box.
   - Type a required value in seconds for **Proactive cycle time (secs)**. The default value is 900 seconds. Branch Session Manager uses this value for monitoring and polling an administered SIP entity at this interval till that entity is reachable.
   - Type a required value in seconds for **Reactive cycle time (secs)**. The default value is 120 seconds.

     This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default value is 120 seconds.

     Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP entities screen for a specific entity.

- Type an integer value in **Number of Retries**. The default value is 1. This value specifies the number of times Branch Session Manager polls a SIP entity before it is deemed unreachable. The default value is 1.

Note:

Regardless of the administered settings, the Branch Session Manager monitors the feature server entity *avaya-lsp-fs* every 1 second. These monitoring settings are important since this link is used specially for failover and failback procedures on Branch Session Manager. If an additional connection exists to the LSP for the trunk gateway, these administered monitoring settings also applies.

7. **Personal Profile Manager (PPM) - Connection Settings** section specifies the global parameters that apply to all Branch Session Manager instances. Under the **Personal Profile Manager (PPM) - Connection Settings** section, specify related information:
   a. Select the **Limited PPM Client Connection** check box to enable selecting **Maximum Connection per PPM client**. Default value is Enabled.
   b. Specify the value of **Maximum Connection per PPM client**. Valid values are integers between 1 and 10. Default value is 3.
   c. Select the **PPM Packet Rate Limiting** check box to enable selecting **PPM Packet Rate Limiting Threshold**. Default value is Enabled.
   d. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. Value Range: 1-500. The default value is 50.

   During normal operation, Branch Session Manager receives data from a Communication Manager feature server for synchronization to Avaya SIP endpoints.
8. **Event Server** section specifies the option to clear Subscription on Notification Failure.
9. Click **Commit** .

Using Manage Elements pages

Procedure

1. On System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On New Elements page, select an application type **Session Manager**.
5. Select **Branch Session Manager** and click **Continue**.

   Add Branch Session Manager page opens.
6. In the **General** section, enter the following information:
   - From the drop-down list, select the **SIP Entity Name**.
   - In the **Description** field for this entity, add a comment if required.

- In the **Management Access Point Host Name/IP** field, add the IP address of the host on which the management agent is running; that is, the host on which the Branch Session Manager is installed.
- From the drop-down list, select the **Main CM for LSP**. Click the **View / Add CM Entities** link to add new CM applications.
- From the drop-down list, select the **Direct Routing to Endpoints**.
- From the drop-down list, select the **Adaptation for Trunk Gateway**. This selected adaptation is used by the Branch Session Manager for routing calls to or from the Communication Manager LSP trunk gateway.

Note:

In case of Communication Manager Feature Server (CM-FS) or Communication Manager Trunk Gateway (CM-TG), the adaptation from the core CM-TG is used by default. This field adaptation selection overrides the default CM-TG adaptation and is applied to all calls routed on the trunk gateway entity to the LSP. For Communication Manager Evolution Server (CM-ES), the default adaptation is taken from the core Communication Manager entity. The adaptation is applied either to calls that are routed through the gateway to the LSP and also to calls that are application sequenced.

Note:

To be a part of the Branch Session Manager instances network of an enterprise, a Branch Session Manager instance must first be administered as a management access point. This is the network mask of the domain name of the server that hosts the Branch Session Manager application. The address is passed to the security module for the agent to query the server for the required information.

7. Under the **Security Module** section, enter the following information to configure the security module:
   - In the **Network Mask** field, enter the value for the network mask. The network mask is passed to the security module. The agent configures the network mask to define the subnet that the security module is to be associated with.
   - In the **Default Gateway** field, add the correct IP address.
   - In the **Call Control PHB** field, enter a value.

     The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from security module that you may expect as it travels through the IP network. All packets containing SIP signaling that leave the security module have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence—they must either support this by default or be specially configured to do so.

     Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Branch Session Manager uses a default DSCP value of 46 that indicates forwarding with the highest priority.

- In the **Speed & Duplex** field, you can configure the security module interface speed and duplex values. The drop-down menu contains a list of the valid values.
- In the **QOS Priority** field, enter the 802.1q priority value.

  This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Branch Session Manager for any SIP traffic. The default is 6. Range of this value is 0-7. This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, the lower the QOS priority number.
- In the **VLAN ID** field, enter an integer value. This is the VLAN that the Branch Session Manager is to be associated with. Call traffic segregation could be based on the VLAN associated with the Branch Session Manager.
- Select the associated SIP Firewall Configuration with the Branch Session Manager instance.

SIP Entity IP Address field is populated as per the IP address of the SIP entity.

8. In the **Monitoring** section, enter the following information to configure how this Branch Session Manager instance should monitor SIP entities:
   - To enable or disable monitoring of the SIP entities by this Branch Session Manager instance, select or clear the **Enable Monitoring** check box.
   - Type a required value in seconds for **Proactive cycle time (secs)**. The default value is 900 seconds. Branch Session Manager uses this value for monitoring and polling an administered SIP entity at this interval till that entity is reachable.
   - Type a required value in seconds for **Reactive cycle time (secs)**. The default value is 120 seconds.

     This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default value is 120 seconds.

     Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP entities screen for a specific entity.
   - Type an integer value in **Number of Retries**. The default value is 1. This value specifies the number of times Branch Session Manager polls a SIP entity before it is deemed unreachable. The default value is 1.

   Note:

   Regardless of the administered settings, the Branch Session Manager monitors the feature server entity *avaya-lsp-fs* every 1 second. These monitoring settings are important since this link is used specially for failover and failback procedures on Branch Session Manager. If an additional connection exists to the LSP for the trunk gateway, these administered monitoring settings also applies.

9. **Personal Profile Manager (PPM) - Connection Settings** section specifies the global parameters that apply to all Branch Session Manager instances. Under the **Personal Profile Manager (PPM) - Connection Settings** section, specify related information:
    a. Select the **Limited PPM Client Connection** check box to enable selecting **Maximum Connection per PPM client**. Default value is Enabled.
    b. Specify the value of **Maximum Connection per PPM client**. Valid values are integers between 1 and 10. Default value is 3.
    c. Select the **PPM Packet Rate Limiting** check box to enable selecting **PPM Packet Rate Limiting Threshold**. Default value is Enabled.
    d. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. Value Range: 1-500. The default value is 50.

    During normal operation, Branch Session Manager receives data from a Communication Manager feature server for synchronization to Avaya SIP endpoints.
10. **Event Server** section specifies the option to clear Subscription on Notification Failure.
11. Click **Commit** .

Viewing the Branch Session Manager administration settings

About this task

You can view Branch Session Manager instances either using:

- Session Manager pages.
- Manage Elements pages.

Using Session Manager pages

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Session Manager Administration**.
3. In the Branch Session Manager Instances section, select a Branch Session Manager from the Branch Session Manager Instances list and click **View**. The View Branch Session Manager screen displays information about the selected Branch Session Manager instance.
4. After you have viewed the information, click **Return**.

Using Manage Elements pages

Procedure

1. On System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Select a Branch Session Manager instance and click **View**. The View Branch Session Manager screen displays information about the selected Branch Session Manager instance.

4. After you have viewed the information, click **Return**.

Modifying the Branch Session Manager administration settings

About this task

This option allows you to modify the configuration settings for an already configured Branch Session Manager.

You can modify Branch Session Manager either using:

- Session Manager pages.
- Manage Elements pages that creates an application system in the element inventory managed by System Manager.

Using Session Manager pages

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Session Manager Administration**.
3. Click **Edit** on the Branch Session Manager Instances section of Session Manager Administration screen. The system displays the Edit Branch Session Manager screen.
4. In the **General** section, change the following information, if required:
   - Add a comment in the Description field for the Branch Session Manager SIP entity.
   - Change the IP address of the host on which the Branch Session Manager is installed in the **Management Access Point Host Name/IP** field.
   - From the drop-down list, select the **Main CM for LSP**. Click the **View / Add CM Entities** link to add new CM applications.
   - From the drop-down list, select the **Direct Routing to Endpoints**.
   - From the drop-down list, select the **Adaptation for Trunk Gateway**. This selected adaptation is used by the Branch Session Manager during routing calls to or from the Communication Manager LSP trunk gateway.

     Note:

     In case of Communication Manager Feature Server (CM-FS) or Communication Manager Trunk Gateway (CM-TG), the adaptation from the core CM-TG is used by default. This field adaptation selection overrides the default CM-TG adaptation and is applied to all calls routed on the trunk gateway entity to the LSP. For Communication Manager Evolution Server (CM-ES), the default adaptation is taken from the core Communication Manager entity. The adaptation is applied either to calls that are routed through the gateway to the LSP and also to calls that are application sequenced.

5. In the **Security Module** section, change the following information, if required
   - Modify the network mask in the **Network Mask** field. Branch Session Manager passes this network mask to the security module. The agent configures the network mask to define the subnet that the security module is to be associated with.
   - Modify the IP address in the **Default Gateway** field.
   - Modify the value for **Call Control PHB**. The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from security module that you may expect as it travels through the IP network. All packets containing SIP signaling that leave the security module have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence--they must either support this by default or be specially configured to do so.

     Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Branch Session Manager uses a default DSCP value of 46 that indicates forwarding with the highest priority.
   - Select the **Speed & Duplex** value to configure the security module interface speed and duplex values.
   - Modify the **QOS Priority** value. This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Branch Session Manager for any SIP traffic. The default is 6. Range of this value is 0-7. This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, the lower the QOS priority number.
   - Modify the value for **VLAN ID**. This is the VLAN that the Branch Session Manager is to be associated with. Call traffic segregation could be based on the VLAN that the Branch Session Manager is associated with.
   - Modify the associated SIP Firewall Configuration with the Branch Session Manager instance.
6. In the **Monitoring** section, modify the following information as required to configure how this Branch Session Manager instance should monitor SIP entities:
   - To enable or disable monitoring of the SIP entities by this Branch Session Manager instance, select or clear the **Enable Monitoring** check box.
   - Type a required value in seconds for **Proactive cycle time (secs)**. The default value is 900 seconds.
   - Branch Session Manager uses this value for monitoring and polling an administered SIP entity at this interval till that entity is reachable.
   - Type a required value in seconds for **Reactive cycle time (secs)**. The default value is 120 seconds. This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default value is 120 seconds.

Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP entities screen for a specific entity.

- Type an integer value in **Number of Retries**. The default value is 1. This value specifies the number of times Branch Session Manager polls a SIP entity before it is deemed unreachable.

Note:

Regardless of the administered settings, the Branch Session Manager monitors the feature server entity *avaya-lsp-fs* every 1 second. These monitoring settings are important since this link is used specially for failover and failback procedures on Branch Session Manager. If an additional connection exists to the LSP for the trunk gateway, these administered monitoring settings also applies.

7. **Personal Profile Manager (PPM) - Connection Settings** section specifies the global parameters that apply to all Branch Session Manager instances. Under the **Personal Profile Manager (PPM) - Connection Settings** section, specify related information:
   a. Select the **Limited PPM client connection** check box to enable selecting **Maximum Connection per PPM client**. Default value is Enabled.
   b. Specify the value of **Maximum Connection per PPM client**. Valid values are integers between 1 and 10. Default value is 3.
   c. Select the **PPM Packet Rate Limiting** check box to enable selecting **PPM Packet Rate Limiting Threshold**. Default value is Enabled.
   d. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. Value Range: 1-500. The default value is 50.

   During normal operation, Branch Session Manager receives data from a Communication Manager feature server for synchronization to Avaya SIP endpoints.
8. **Event Server** section specifies the option to clear Subscription on Notification Failure.
9. Click **Commit**.

Using Manage Elements pages

Procedure

1. On System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Select a Branch Session Manager instances and click **Edit**. The system displays the Edit Branch Session Manager page.
4. In the **General** section, change the following information, if required:
   - Add a comment in the Description field for the Branch Session Manager SIP entity.
   - Change the IP address of the host on which the Branch Session Manager is installed in the **Management Access Point Host Name/IP** field. This is the IP address of the domain name of the server that hosts the Branch Session Manager application. Branch Session

Manager passes the address to the security module to allow the agent to query the server for the required information. To be a part of the Branch Session Manager instances network of an enterprise, a Branch Session Manager instance must first be administered as a management access point.

- From the drop-down list, select the **Main CM for LSP**. Click the **View / Add CM Entities** link to add new CM applications.
- From the drop-down list, select the **Direct Routing to Endpoints**.
- From the drop-down list, select the **Adaptation for Trunk Gateway**. This selected adaptation is used by the Branch Session Manager during routing calls to or from the Communication Manager LSP trunk gateway.

Note:

In case of Communication Manager Feature Server (CM-FS) or Communication Manager Trunk Gateway (CM-TG), the adaptation from the core CM-TG is used by default. This field adaptation selection overrides the default CM-TG adaptation and is applied to all calls routed on the trunk gateway entity to the LSP. For Communication Manager Evolution Server (CM-ES), the default adaptation is taken from the core Communication Manager entity. The adaptation is applied either to calls that are routed through the gateway to the LSP and also to calls that are application sequenced.

5. In the **Security Module** section, change the following information, if required
   - Modify the network mask in the **Network Mask** field. Branch Session Manager passes this network mask to the security module. The agent configures the network mask to define the subnet that the security module is to be associated with.
   - Modify the IP address in the **Default Gateway** field.
   - Modify the value for **Call Control PHB**. The Call Control PHB (per hop behavior) specifies the type of service and priority SIP traffic from security module that you may expect as it travels through the IP network. All packets containing SIP signaling that leave the security module have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence--they must either support this by default or be specially configured to do so.

     Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Branch Session Manager uses a default DSCP value of 46 that indicates forwarding with the highest priority.
   - Select the **Speed & Duplex** value to configure the security module interface speed and duplex values.
   - Modify the **QOS Priority** value. This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Branch Session Manager for any SIP traffic. The default is 6. Range of this value is 0-7. This value specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, the lower the QOS priority number.

- Modify the value for **VLAN ID**. This is the VLAN that the Branch Session Manager is to be associated with. Call traffic segregation could be based on the VLAN that the Branch Session Manager is associated with.
- Modify the associated SIP Firewall Configuration with the Branch Session Manager instance.

6. In the **Monitoring** section, modify the following information as required to configure how this Branch Session Manager instance should monitor SIP entities:
   - To enable or disable monitoring of the SIP entities by this Branch Session Manager instance, select or clear the **Enable Monitoring** check box.
   - Type a required value in seconds for **Proactive cycle time (secs)**. The default value is 900 seconds.
   - Branch Session Manager uses this value for monitoring and polling an administered SIP entity at this interval till that entity is reachable.
   - Type a required value in seconds for **Reactive cycle time (secs)**. The default value is 120 seconds. This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default value is 120 seconds.

     Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP entities screen for a specific entity.
   - Type an integer value in **Number of Retries**. The default value is 1. This value specifies the number of times Branch Session Manager polls a SIP entity before it is deemed unreachable.

   Note:

   Regardless of the administered settings, the Branch Session Manager monitors the feature server entity *avaya-lsp-fs* every 1 second. These monitoring settings are important since this link is used specially for failover and failback procedures on Branch Session Manager. If an additional connection exists to the LSP for the trunk gateway, these administered monitoring settings also applies.

7. **Personal Profile Manager (PPM) - Connection Settings** section specifies the global parameters that apply to all Branch Session Manager instances. Under the **Personal Profile Manager (PPM) - Connection Settings** section, specify related information:
   a. Select the **Limited PPM client connection** check box to enable selecting **Maximum Connection per PPM client**. Default value is Enabled.
   b. Specify the value of **Maximum Connection per PPM client**. Valid values are integers between 1 and 10. Default value is 3.
   c. Select the **PPM Packet Rate Limiting** check box to enable selecting **PPM Packet Rate Limiting Threshold**. Default value is Enabled.
   d. Specify the value of **PPM Packet Rate Limiting Threshold**. This value is applied per PPM client. Value Range: 1-500. The default value is 50.

During normal operation, Branch Session Manager receives data from a Communication Manager feature server for synchronization to Avaya SIP endpoints.

8. **Event Server** section specifies the option to clear Subscription on Notification Failure.
9. Click **Commit**.

Deleting a Branch Session Manager instance

About this task

You can delete Branch Session Manager instances either using:

- Session Manager pages.
- Manage Elements pages.

Using Session Manager pages

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Session Manager Administration**.
3. Select a Branch Session Manager instance from the list and click **Delete**.
4. On the Delete Confirmation screen, click **Delete** to delete the Branch Session Manager instance.

Note:

Before deleting a Branch Session Manager instance, you should either dissociate the Session Manager instance from all the related Communication Profiles or delete the associated users.

Using Manage Elements pages

Procedure

1. On System Manager Web Console, click **Elements** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. Select a Branch Session Manager instance and click **Delete**.
4. On the Delete Confirmation screen, click **Delete** to delete the Branch Session Manager instance.

Note:

Before deleting a Branch Session Manager instance, you should either dissociate the Session Manager instance from all the related Communication Profiles or delete the associated users.

Delete Confirmation page field descriptions

Button	Description
Delete	Deletes the selected Branch Session Manager instance.
Cancel	Cancels the deletion of the selected Branch Session Manager instance.

Branch Session Manager page field descriptions

General

Name	Description
SIP Entity Name	Name of the SIP entity that you wish to add as a Branch Session Manager instance. The entity must be of type Session Manager and it must be in Sync state.
Description	Description of the entity added. This field is optional.
Management Access Point Host Name / IP	The IP address of the host on which the management agent is running, that is, the host on which the Branch Session Manager is installed.
Main CM for LSP	Main CM for the LSP associated with this Branch Session Manager. **Refresh**: Updates the list of CM Systems. **View/Add CM Systems**: Enables adding and viewing of currently provisioned CM Systems.
Direct Routing to Endpoints	Option to enable or disable direct routing to endpoints.
Adaptation for Trunk Gateway	Digit conversion when routing calls to or from the Communication Manager LSP trunk gateway.

Security Module

Name	Description
SIP Entity IP Address	Provides IP address of the Branch Session Manager as specified in the SIP Entity Details screen.
Network Mask	Enables you to enter the value of the Network mask. The network mask is passed to the SM100 agent. The agent configures the network mask to define the subnet that the SM100 card is to be associated with.
Default Gateway	Provides the IP address of the default gateway.

Table continues…

Name	Description
Call Control PHB	Specifies the type of service and priority SIP traffic from SM100 may expect as it travels through the IP network. All packets containing SIP signaling that leave SM100 have the specified value in the DSCP (differentiated service code point) field of the IP header. Intervening routers may or may not treat packets with this value with a different level of precedence--they must either support this by default or be specially configured to do so. Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Branch Session Manager uses a default DSCP value of 46 that indicates forwarding with the highest priority.
QOS Priority	Specifies the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance for a call on a local area network. The higher the priority, lower the QOS priority number. This is the value of 802.1q priority bit (Layer 2 QoS) configuration to be used by Branch Session Manager for any SIP traffic. The default is 6. Range of this value is 0-7.
Speed & Duplex	Enables configuring of the security module interface speed and duplex values. The drop-down menu contains a list of the valid values.
VLAN ID	The VLAN that Branch Session Manager should be associated with. Call traffic segregation could be based on the VLAN that Branch Session Manager is associated with.
SIP Firewall Configuration	Shows the associated SIP Firewall Configuration with the Branch Session Manager instance.

Monitoring

Button	Description
Enable Monitoring	Select to enable monitoring of the administered SIP entities by the added Branch Session Manager instance. Clear the check box to disable monitoring.
Proactive cycle time (secs)	Enter a value in seconds for polling the administered SIP entities by the added Branch Session Manager. Monitoring ensures that the entities are still reachable. Proactive monitoring occurs as long as no outages are detected. The default is 900 seconds. These default values are used for each administered SIP entity unless overridden by the Monitoring

Table continues…

Button	Description
	options that you specified on the SIP entities page for a specific entity.
Reactive cycle time (secs)	Enter a value in seconds. This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. The default value is 120 seconds. Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP entities page for a specific entity.
Number of Retries	Enter an integer value. This value specifies the number of times Branch Session Manager polls a SIP entity before it is deemed unreachable. The default value is 1. Branch Session Manager uses these default values for each administered SIP entity unless overridden by the Monitoring options that you specified on the SIP entities page for a specific entity.

Personal Profile Manager (PPM) - Connection Settings

Name	Description
Limited PPM client connection	Enables selecting **Maximum Connection per PPM client**. Default value is Enabled.
Maximum Connection per PPM client	Valid values are integers between 1 and 10. Default value is 3.
PPM Packet Rate Limiting	Enables selecting **PPM Packet Rate Limiting Threshold**. Default value is Enabled.
PPM Packet Rate Limiting Threshold	This value is applied per PPM client. Value Range: 1-500. The default value is 25.

Event Server

Name	Description
Clear Subscription on Notification Failure	Specifies the option to clear Subscription on Notification Failure.

Button	Description
Cancel	Cancels the Branch Session Manager addition operation.

Table continues…

Button	Description
Commit	Saves the added SIP entity as a Branch Session Manager instance with the selected configuration options.

Communication Profile Editor

Communication Profile Editor

Using the Communication Profile Editor, you can:

- View a list of all Session Manager Communication Profiles using sort and filter options.
- Bulk edit required Communication Profile attributes across selected Communication Profiles. For example, replace a Session Manager instance for the selected Communication Profiles at one time instead of editing individual profiles using the User Profile Edit screen.
- View the background edit job status of bulk editing a Communication Profile.
- View the Communication Profile edit failures during bulk editing operations.

Important:

You add a SIP endpoint to the Aura Network by creating a Communication Profile that contains a Communication Manager endpoint profile and a Session Manager profile. The Communication Manager profile associates the user with a station on a Communication Manager that is in the core network. The Session Manager profile assigns the primary and secondary Session Managers of the user, the application sequences, and the survivability server. For correct application sequencing to Communication Manager, the application sequences must reference the same Communication Manager as the Communication Manager endpoint profile. For correct survivability configuration, if a Branch Session Manager is specified as the survivability server, the Branch Session Manager must also reference the same Communication Manager as the Communication Manager endpoint profile.

Note:

When you change the Primary Session Manager, the Secondary Session Manager or the Survivable Server (Branch Session Manager) for one or more users using the Communication Profile Editor page, the system performs a check to ensure that valid SIP Entity links exist between the components. If any of these links do not exist, the system automatically creates the required links. The default protocol and ports of the generated links are specified in the **Entity Links** section of the **Routing** > **Defaults - Personal Settings** page.

Viewing Communication Profiles

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Communication Profile Editor** to open the Communication Profile Editor page.

   The Communication Profile Editor page displays under the Session Manager Communication Profiles section the list of all Session Manager Communication Profiles provisioned for all the registered users.
3. To view using sorting option, click a column title to sort the information in the table as the primary sorting order.
4. To view using filtering option, enable **Filter** option. Filtering can be as a compound of one or more fields. On filtering, the table displays only those results that match the filtering criteria.

Related Links

Communication Profile Editor field descriptions on page 414

Customizing column display

About this task

You can customize the column display on the Communication Profile Editor page. Use any of the following methods to customize a column display:

- Select the columns you need to get displayed in the table
- Order the appearance of the columns
- Reset the column appearance to the default columns

Note:

The customization settings are valid for the current user session, that is, after the user logs out, the customization settings revert to the default appearance.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Communication Profile Editor** to open Communication Profile Editor page.
3. Click **Customize** link to view this section.
4. Select columns in **Available Columns** and click the **Move** link to move the selected columns to **Display Columns** list. Click **Move All** link to move all columns to be displayed.
5. Click **Remove** and **Remove All** links to remove selected or all columns from displayed columns.

6. To rearrange the selected columns under **Display Columns**, perform the following steps:
   a. Click the **Top** link to move the selected column to the top of the list.
   b. Click the **Up** link to move the selected column one position up on the list.
   c. Click the **Down** link to move the selected column one position down on the list.
   d. Click the **Up** link to move the selected column to the bottom of the list.
7. Click **Default** to restore the default settings.
8. Click **Apply** to save the changed settings.
9. Click **Close** to close the customization section.

Modifying Communication Profiles

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Communication Profile Editor** to open the Communication Profile Editor page.
3. In the Session Manager Communication Profiles section, select the rows that you need to be modified. Click the **All** link at the bottom left of the table to select all of the rows.
4. In the New Communication Profile Values section, all fields initially have the default value as Use existing values. Modify the field values to be set as property values for the selected list of Communication Profiles.

   You cannot set the value for **Primary Session Manager** and **Home Location** fields as None. For adding a new value for the **Home Location** field, you need to add location using **Routing** > **Locations** menu selection.
5. Click **Commit Changes** to save the changes. In the Communication Profile Edit Confirmation screen, click **Commit** to save the changes.

Related Links

Communication Profile Edit Confirmation page field descriptions on page 417
Communication Profile Editor field descriptions on page 414

Viewing background edit job status

About this task

When the number of simultaneous Communication Profile editing operations exceed 15 then these operations are queued as batch jobs.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.

2. In the left navigation pane, click **Communication Profile Editor** to open the Communication Profile Editor page.

   In the Background Edit Job Status section, you can view the status of all background edit jobs since the last restart of System Manager.

Related Links

Communication Profile Editor field descriptions on page 414

Viewing Communication Profile edit failures

Procedure

1. On the System Manager Web Console, under **Elements**, click **Session Manager**.
2. Click **Communication Profile Editor** to open the Communication Profile Editor page.
3. In the Background Edit Job Status section, select the edit job that did not finish running successfully.
4. Click **View Profile Edit Failures** to view the details of all Communication Profiles that cannot be modified in the selected job run.

   The Session Manager Communication Profiles section shows the details of those existing profiles that could not be edited due to the failed job run.
5. Click **Return to View All Profiles** to return to the original Communication Profile Editor screen.

Related Links

Communication Profile Editor field descriptions on page 414

Stopping Communication Profile editing jobs

About this task

This functionality enables termination of the current running Communication Profile background editing jobs.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Communication Profile Editor** to open the Communication Profile Editor page.
3. In Local Host Name Resolution page, in the Background Job Status section, select a running edit job and click **Stop Job**.

Related Links

Communication Profile Editor field descriptions on page 414

Communication Profile Editor field descriptions

Customize Column Display section

List	Description
Available Columns	Shows the list of available columns.
Display Columns	Shows the list of selected columns.

Link	Description
Customize	Expands **Customize Column Display** section.
Move	Moves selected items from **Available Columns** list to the **Display Columns** list.
Move All	Moves all items from **Available Columns** list to the **Display Columns** list.
Remove	Removes selected items from the **Display Columns** list.
Remove All	Moves all items from the **Display Columns** list.
Top	Moves the selected items of **Display Columns** list to the top of the list.
Up	Moves the selected items of **Display Columns** list to one position up in the list.
Down	Moves the selected items of **Display Columns** list to one position down in the list.
Bottom	Moves the selected items of **Display Columns** list to the bottom of the list.

Button	Description
Default	Reverts back to the default column settings of **Available Columns** and **Display Columns** lists.
Apply	Applies the changes made in the column customizing lists to the **AST Device Notifications** section.
Close	Collapses **Customize Column Display** section.

Session Manager Communication Profiles

Name	Description
Login Name	Full login name of the user and is a unique name that gives access to the system.
Address: Handle	Handle part of the Communication Address.

Table continues…

Name	Description
	Note: The displayed address can be either the “E. 164 ” or the “Avaya E.164” address as specified in the User Profile page.
Address: Domain	Domain part of the Communication Address.
Primary Session Manager	The name of the primary Session Manager that is used as the default access point for connecting devices associated with the Communication Profile to the Avaya Aura® network. You must select the Session Manager server.
Secondary Session Manager	The name of the secondary Session Manager that provides continued service to SIP devices associated with the Communication Profile when the primary Session Manager server becomes unavailable. A selection is optional.
Origination Sequence	Defines application sequences that will be invoked when the system routes the calls from this user. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, then Communication Manager must be the same in both the sequences.
Termination Sequence	Defines application sequences that will be invoked when the system routes the calls to this user. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, then Communication Manager must be the same in both the sequences.
Conference Factory Set	Name of the Conference Factory Set associated with this user.
Survivability Server	Name of the Survivability Server that provide survivability communication services for devices associated with a Communication Profile, when the local connectivity to Session Manager instances in the Avaya Aura® core is lost.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this Communication Profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.

Table continues…

Name	Description
	The values must be numeric in the range from 1 to 10, with the default of 1.
Home Location	Specify a Home Location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any of the location. This is a mandatory field. **Note:** A user's call is routed according to the user's home location except for the following cases: • CAC (Call Admission Control) routes based on actual location • Emergency calling routes based on actual location
Enable Centralized Call History	Enable (Yes) or disable (No) Call History logging.

The field descriptions for **New Communication Profile Values** section are same as above. Click **Commit Changes** to save the field values for the selected Communication Profiles.

Background Edit Job Status

This section provides a list of Communication Profile editing operations that run as background jobs since the last restart of System Manager. When the number of simultaneous Communication Profile editing operations exceed 15, the system queues these operations as batch jobs.

Button	Description
View Profile Edit Failures	Shows the details of all Communication Profiles that could not be modified in the selected job run and states the reason for the editing failures.
Stop Job	This operation stops the current running background edit job.

Name	Description
Start Time	Start time of the background edit job.
Status	Status of completion of the background edit job.
Percent Completed	Percentage completion of the background edit job.
Total Edits to Perform	Number of background edits performed in the job run.
Failed Edits	Number of failed background edits during the job run.
Last Updated	Finish time of the background edit job run.
Job Name	Name of the background edit job.

Related Links

Viewing Communication Profiles on page 411
Modifying Communication Profiles on page 412
Viewing background edit job status on page 412
Stopping Communication Profile editing jobs on page 413
Viewing Communication Profile edit failures on page 413

Communication Profile Edit Confirmation page field descriptions

Button	Description
Commit	Saves the changes to the selected Session Manager Communication Profiles. **Note:** If the Communication Profiles for bulk editing equals 15 or less in number then the edit changes are committed immediately. Otherwise for Communication Profiles numbering more than 15, the edit changes run as background job.
Cancel	Cancels the changes to the selected Session Manager Communication Profiles.

Related Links

Modifying Communication Profiles on page 412

Network Configuration

Failover Groups

A Failover Group is a group of two active Session Manager instances that are interconnected to ensure high availability of Session Manager services.

During normal operations, only one Session Manager instance in a Failover Group is preferred to handle a call and the other instance is active but considered as backup. In cases when the preferred Session Manager instance fails to handle a call or becomes unreachable to the peer SIP entities, the failover mechanism preserves the session information and switches the call control from the failed Session Manager instance to the backup Session Manager instance. The backup Session Manager instance then uses the preserved session information and resumes the call.

You can associate peer SIP entities with the Failover Group. These peer SIP entities can detect the Session Manager instance failure and reroute the call to the backup Session Manager instance.

Each Failover Group has a Group Name and a unique Failover Group Domain Name (FGDN) for each Session Manager instance in the group. The peer SIP entities use FGDN to resolve the preferred as well as the backup Session Manager instance at the time of network outage. The Failover Group has two ordered resolution sets, namely Session Manager 1 Preferred Domain Name and Session Manager 2 Preferred Domain Name.

- Session Manager 1 Preferred Domain Name resolves the preferred Session Manager instance as high priority and the backup Session Manager instance as secondary
- Session Manager 2 Preferred Domain Name resolves the backup Session Manager instance as high priority and the operational Session Manager instance as secondary

In some cases, the source and the destination entities in a call do not have the same Failover Group domain associations. To preserve a call in such cases, Session Manager Failover Group provides a Two-Tier Routing mechanism called route-through . Two-Tier routing mechanism ensures that during the Session Manager outage, either entity can route responses or mid-dialog requests using alternate Session Manager instances of different Failover Groups.

For more details and comprehensive scenarios, see Scenarios for Two-Tier Routing on page 418.

See the book *Call Preservation Feature Description and Administration Guide* for detailed system administration of different configurations.

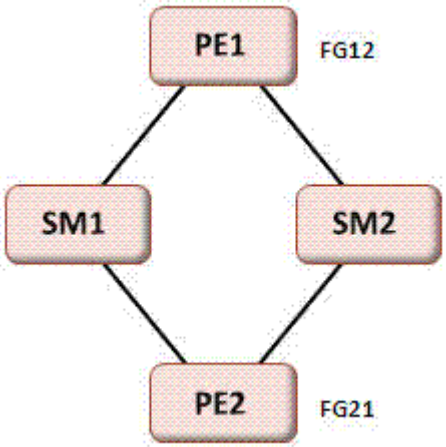
Scenarios for Two-Tier Routing

The Two-Tier Routing, route through mechanism of Failover Group feature, at the time of outage helps in call preservation even if the source and the destination peer SIP entities in a call are associated with different Session Manager instances of different Failover Groups.

The following sample scenarios describe the call routing process in different situations.

Scenario 1

In this scenario, the source and the destination Peer SIP entities have different associated failover group domains, and are connected to the same set of Session Manager instances.



In short, PE1 prefers SM1 (Failover Group FG12) while PE2 prefers SM2 (Failover Group FG21).

In this case, FG12 and FG21 resolve SM1 as well as SM2.

During normal condition, the request and response between PE1 and PE2 is routed as: PE1—SM1—SM2—PE2

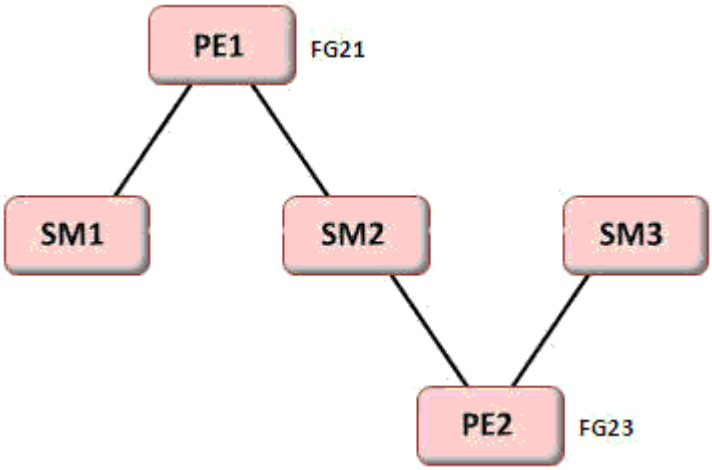
If SM1 fails, the request and response is routed as: PE1—SM2—SM2—PE2

If SM2 fails, the request and response is routed as: PE1—SM1—SM1—PE2

In this way, Failover Group preserves the call between PE1 and PE2.

Scenario 2

In this scenario, the source and the destination Peer SIP entities have different associated failover group domains, and different set of Session Manager instances. However, both the Peer SIP entities are connected to the common Session Manager instance.



In short, PE1 prefers SM2 (Failover Group FG21) and PE2 also prefers SM2 (Failover Group FG23).

In this case, FG21 and FG23 resolve SM2. There is no direct connectivity between SM1 and PE2 as well as SM3 and PE1.

During normal condition, the request and response between PE1 and PE2 is routed as: PE1–>SM2–>SM2–>PE2

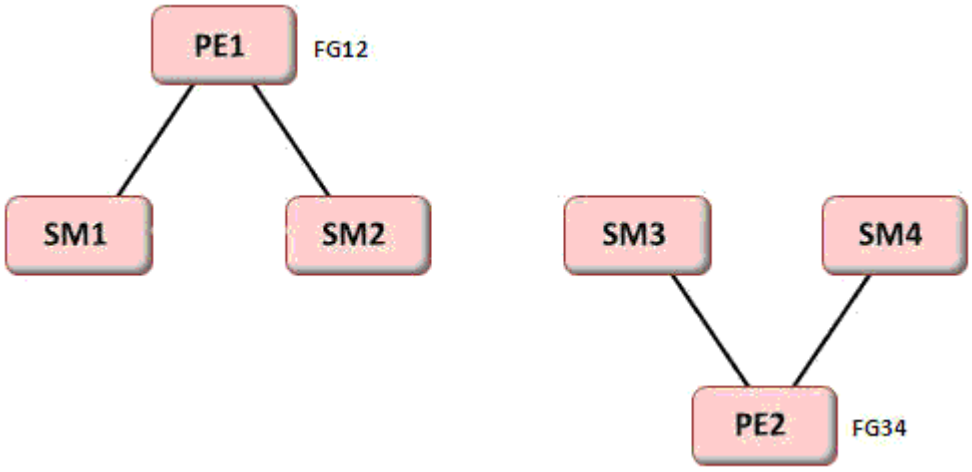
If SM2 fails, the Failover Group feature establishes a connection (Two Tier Routing or route through) between SM1 and SM3.

Then, the request and response is routed as: PE1–>SM1–>SM3–>PE2

In this way, Failover Group preserves the call between PE1 and PE2.

Scenario 3

In this scenario, the source and the destination Peer SIP entities have different associated failover group domains, different set of Session Manager instances, and both the Peer SIP entities are connected to the different Session Manager instance.



In short, PE1 prefers SM1 (Failover Group FG12) while PE2 prefers SM3 (Failover Group FG34).

In this case, there is no direct connectivity between SM1 and PE2 as well as SM4 and PE1.

During normal condition, the request and response between PE1 and PE2 is routed as: PE1–>SM1–>SM3–>PE2

If SM1 fails, the Failover Group feature establishes a connection (Two Tier Routing or route through) between SM2 and SM3.

Then, the request and response is routed as: PE1–>SM2–>SM3–>PE2

If SM3 fails, the Failover Group feature establishes a connection (Two Tier Routing or route through) between SM1 and SM4.

Then, the request and response is routed as: PE1–>SM1–>SM4–>PE2

In this way, Failover Group preserves the call between PE1 and PE2.

Failover Groups Page Field Description

Button	Description
Add	Opens the Add Failover Group page. Use this page to add new Failover Groups.
Edit	Opens the Edit Failover Group page. Use this page to modify existing Failover Groups.
Delete	Opens delete confirmation page. Use this page to delete one or more existing Failover Groups.
Manage Peer Entities	Opens the Managing Peer SIP Entities page. Use this page to associate or remove peer SIP entities with a Session Manager instance.

Fields	Description
Group Name	Name of the Failover Group.

Table continues…

Fields	Description
Session Manager 1	
Preferred Domain Name	A unique and a fully qualified preferred domain name for the backup Session Manager instance of the Failover Group.
Session Manager	Name of the operational Session Manager instance from the drop-down list.
Session Manager 2	
Preferred Domain Name	A unique and a fully qualified preferred domain name for the backup Session Manager instance of the Failover Group.
Session Manager	Name of the backup Session Manager instance from the drop-down list. **Note:** You must not select the same Session Manager instance for Session Manager 1 and Session Manager 2.

Related Links

Adding a new Failover Group in Session Manager on page 421
Editing Failover Group information in Session Manager on page 423
Deleting Failover Group from Session Manager on page 425
Adding peer SIP entities in Failover Group on page 426
Removing peer SIP entities from Failover Group on page 428

Adding a new Failover Group in Session Manager

Before you begin

Ensure that you have added Session Manager instances and peer SIP entities to associate with the Failover Group. Each Session Manager instances that are members of a Failover Group needs to have failover ports administered, one per supported transport type – TCP and TLS, for ensuring call preservation flows.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **Failover Group** to open the **Failover Groups** page.
3. To add a new Failover Group entry, click **Add**.
4. On the **Add Failover Group** page, enter the appropriate information in the as follows:
   - **Group Name** : Enter a name for the Failover Group.
   - **Preferred Domain Name** : Enter a unique and a fully qualified preferred domain name for the operational Session Manager instance of the Failover Group. The Preferred Domain name for Session manager 1 resolves to SM1 and SM2, preferring SM1 over SM2.

- **Session Manager** : From the drop-down menu, select an appropriate operational Session Manager instance . If you do not administer the TCP and TLS failover listen port for the selected Session Manager entity, then a link appears to navigate to the appropriate Network Routing Policy (NRP) page to administer these ports.
- **Preferred Domain Name** : Enter a unique and a fully qualified preferred domain name for the backup Session Manager instance of the Failover Group. The Preferred Domain name for Session manager 2 resolves to SM2 and SM1, preferring SM2 over SM1.
- **Session Manager** : Select an appropriate backup Session Manager instance from the drop-down menu. If TCP and TLS failover listen port are not administered for the selected Session Manager entity, then a link appears to navigate to the appropriate Network Routing Policy (NRP) page to administer these ports.

Note:

Do not select the same Session Manager instance for Session Manager 1 and Session Manager 2.

5. Click **Commit**. The **Session Manager Entity Link Audit** page opens that shows the list of Trusted Entity Links that must be added for ensuring failover service.

   System runs an entity link audit to ensure every Session Manager that are members of a failover group are connected to every other such Session Manager by a TCP and a TLS entity link using administered failover ports of each Session Manager. Entity link audit process is based on the following cases:

   - If one or more such entity links have not yet been added.
   - If existing entity links do not use the correct listen ports or is not trusted.

   For example, if SM1 and SM2 constitute one Failover Group, and SM2 and SM3 constitute another Failover Group, Session Manager runs an audit and generates the missing entity links automatically between SM1 and SM2, SM2 and SM3, and SM1 and SM3 at the failover ports for each transport type TCP and TLS . The link between SM1 and SM3 is a newly generated link.

6. To add the links on the **Session Manager Entity Link Audit** page, click **Commit** .

Related Links

Failover Groups Page Field Description on page 420
Add Failover Group Page Field Description on page 422

Add Failover Group Page Field Description

Fields	Description
Group Name	Name of the Failover Group.
Session Manager 1	
Preferred Domain Name	A unique and a fully qualified preferred domain name for the backup Session Manager instance of the

Table continues…

Fields	Description
	Failover Group. The Preferred Domain name for Session manager 1 resolves to SM1 and SM2, preferring SM1 over SM2.
Session Manager	Name of the operational Session Manager instance from the drop-down list.
Session Manager 2	
Preferred Domain Name	A unique and a fully qualified preferred domain name for the backup Session Manager instance of the Failover Group. The Preferred Domain name for Session manager 2 resolves to SM2 and SM1, preferring SM2 over SM1.
Session Manager	Name of the backup Session Manager instance from the drop-down list. **Note:** You must not select the same Session Manager instance for Session Manager 1 and Session Manager 2.

Button	Description
Commit	Creates a new Failover Group.
Cancel	Cancels the Failover Group creation.

Related Links

Adding a new Failover Group in Session Manager on page 421

Editing Failover Group information in Session Manager

Before you begin

Ensure that you have added Session Manager instances and peer SIP entities to associate with the Failover Group. Session Manager instances need to have failover ports administered, one per supported transport type, that is , TCP and TLS, for ensuring call preservation flows.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **Failover Group** to open the **Failover Groups** page.
3. Select the Failover Group for modification and click **Edit**.

   You can edit only one Failover Group at one time.
4. Modify the required fields on the Edit Failover Group page as follows:
   - **Group Name** : Modify the name of the Failover Group, if required.
   - **Preferred Domain Name** : Modify the preferred domain name for the operational Session Manager instance of the Failover Group, if required. You must enter a unique and a fully

qualified domain name. The Preferred Domain name for Session manager 1 resolves to SM1 and SM2, preferring SM1 over SM2.

- **Session Manager** : Select the appropriate Primary Session Manager instance from the drop-down list, if required. If TCP and TLS failover listen port are not administered for the selected Session Manager entity, then a link appears to navigate to the appropriate Network Routing Policy (NRP) page to administer these ports.
- **Preferred Domain Name** : Modify the preferred domain name for the backup Session Manager instance of the Failover Group, if required. You must enter a unique and a fully qualified domain name. The Preferred Domain name for Session manager 2 resolves to SM2 and SM1, preferring SM2 over SM1.
- **Session Manager** : Select the appropriate backup Session Manager instance from the drop-down list, if required. If TCP and TLS failover listen port are not administered for the selected Session Manager entity, then a link appears to navigate to the appropriate Network Routing Policy (NRP) page to administer these ports.

Note:

Do not select the same Session Manager instance for Session Manager 1 and Session Manager 2.

5. Click **Commit**. The Session Manager Entity Link Audit page shows the list of Trusted Entity Links that must be added for ensuring failover service.

   System runs an entity link audit to ensure every Session Manager that are members of a failover group are connected to every other such Session Manager by a TCP and a TLS entity link using administered failover ports of each Session Manager. Entity link audit process is based on the following cases:

   - If one or more such entity links has not yet been added.
   - If existing entity links do not use the correct listen ports or is not trusted.

   For example, if SM1 and SM2 constitute one Failover Group, and SM2 and SM3 constitute another Failover Group, Session Manager runs an audit and generates the missing entity links automatically between SM1 and SM2, SM2 and SM3, and SM1 and SM3 at the failover ports for each transport type, TCP and TLS. The link between SM1 and SM3 is a newly generated link.

6. To add the links on **Session Manager Entity Link Audit** page, click **Commit** .

Related Links

Failover Groups Page Field Description on page 420
Edit Failover Group Page Field Description on page 424

Edit Failover Group Page Field Description

Fields	Description
Group Name	Name of the Failover Group.

Table continues…

Fields	Description
Session Manager 1	
Preferred Domain Name	A unique and a fully qualified preferred domain name for the backup Session Manager instance of the Failover Group. The Preferred Domain name for Session manager 1 resolves to SM1 and SM2, preferring SM1 over SM2.
Session Manager	Name of the operational Session Manager instance from the drop-down list.
Session Manager 2	
Preferred Domain Name	A unique and a fully qualified preferred domain name for the backup Session Manager instance of the Failover Group. The Preferred Domain name for Session manager 2 resolves to SM2 and SM1, preferring SM2 over SM1.
Session Manager	Name of the backup Session Manager instance from the drop-down list. **Note:** You must not select the same Session Manager instance for Session Manager 1 and Session Manager 2.

Button	Description
Commit	Saves the changes to the Failover Group.
Cancel	Cancels the Failover Group information modification.

Related Links

Editing Failover Group information in Session Manager on page 423

Deleting Failover Group from Session Manager

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **Failover Group** to open the **Failover Groups** page.
3. Select the respective check box for the Failover Group from the list and click **Delete**.

   You can delete more than one Failover Group simultaneously.
4. On the delete confirmation notice, click **OK**.
5. Click **Refresh** to refresh the data.

Related Links

Failover Groups Page Field Description on page 420

Managing peer SIP entities for Failover Group

This section provides the basic steps for managing peer SIP entities associated with the respective Failover Group. You can add or remove one or more peer SIP entities within the Failover Group.

The display criteria for peer SIP entities while adding these entities in a Failover Group is as follows:

- One peer SIP entity can be associated with only one Failover Group. Hence, when you need to add peer SIP entities, only those entities are displayed that are not associated to any other Failover Group.
- Session Manager type entities are not displayed.

Manage Peer Sip Entities Page Field Description

Name	Description
Name	Name of the peer SIP entity.
Address	IP address/FQDN of the peer SIP entity.
Type	SIP entity type.
Location	Location details of the peer SIP entity.

Button	Description
Add	Opens Add Peer SIP Entities page using which you can add the selected peer SIP entities to the Failover Group.
Remove	Removes the selected peer SIP entity from the Failover Group.
Remove All	Removes all the peer SIP entity from the Failover Group.

Related Links

Adding peer SIP entities in Failover Group on page 426
Removing peer SIP entities from Failover Group on page 428

Adding peer SIP entities in Failover Group

Before you begin

Before starting this procedure, make sure that the peer SIP entities you want to add are created. Define entity links between peer SIP entities and both Session Manager instances in the Failover Group.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **Failover Group** to open the **Failover Groups** page.
3. Select the respective check box for the Failover Group from the list and click **Manage Peer Entities** to open the Manage SIP Entities page that shows the list of associated SIP entities.

4. Click **Add** to view the list of all of the previously administered SIP entities.
5. Click **Refresh** to refresh the list of administered SIP entities.
6. On the Add Peer SIP Entities page, select the respective peer SIP entities to be added to the Failover Group.
7. Click **Add Selected** for associating the selected peer SIP entities with the Failover Group.

Next steps

Session Manager automatically runs an audit process to ensure the existence of entity links between Session Manager instances and the associated peer SIP entities. Based on the audit process:

- If there are no Entity Links between the peer SIP entity and either of Session Managers in the Failover Group, the system displays an error message that Entity Links must be added in order to perform the operation.
- If there is an Entity Link between the SIP entity (for TCP or TLS) and only one of the Failover Group Session Managers, the system displays a message that a trusted Entity Link will be added between the SIP Entity and the other Session Manager before the operation can be completed.
- If any of the Entity Links between the SIP Entity and Failover Group Session Managers are not trusted or do not use the Failover listen port of Session Manager as the Session Manager listen port, the system displays a message that these Entity Links will be updated before the operation can be completed.

Related Links

Failover Groups Page Field Description on page 420
Manage Peer Sip Entities Page Field Description on page 426
Add Peer SIP Entities Page Field Description on page 427

Add Peer SIP Entities Page Field Description

Name	Description
Name	Name of the peer SIP entity.
Address	IP address/FQDN of the peer SIP entity.
Type	SIP entity type.
Location	Location details of the peer SIP entity.

Button	Description
Add Selected	Adds the peer SIP entities to the Failover Group.
Cancel	Cancels the addition of the selected peer SIP entities to the Failover Group.

Related Links

Adding peer SIP entities in Failover Group on page 426

Removing peer SIP entities from Failover Group

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **Failover Group** to open the **Failover Groups** page.
3. Select the respective check box for the Failover Group from the list and click **Manage Peer Entities**.
4. On the Manage Peer SIP Entities page, select the check boxes for the peer SIP entities you need to remove.

   Note:

   You must select at least one peer SIP entity to enable **Remove** and **Remove All** buttons.
5. Click **Remove** to remove the selected peer SIP entities, or click **Remove All** to remove all the peer SIP entities simultaneously.
6. On the delete confirmation notice, click **OK.**
7. Click **Refresh** to refresh the data.

Related Links

Failover Groups Page Field Description on page 420
Manage Peer Sip Entities Page Field Description on page 426

Local Host Name Resolution

About Local Host Name Resolution

Session Manager can locally resolve hostnames into an ordered set of IP address, port, and transport tuples and can assign priority and weights to each tuple. Local Hostname Resolution is only applied to hostnames provisioned by the administrator and overrides normal DNS resolution. For example, if Session Manager is attempting to resolve nj.proxy.avaya.com, and that hostname is provisioned as a local hostname, Session Manager will skip DNS resolution and instead determine the request target using the tuples for nj.proxy.avaya.com that it has been provisioned with. To route a SIP INVITE, Session Manager needs the IP addresses corresponding to the Fully Qualified Domain Name (FQDN) in the INVITE. To resolve a host name by replacing it with its IP address, Session Manager checks for the host name on the local network. When the host name cannot be resolved through broadcasting on the local network, Session Manager searches for it in the host names file or by querying the DNS server that maintains the host name to IP address mapping.

Resolving local host name

About this task

Local Host Name Resolution screen allows you to create, edit, and delete local host name entries. Host name entries on this screen override the information provided by DNS.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** .
3. Click **Network Configuration** > **Local Host Name Resolution**.
4. To add a host name entry, click **New**.
5. Enter host name information on the New Local Host Name Entries screen as follows.

   You can enter a maximum of ten host names.

   - **Host Name (FQDN)**: Enter Fully Qualified Domain Name or IP address of the host. The host name entries override the information provided by DNS.
   - **IP Address**: IP address that the host name is mapped to. A host can be mapped to more than one IP addresses and each of these mappings are a separate entry.
   - **Port**: Port number that the host should use for routing using the particular IP address.
   - **Priority**: If there are multiple IP address entries for a given host, Session Manager tries the administered IP addresses in the order of the priority.
   - **Weight**: If there are multiple IP address entries for a given host, and if some entries have the same priority, then for each priority level, Session Manager picks a host according to the specified weights.
   - **Transport**: The transport protocol that should be used for routing, such as TLS, TCP, or UDP. The default is TLS.
6. Click **Commit** to save the host name entry to the host name table.

   Note:

   - Ensure that at least one entity link has been defined for each FQDN and Transport entries.
   - You can import or export XML Schema instance file, containing LHN entries, using **More Actions** menu on the Local Host Name Resolution page.

Related Links

Local Host Name Resolution page field descriptions on page 433
New Local Host Name Entries page field descriptions on page 434

Viewing import job status

About this task

Using this functionality, you can view the job status of importing Local Host Name Resolution entries since the last restart of System Manager.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** .
3. Click **Network Configuration** > **Local Host Name Resolution**.

Result

In Local Host Name Resolution page, under Background Job Status section, you can view the status of all background import jobs since the last restart of System Manager.

Related Links

Local Host Name Resolution page field descriptions on page 433

Viewing failed job entries

View the list of **Local Host Name Resolution** entries that failed to be imported, along with the reason for the import failure.

Procedure

1. On the System Manager Web Console, under **Elements**, click **Session Manager**.
2. Click **Network Configuration** > **Local Host Name Resolution**.
3. On the Local Host Name Resolution page, under the Background Job Status section, select a failed import job and click **View Failures**.

   The **Local Host Name Entries** page displays the list of Local Host Name Resolution entries that failed to be imported during the selected import job process.
4. Under the Local Host Name Entries section, click **Return to View All Entries** to return to the normal view mode.

Related Links

Local Host Name Resolution page field descriptions on page 433

Stopping import jobs

About this task

Using this functionality, you can terminate current running background import jobs.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** .
3. Click **Network Configuration** > **Local Host Name Resolution**.
4. In Local Host Name Resolution page, under Background Job Status section, select a running import job and click **Stop Job**.

   The running import job terminates.

Related Links

Local Host Name Resolution page field descriptions on page 433

Local Host Name Schema

XML schema provides the format for generation of XML schema instance file in the event of import of Local Host Name data.

Example

The format of the JAXB-compliant XSD schema of the XML files used in the Local Host Name Import and Export feature is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:jxb="http://java.sun.com/xml/ns/jaxb"
            jxb:version="2.0">

<xsd:annotation>
  <xsd:documentation xml:lang="en">
    XML schema definition for 'Local Host Name Resolution' entries.

    Copyright Avaya Inc., All Rights Reserved
    THIS IS UNPUBLISHED PROPRIETARY SOURCE CODE OF AVAYA INC
    The copyright notice above does not evidence any
    actual or intended publication of such source code.
    Some third-party source code components may have been modified from
    their original versions by Avaya Inc.
    The modifications are Copyright Avaya Inc., All Rights Reserved.
  </xsd:documentation>
</xsd:annotation>

<xsd:element name="LocalHostNameEntries" type="LocalHostNameEntryListType"/>

<xsd:complexType name="LocalHostNameEntryListType">
        <xsd:sequence>
                <xsd:element name="LocalHostNameEntry" type="LocalHostNameEntryType"
                                    maxOccurs="unbounded"/>
        </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="LocalHostNameEntryType">
  <xsd:sequence>
    <xsd:element name="hostName" type="hostNameType"/>
    <xsd:element name="ipAddress" type="ipAddressType"/>
    <xsd:element name="port" type="portType"/>
    <xsd:element name="priority" type="priorityType"/>
    <xsd:element name="weight" type="weightType"/>
    <xsd:element name="transport" type="transportType"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:simpleType name="hostNameType">
  <xsd:restriction base="xsd:string">
    <xsd:minLength  value="1"/>
    <xsd:maxLength  value="255"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="ipAddressType">
  <xsd:restriction base="xsd:string">
    <xsd:minLength  value="7"/>
    <xsd:maxLength  value="15"/>
```

```
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="portType">
  <xsd:restriction base="xsd:int">
    <xsd:minInclusive value="0"/>
    <xsd:maxInclusive value="65535"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="priorityType">
  <xsd:restriction base="xsd:int">
    <xsd:minInclusive value="0"/>
    <xsd:maxInclusive value="2147483647"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="weightType">
  <xsd:restriction base="xsd:int">
    <xsd:minInclusive value="0"/>
    <xsd:maxInclusive value="100"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="transportType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="TLS"/>
    <xsd:enumeration value="TCP"/>
    <xsd:enumeration value="UDP"/>
  </xsd:restriction>
</xsd:simpleType>

</xsd:schema>
```

Example

Following is a sample XML Schema :

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<LocalHostNameEntries>
        <LocalHostNameEntry>
                <hostName>www.domain1.com</hostName>
                <ipAddress>192.168.1.100</ipAddress>
                <port>1024</port>
                <priority>900</priority>
                <weight>50</weight>
                <transport>TLS</transport>
        </LocalHostNameEntry>
        <LocalHostNameEntry>
                <hostName>www.domain2.com</hostName>
                <ipAddress>192.168.1.101</ipAddress>
                <port>1024</port>
                <priority>600</priority>
                <weight>25</weight>
                <transport>TCP</transport>
        </LocalHostNameEntry>
</LocalHostNameEntries>
```

Local Host Name Resolution page field descriptions

Local Host Name Entries

Button	Description
New	Opens the New Local Host Name Entries page using which you can add new local hosts
Edit	Opens the Edit Local Host Name Entries page using which you can modify the selected local hosts
Delete	Opens the Delete Local Host Name Entries Confirmation page using which you can confirm or cancel the deletion of the selected local hosts
More Actions > **Import Local Host Name Entries**	Opens Import Local Host Name Entries page where you can select for importing or uploading an XML Schema instance file containing a list of LHN entries for adding to the LHN resolution table.
More Actions > **Export Local Host Name Entries**	Use this field to Export (download) an XML Schema instance file containing a list of LHN entries currently in the LHN resolution table.
More Actions > **Get Local Host Name Schema**	Use this field to get/retrieve the XML Schema for the current version of the Session Manager release. This enables you to understand the XML schema format for a creating new XML schema instance file for import purpose.

Name	Description
Host Name (FQDN)	Enter Fully Qualified Domain Name or IP address of the host. The host name entries override the information provided by DNS.
IP Address	Shows the IP address that the host name is mapped to. A host can be mapped to more than one IP addresses and each of these mappings are a separate entry.
Port	Shows the port number that the host should use for routing using the particular IP address.
Priority	If there are multiple IP address entries for a given host, Session Manager tries the administered IP addresses in the order of the priority.
Weight	If there are multiple IP address entries for a given host, and if some entries have the same priority, then for each priority level, Session Manager picks a host according to the specified weights.
Transport	Shows the transport protocol that should be used for routing, such as TLS, TCP, or UDP. The default protocol is TLS.

Background Job Status

Button	Description
View Failures	Use this field to view the failed Local Host Name Resolution entries for the selected failed import job.
Stop Job	Use this field to stop the selected background running import job.

Name	Description
Start Time	Time since the import job process was started.
Status	Status information about the state of the import job.
Percent Completed	Percentage of completion of the import job process.
Total Entries to Process	Total number of Local Host Name Resolution entries to be imported during the import job process.
Failed Entries	Number of Local Host Name Resolution entries that failed to be imported during the import job process.
Last Updated	Time of last import job process.
Job Name	Details of the import job.

Related Links

Resolving local host name on page 429
Viewing import job status on page 429
Viewing failed job entries on page 430
Stopping import jobs on page 430

New Local Host Name Entries page field descriptions

Name	Description
Host Name (FQDN)	Enter Fully Qualified Domain Name or IP address of the host. The host name entries override the information provided by DNS. You can add a maximum of ten entries on a page.
IP address	IP address that the host name is mapped to.
Port	Port number that the host should use for routing using the particular IP address.
Priority	If there are multiple IP address entries for a given host, Session Manager tries the administered IP addresses in the order of the priority.
Weight	If there are multiple IP address entries for a given host, and if some entries have the same priority, then for each priority level, Session Manager picks a host according to the specified weights.

Table continues…

Name	Description
Transport	The transport protocol that should be used for routing, such as TLS, TCP, or UDP. The default protocol is TLS

Button	Description
Cancel	Cancels the addition of the new host name entry to the local host name table.
Commit	Saves the addition of the new host name entry to the local host name table.

Related Links

Resolving local host name on page 429

Edit Local Host Name Entries page field descriptions

Name	Description
Host Name (FQDN)	Enter Fully Qualified Domain Name or IP address of the host. The host name entries override the information provided by DNS.
IP address	IP address that the host name is mapped to. A host can be mapped to more than one IP addresses and each of these mappings are a separate entry.
Port	Port number that the host should use for routing using the particular IP address.
Priority	If there are multiple IP address entries for a given host, Session Manager tries the administered IP addresses in the order of the priority.
Weight	If there are multiple IP address entries for a given host, and if some entries have the same priority, then for each priority level, Session Manager picks a host according to the specified weights.
Transport	The transport protocol that should be used for routing, such as TLS, TCP, or UDP. The default protocol is TLS.

Button	Description
Cancel	Cancels the modification of the host name entry.
Commit	Saves the modified host name entry to the local host name table.

Delete Local Host Name Entries Confirmation page field descriptions

Button	Description
Cancel	Cancels the deletion of the selected local host name from the local host name entries table.
Delete	Deletes the selected local host name from the local host name entries table.

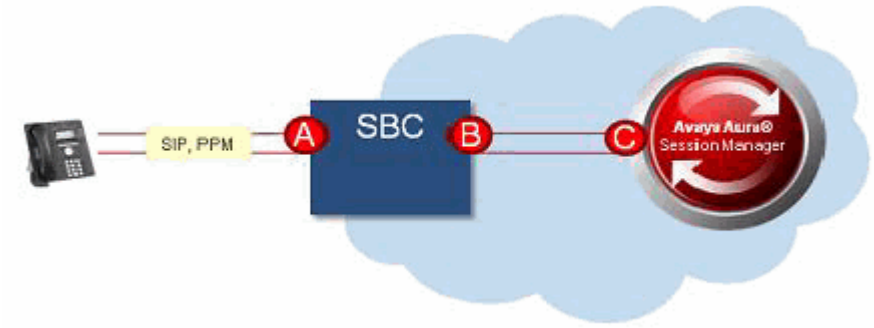
Remote Access

About Remote Access

Enterprises or Hosted Communication Solution Providers can use the Session Manager Remote Access feature to provide fully functional Avaya communication services to a remote user over the public Internet without VPN connectivity.

Reference configuration

A remote endpoint can access Session Manager deployed in the enterprise network using a Session Border Controller (SBC). Remote users can connect over the Internet to the public interface of the SBC, which is at the edge of the enterprise network.



- Reference point A indicates the external, public facing IP address on the SBC.
- Reference point B indicates the internal facing IP address and port on the SBC.
- Reference point C indicates the IP address of Session Manager.

For the list of supported endpoints, see *Avaya Aura® Session Manager Overview and Specification*.

Creating a Remote Access configuration

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **Remote Access**.

   The system displays the Remote Access page.
3. Click **New**.

The system displays the Remote Access Configuration page.

4. To add a new SIP Proxy mapping with Session Manager, in the **SIP Proxy Mapping** table, click **New** and enter the required information.
5. To add a new SIP Proxy Private IP address, in the **SIP Proxy Private IP Addresses** table, click **New** and enter the required information.
6. Click **Add**.

Related Links

Remote Access page field descriptions on page 440
Remote Access Configuration page field descriptions on page 440

Modifying a Remote Access configuration

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **Remote Access**.

   The system displays the Remote Access page.
3. Select the Remote Access configuration to be modified and click **Edit**.

   You can edit only one Remote Access configuration at one time.
4. Modify the required fields on the Remote Access Configuration page.
5. Click **Commit**.

Related Links

Remote Access page field descriptions on page 440

Deleting Remote Access configurations

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **Remote Access** .

   The system displays the Remote Access page.
3. Select the checkboxes for the Remote Access configurations that you want to remove, and click **Delete**.

   You can also delete more than one Remote Access Configurations simultaneously.
4. On the Delete Confirmation page, click **Delete**.

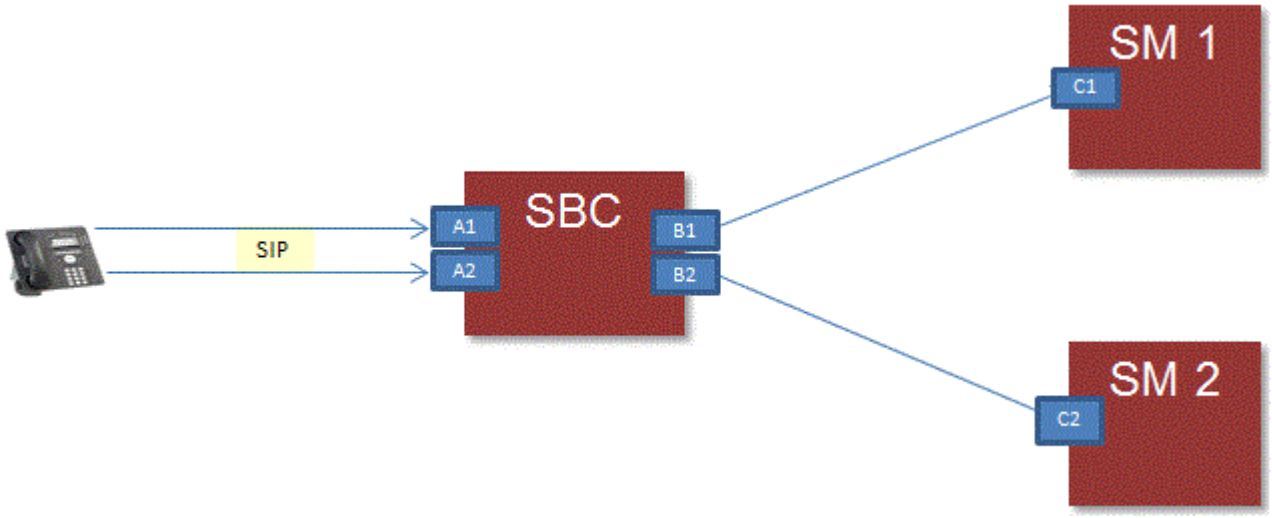
Related Links

Remote Access page field descriptions on page 440

Configuring SIP core redundancy

About this task

You can configure Remote Worker solution with multiple core Session Manager instances for added redundancy and resiliency of the Session Manager connection from the endpoint device.



For configuring the core redundancy solution,

1. configure multiple external facing interfaces, such as *reference point A1* and *reference point A2*, for each SBC.
2. associate the *reference point A1, A2* with distinct Session Manager instances (SM1 and SM2 with *reference point C1 and C2* respectively) in order to enable the registered endpoints to failover in the case of a loss of connection to Session Manager.
3. configure the SIP Private Address (*reference point B1* and *reference point B2*) for the SBC.

The remote endpoint simultaneously registers with:

- core Session Manager (SM1) through *reference point A1*
- core Session Manager (SM2) through *reference point A2*

The SBC in the Remote Worker configuration proxies addresses in both directions. Session Manager interprets all communication, from remote endpoints that traverse the SBC, as having an SBC address (*reference point B1 or B2*). The remote endpoints interpret Session Manager as having the public address of the SBC (*reference point A1 or A2*).

Where,

- SIP Proxy Public Address (*reference point A*) is the Public IP address of the enterprise SBC.
- Session Manager (*reference point C*) is the IP address of the selected Session Manager instance.
- SIP Private Address (*reference point B*) is the Private IP address of the enterprise SBC.

When SM1 fails or connection to SM1 is lost, the registered SM2 instance can serve the registered endpoints.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **Remote Access**.

   The system displays the Remote Access page.
3. Click **New**.

   The system displays the Remote Access Configuration page.
4. Enter the value of SIP Proxy Private IP Address as *reference point B1* and *reference point B2*.
5. To add a new SIP Proxy mapping with Session Manager, in the SIP Proxy Mapping table, click **New** and enter the required information.

   This creates a new row in the SIP Proxy Mapping table where the Reference point A (A1) and Reference point C (C1) are mapped.

   Similarly add a second set of addresses if needed to support dual registration. This creates a new row in the SIP Proxy Mapping table where the Reference point A (A2) and reference point C (C2) are mapped. Both SIP Proxy Public IP addresses must be in the phone settings file.
6. To add a new SIP Proxy Private IP address, in the SIP Proxy Private IP Addresses table, click **New** and enter the required information.
7. Click **Commit**.

   This creates a new row in the SIP Proxy Private IP Addresses table for the Reference point B.

Verifying user registration details

About this task

Use the User Registrations module to view the basic registration information for the remote user.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open User Registrations page.

   The User Registrations page displays the list of registered users.
3. Verify the user registration status under the **Remote Office** column of the User Registrations page.
4. Click **Refresh** to retrieve the latest user registration summary results.

Remote Access page field descriptions

Button	Description
New	Opens the Remote Access Configuration page that you can use to add a new Remote Access configuration.
Edit	Opens the Remote Access Configuration page that you can use to modify an existing Remote Access configuration.
Delete	Opens the Delete Confirmation page that you can use to confirm or cancel the deletion of selected Remote Access configuration.

Name	Description
Remote Access Configuration Name	The name of the administered Remote Access configuration.

Related Links

[Creating a Remote Access configuration](#) on page 436
[Modifying a Remote Access configuration](#) on page 437
[Deleting Remote Access configurations](#) on page 437

Remote Access Configuration page field descriptions

Name	Description
Name	The name of the Remote Access configuration.
Note	Details on the Remote Access configuration.

Remote Access Reference Map

Shows the reference configuration of the remote access solution. For details, see the introduction of the *Remote Access* section.

SIP Proxy Mapping Table

Button	Description
New	Adds a new row in the SIP Proxy Mapping table.
Delete	Deletes the selected row in the SIP Proxy Mapping table.

Name	Description
SIP Proxy Public Address (Reference A)	The Public IP address of the enterprise SBC.
Session Manager (Reference C)	The selected Session Manager instance.

SIP Proxy Private IP Addresses

Button	Description
New	Adds a new row in the SIP Proxy Private IP Addresses table.
Delete	Deletes the selected row in the SIP Proxy Private IP Addresses table.

Name	Description
SIP Private Address (Reference B)	The Private IP address of the enterprise SBC.
SBC Type	The type of SBC used in the Remote Access configuration.
Note	Details about the SIP Proxy Private IP address.

Button	Description
Add	Adds the Remote Access configuration.
Cancel	Cancels the addition of the Remote Access configuration.

Related Links

Creating a Remote Access configuration on page 436

SIP Firewall

About SIP Firewall

SIP Firewall controls the SIP traffic entry into the Session Manager server. SIP Firewall allows or drops SIP messages based on the sender, location, and other criteria defined in Rule Sets.

SIP Firewall configuration consists of a collection of Rule Sets. You can assign these SIP Firewall Rule Sets to Session Manager and Branch Session Manager instances in the network.

SIP Firewall default Rule Set

Installation of Session Manager automatically provides a default SIP Firewall Rule Set for the SIP Firewall. The system preserves the default Rule Sets for different Session Manager releases. You can rollback to an earlier release of Avaya provided Rule Set by assigning prior Rule Set versions.

Session Manager and Branch Session Manager systems, with customer created Rule Sets assigned, remain unaffected after a system upgrade.

After a system upgrade, the default Rule Sets associated with the Session Managers and Branch Session Managers get automatically updated with the latest versions of Rule Sets.

SIP Firewall Rule Set

Rules:

SIP Firewall rules can generate log events, which are monitored by the serviceability agents. You must always enable logging in each SIP Firewall rule to have a record of the actions taken by the SIP Firewall.

Note:

SIP Firewall log messages are rate-limited. Each rule can log a maximum of one log message per second. Rate-limiting of log messages provides protection from flooding of the logging system that might occur because of bad configuration of SIP Firewall rules.

You can apply SIP filtering and DoS protection to:

- SIP gateway or proxy connections (SIP Multiplexed connection or trunk). For example, a SIP Firewall rule can set a rate limit on the number of INVITE messages from a specific user, without affecting the traffic from other users in that gateway.
- SIP TLS connection. Session Manager Security Module decrypts all the incoming SIP TLS packets before any filtering rules are applied by the SIP Firewall.

For more information about the default SIP Firewall rules, see *Avaya Aura® Session Manager Security Design*.

Blacklist:

SIP Blacklist blocks any known bad SIP elements. The SIP Firewall drops any SIP packet that matches a rule in the Blacklist.

Whitelist:

SIP Whitelist allows only known good SIP elements. SIP Firewall allows any SIP packets that matches a rule in the Whitelist and does not apply any other filtering rules.

Rule precedence and traversal

The precedence order for using the rules is:

1. Blacklist
2. Whitelist
3. Rules

Each list can contain more than one rule. Session Manager traverses the rules from top to bottom, within any of the previous lists.

SIP Firewall is a packet-based filtering engine. Any time a packet matches a rule, SIP Firewall stops the rule traversal and either permits or drops the packet, according to the rule action. This process does not apply to rules defined with a *None* action type.

Deep inspection filtering

SIP Firewall rules provide the following filters for deep inspection:

- SIP Layer content
- IP and Transport layer parameters such as IP address, protocol, and port.

You can combine both SIP Layer content and IP transport layer parameters in a single Firewall rule. For example, a SIP Firewall rule can limit the high rate of INVITE packets coming from a remote IP address.

Denial of Service protection

SIP Firewall provides protection from the Denial of Service (DoS) attacks as follows:

- Flood Protection from a specified source.
- Advanced Flood Protection: You can define a rule to detect or mitigate flood attacks within the live SIP stream, without knowing the flood source in advance. You need not know the host causing the flood when the configuring a rule. A high performance database tracks all matching messages.
- Rate-Limiting: You can configure a *Rate Limit* action to limit the number of SIP packets that are forwarded within a specified period. For more information about how to configure Rate Limit rules, see the topic Creating a new SIP Firewall rule.
- Rate-Blocking: You can configure a *Rate Block* action to block an offending SIP source when the traffic reaches a specified threshold within a given period. Traffic is then blocked until the configured timeout expires. For more information on how to configure the Rate Block rules, see the topic Specifying a new SIP Firewall rule.
- Signature Detection: You can configure a rule to perform signature detection and drop packets matching the signature. The rule can support both simple and regular-expression type string searching across the entire SIP header region of the message or across the full message (headers and body).

SIP Firewall status

Use this function to view the status of SIP Firewalls for each Session Manager and Branch Session Manager instances deployed across the network. Additionally, you can also perform the following functionality:

- View the assignment details of specific rule sets for each Session Manager and Branch Session Manager instance.
- View the SIP Firewall processing status for each Session Manager and Branch Session Manager instance.
- Perform sanity audit of the Session Manager Rule Set assignments.
- Reset the processing counters of the selected Session Manager and Branch Session Manager instances.

Related Links

Security Module Status page field descriptions on page 510

Creating a new Rule Set

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **SIP Firewall** to open the SIP Firewall Configuration page.

3. Click **New** to open the Rule Set page.
4. Enter the name and description of the new Rule Set.

   On Rules tab, perform the following Rule-based operations:
5. To enable or disable all the rules, select or clear the **Enabled** check box.
6. To create a new rule, click **New**.

   You can define up to 50 rules.

   For details, see the topic *Creating a new SIP Firewall rule*.
7. To modify a rule, select the respective check box and click **Edit**.
8. To delete a rule, select a rule and click **Delete**.
9. Select a rule from the list, and click **Up** or **Down** to move the rule and change the order.

   On Blacklist tab, perform the following Blacklist-based operations:
10. Select **Enabled** to drop messages from untrusted hosts.
11. Click **New** to create a new rule to drop messages from untrusted hosts.
    a. In the **Key** field, click a key for filtering messages for blacklisting from Remote IP address, CONTACT, and FROM.
    b. In the **Value** field, enter a value of the Key.

       Specify the following values:

       - Remote IP address: IP address of the host sending the messages.
       - CONTACT: String for searching in the *Contact* SIP Header in the SIP message. This string need not be an exact match with the *Contact* SIP header content and can be a subset of the *Contact* SIP Header. The value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.
       - FROM: String for searching in the *From* SIP Header in the SIP message. This string need not be an exact match with the *From* SIP header content and can be a subset of the *From* SIP Header. The value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.

    c. In the **Mask** field, specify the Subnet mask only when you have used the Remote IP address in the Key.

       You can use this field to blacklist an entire IP subnet.

    You can create up to 200 blacklist rules.
12. Click **Delete** to delete a selected blacklist rule.

    On Whitelist tab, perform the following whitelist-based operations:
13. Select **Enabled** to allow messages from trusted hosts to bypass the SIP firewall.

14. Click **New** to create a new rule to allow messages from trusted hosts.
    a. In the **Key** field, click a key for filtering messages for whitelisting from Remote IP address, CONTACT, and FROM.
    b. In the **Value** field, enter a value of the Key.

       Specify the following values.

       - Remote IP address: IP address of the host sending the messages.
       - CONTACT: String for searching in the *Contact* SIP Header in the SIP message. This string need not be an exact match with the *Contact* SIP header content and can be a subset of the string present in the *Contact* SIP Header. The value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.
       - FROM: String for searching in the *From* SIP Header in the SIP message. This string need not be an exact match with the *From* SIP header content and can be a subset of the string present in the *From* SIP Header. The value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.

    c. In the **Mask** field, specify the subnet mask only when you have used the Remote IP address in the Key.

       You can use this field to whitelist an entire IP subnet.
15. Click **Delete** to delete a selected whitelist rule.

Related Links

SIP Firewall Configuration page field descriptions on page 450

Creating a new SIP Firewall rule

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **SIP Firewall** to open the SIP Firewall Configuration page.
3. Click **New** to open the Rule Set page.
4. On the Rule Set page, under the **Rules** tab, click **New**.
5. Enter the appropriate information in the **Rule** page.

   See the *Rule page field descriptions* for details.
6. Click **Commit** to save the rule or **Cancel** to cancel the changes.

   This operation does not save the SIP Firewall configuration to Session Manager. To save the configuration to Session Manager after creating or editing the configuration, return to the **Rule Set** page and click **Commit**.

Related Links

Rule page field descriptions on page 454

Creating a duplicate Rule Set

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **SIP Firewall** to open the SIP Firewall Configuration page.
3. From the list, select a Rule Set for creating a duplicate Rule Set.
4. Click **Duplicate** to open the Rule Set page.
5. Enter a name and description for the duplicate Rule Set.
6. On the Rule Set page, modify the appropriate information of the duplicate Rule Set.

   For more information, see *Creating a new Rule Set*.
7. Click **Commit**.

Related Links

SIP Firewall Configuration page field descriptions on page 450

Modifying a Rule Set

About this task

You cannot modify a default Rule Set. After you modify a Rule Set, the system updates the associated Session Manager and Branch Session Manager instances with the changes.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **SIP Firewall** to open the SIP Firewall Configuration page.
3. From the list, select a Rule Set for modification.
4. Click **Edit** to open the Rule Set page.
5. On the Rule Set page, modify the appropriate information of the duplicate Rule Set.

   For more information, see *Creating a new Rule Set*.
6. Click **Commit**.

Related Links

SIP Firewall Configuration page field descriptions on page 450

Viewing a Rule Set

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **SIP Firewall** to open the SIP Firewall Configuration page.

3. From the list, select a Rule Set for viewing.
4. Click **View** to open the Rule Set page.
5. Click **Commit**.

Related Links

SIP Firewall Configuration page field descriptions on page 450

Deleting a Rule Set

About this task

You cannot delete a default Rule Set or a previously assigned Rule Set. To delete a previously assigned Rule Set, you must reassign all the associated Session Manager and Branch Session Manager instances to another Rule Set.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **SIP Firewall** to open the SIP Firewall Configuration page.
3. From the list, select a Rule Set for deletion.
4. Click **Delete** to delete the selected Rule Set.

Related Links

SIP Firewall Configuration page field descriptions on page 450

Assigning Rule Sets to all core Session Managers

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **SIP Firewall** to open the SIP Firewall Configuration page.
3. From the list, select a Rule Set for assigning to all core Session Managers.
4. Click **Assign** > **Assign All Core SMs**.
5. In the Confirm Rule Set Assignment page, click **Confirm**.

Related Links

SIP Firewall Configuration page field descriptions on page 450

Assigning Rule Sets to all Branch Session Managers

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **SIP Firewall** to open the SIP Firewall Configuration page.
3. From the list, select a Rule Set for assigning to all Branch Session Managers.

4. Click **Assign** > **Assign All BSMs**.
5. In the Confirm Rule Set Assignment page, click **Confirm**.

Related Links

SIP Firewall Configuration page field descriptions on page 450

Assigning Rule Sets to all core Session Managers and Branch Session Managers

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **SIP Firewall** to open the SIP Firewall Configuration page.
3. From the list, select a Rule Set for assigning to all core Session Managers and Branch Session Managers.
4. Click **Assign** > **Assign All (Core SMs and BSMs)**.
5. In the Confirm Rule Set Assignment page, click **Confirm**.

Related Links

SIP Firewall Configuration page field descriptions on page 450

Selecting Session Managers and Branch Session Managers for Rule Set assignment

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **SIP Firewall** to open the SIP Firewall Configuration page.
3. From the list, select a Rule Set to be assigned to selected Session Managers and Branch Session Managers.
4. Click **Assign** > **Select SMs and BSMs** for assignment.
5. In the Assign Rule Set page, select the Session Managers and Branch Session Managers.
6. Click **Commit**.

Related Links

SIP Firewall Configuration page field descriptions on page 450

Viewing assigned Session Managers and Branch Session Managers

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **SIP Firewall** to open the SIP Firewall Configuration page.

3. From the list, select a Rule Set.
4. Click **Assign** > **View Assigned SMs and BSMs**.

   View Rule Set Assignment page shows the list of Session Managers and Branch Session Managers, which are assigned to the selected Rule Set.
5. Click **Done**.

Note:

In the SIP Firewall Configuration page, you can also click a Rule Set to view the list of assigned Session Managers and Branch Session Managers.

Related Links

SIP Firewall Configuration page field descriptions on page 450

Viewing SIP Firewall status

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **SIP Firewall** to open the SIP Firewall Configuration page.
3. Click **Status** to open the SIP Firewall Status page.

Result

The SIP Firewall Status page shows the SIP Firewall processing status for each Session Manager and Branch Session Manager instance.

Related Links

SIP Firewall Configuration page field descriptions on page 450
SIP Firewall Status page field descriptions on page 458

Auditing Firewall configuration

About this task

You can perform periodic audit of Firewall configuration to ensure the functioning state of the SIP Firewall. The audit operation checks for Rule Set upgrades and imports the latest default Rule Sets. The system also performs the audit operation automatically at every 5 minutes.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Network Configuration** > **SIP Firewall** to open the SIP Firewall Configuration page.
3. Click **Status** to open the SIP Firewall Status page.
4. Click **Audit** to open the Rule Set Audit and Repair Results page.
5. Click **Done**.

Result

Rule Set Audit and Repair Results page shows the details of the SIP Firewall configuration state for all Session Manager and Branch Session Manager instances.

SIP Firewall Configuration page field descriptions

Button	Description
New	Opens the Rule Set page. Use this page to create a new SIP Firewall Rule Set.
Duplicate	Opens the Rule Set page. Use this page to duplicate a selected SIP Firewall Rule Set to a new Rule Set.
Edit	Opens the Rule Set page. Use this page to edit a selected SIP Firewall Rule Set.
View	Opens the Rule Set page. Use this page to view a selected SIP Firewall Rule Set.
Assign (All Core SMs and BSMs)	Opens the Confirm Rule Set Assignment page. Use this page to assign a SIP Firewall Rule Set to all core Session Managers and Branch Session Managers.
Assign All Core SMs	Opens the Confirm Rule Set Assignment page. Use this page to assign a SIP Firewall Rule Set to all core Session Managers.
Assign All BSMs	Opens the Confirm Rule Set Assignment page. Use this page to assign a SIP Firewall Rule Set to all Branch Session Managers.
Select SMs and BSMs for assignment	Opens the Assign Rule Set page. Use this page to assign a SIP Firewall Rule Set to selected Session Managers and Branch Session Managers.
View Assigned SMs and BSMs	Opens the View Rule Set Assignment page. View Rule Set Assignment page displays a list of Session Managers and Branch Session Managers assigned with a selected Rule Set.
Delete	Opens the Confirm Delete of SIP Firewall Rule Set(s) page. Use this page to delete a selected Rule Set.
Import	Opens the Import SIP Firewall Rule Set page. Use this page to import SIP Firewall XML file.
Export	Enables downloading of SIP Firewall XML file for the selected Rule Set.
Status	Opens the SIP Firewall Status page. SIP Firewall Status page displays SIP Firewall status for Session Managers and Branch Session Managers.

Name	Description
Rule Set	The name of the Rule Set.

Table continues…

Name	Description
Assigned Count	The number of Session Managers and Branch Session Managers assigned to a Rule Set.
Avaya Provided	*Yes* or *Default* indicates a Rule Set provided by Avaya. *No* indicates a customer defined Rule Set. On system upgrade, Default Rule Sets are automatically updated.
Description	The Rule Set description.

Related Links

Creating a new Rule Set on page 443
Creating a duplicate Rule Set on page 446
Modifying a Rule Set on page 446
Viewing a Rule Set on page 446
Assigning Rule Sets to all Branch Session Managers on page 447
Assigning Rule Sets to all core Session Managers on page 447
Assigning Rule Sets to all core Session Managers and Branch Session Managers on page 448
Selecting Session Managers and Branch Session Managers for Rule Set assignment on page 448
Viewing assigned Session Managers and Branch Session Managers on page 448
Deleting a Rule Set on page 447
Viewing SIP Firewall status on page 449

Rule Set page field descriptions

Button	Description
Commit	Saves the Rule Set changes.
Cancel	Cancels the Rule Set changes.

Name	Description
Name	The name of the Rule Set.
Description	The description of the Rule Set.

Rules tab

Button	Description
Enabled	Enables or disables all rules in the Firewall Rule Set.
New	Opens the Rules page that enables you to define a new SIP Firewall rule.
Edit	Opens the Rules page that enables you to edit the selected SIP Firewall rule.
Delete	Deletes the selected rule or rules.

Table continues…

Button	Description
Up	Moves a selected rule up in the list.
Down	Moves a selected rule down in the list.

Name	Description
Enabled	Enables or disables the rule.
Name	The name of the SIP Firewall rule. The name can have a maximum of 80 characters.
Action Type	Specifies the following action types for the rule: • None: No specific action required. This action can be used when you want to only generate a log or alarm for matching SIP traffic. Rule traversal continues when a SIP packet matches a rule with the None action. • Permit: If the rule conditions are fulfilled, allow the SIP message to pass through the SIP Firewall. If the rule conditions are not fulfilled, the SIP message is not affected or dropped. • Drop: If the rule conditions are fulfilled, drop the SIP message. • Rate Block: If the packets matching the rule exceed a certain count in a certain period, block the matching SIP packets for the duration of timeout (as defined by the Threshold parameters). • Rate Limit: If the packets matching the rule exceed a certain count in a certain period, drop the additional matching SIP packets for the duration of full period (as defined by the Threshold parameters).
Log Type	Specifies if a log is to be generated or not, and if an alarm should be sent.
Log Message	The message to be logged when the **Log Type** is **Yes** or **Alarm**.

Blacklist tab

Button	Description
New	Creates a rule for dropping messages from untrusted hosts.
Delete	Deletes the selected Blacklist rule.

Name	Description
Enabled	Enables or disables the dropping of messages from untrusted hosts.
Key	Key for filtering messages for blacklisting.
Value	The value of the Key. • Remote IP address: IP address of the host from where the messages are sent. • CONTACT: String to search in the *Contact* SIP Header in the SIP message. This string need not be an exact match with the *Contact* SIP header content and can be a subset of the string present in the *Contact* SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users. • FROM: String to search in the *From* SIP Header in the SIP message. This string need not be an exact match with the *From* SIP header content and can be a subset of the string present in the *From* SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.
Mask	Subnet mask used for the blacklist operation.

Whitelist tab

Button	Description
New	Creates a rule for allowing messages from trusted hosts to bypass the SIP Firewall.
Delete	Deletes the selected Whitelist rule.

Name	Description
Enabled	Enables or disables the allowing of messages from trusted hosts to bypass the SIP Firewall.
Key	Key for filtering messages for whitelisting.
Value	Value of the Key. • Remote IP address: IP address of the host from where the messages are sent. • CONTACT: String to search in the *Contact* SIP Header in the SIP message. This string need not be an exact match with the *Contact* SIP header content and can be a subset of the string present in the *Contact* SIP Header. Its value can be a complete or partial SIP URI, for example,

Table continues…

Name	Description
	jdoe@avaya.com for a specific user, or @avaya.com for a domain of users. • FROM: String to search in the *From* SIP Header in the SIP message. This string need not be an exact match with the *From* SIP header content and can be a subset of the string present in the *From* SIP Header. Its value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.
Mask	Subnet mask used for the whitelist operation.

Rule page field descriptions

General:

Name	Description
Enabled	Enables or disables the rule.
Name	The name of the SIP Firewall rule. The name can have a maximum of 80 characters.
Action Type	Specify one of the following action types for the rule: • None: No specific action required. This action can be used when you want to only generate a log or alarm for matching SIP traffic. Rule traversal continues when a SIP packet matches a rule with the None action. • Permit: If the rule conditions are fulfilled, allow the SIP message to pass through the SIP Firewall. If the rule conditions are not fulfilled, the SIP message is not affected or dropped. • Drop: If the rule conditions are fulfilled, drop the SIP message • Rate Block: If the packets matching the rule exceed a certain count in a certain period, block the matching SIP packets for the duration of timeout (as defined by the Threshold parameters). • Rate Limit: If the packets matching the rule exceed a certain count in a certain period, drop the additional matching SIP packets for the duration of full period (as defined by the Threshold parameters).

Table continues…

Name	Description
Log Type	Specifies if a log is to be generated or not, and if an alarm should be sent. You must specify Log Type when the Action Type is None. • No: Do not save the rule to a log file • Yes: Save the rule to a log file • Alarm: If it is possible, generate an alarm when the rule conditions are met
Log Message	The message to be logged when the **Log Type** is **Yes** or **Alarm**.

IP Layer Match Options:

Name	Description
Protocol	Select the protocol for which the rule is to be used.
Remote IP Address	For any incoming SIP message, select **Any** for using the rule for all IP addresses, or select **Specify** to use the rule for a specific IP address.
IP Address	Type the IP address if you selected **Specify** for Remote IP Address.
Mask	Network Mask for the specified IP address
RemotePort	Select **Any**, **Specify**, or **Specify Range** to enter a single port or a range of ports
Start	Select a port number for the **Specify** option. Specify the port number for the **Specify Range** option to start the range.
End	Specify the port number for the Specify Range option to end the range.
Local Port	Select **Any**, **Specify**, or **Specify Range** to enter a single port or a range of ports.
Start	Select a port number for the **Specify** option. Specify the port number for the **Specify Range** option to start the range.
End	Specify the port number for the **Specify Range** option to end the range. The range includes both the Start and End port numbers specified.

SIP Layer Match Options:

Button	Description
New	Create up to five SIP layer match options
Delete	Delete the selected SIP layer match options

Name	Description
KeyType	Select the key type that the rule should match from the list. You can add up to five key type match options. If more than one match options are defined, then logical AND of the options is used to create a search pattern. • All SIP Headers: This option searches for the Value within all the SIP headers for the SIP packet. • All SIP Headers/Body: This option searches for the Value in the SIP headers and body portions for the SIP packet. • REQUEST-METHOD, RESPONSE-CODE: All the remaining entries in the Key Type list are SIP headers. This option searches for the value within the specified SIP header only.
ValueType	Specify whether the key type is a string or a regular expression. You can create regular expressions using the PERL version 5.8 syntax.
Value	Value of the selected key type. This string need not be an exact match and can be a subset of the string present in the SIP header being used for search.

IP/SIP LayerTrack:

Name	Description
Track	Select an option for tracking SIP messages only if you have selected either Rate Block or Rate Limit in the Action Type field or with None in the Action Type with Log Type enabled. You cannot use IP/SIP Layer Track with Permit/Drop Actions. This option provides advanced flood tracking in the SIP Firewall. • None: No tracking required • Remote IP address: Tracks messages for a specific IP address of the remote host. • Local Port: Tracks messages for a specific local port • From: Sender of the message • To: Receiver of the message • Contact: Tracks messages for a specific contact. • Request URI: URI of the called party

Threshold:

Name	Description
Count (packets)	Threshold for matching packets. The value can range from 3 to 100000. The default value is 20. Specify this value only for the Rate Block and Rate Limit Action Types.
Period (secs)	Threshold for period for matching packets. The value can range from 1 to 86400. The default value is 20. Specify this value only for the Rate Block and Rate Limit Action Types.
Timeout (secs)	Action timeout in seconds. The value can range from 30 to 36000. The default value is 900. Specify this value only for the Rate Block Action Type.

Connection:

Name	Description
Connection Type	The possible connection types are: • Any : This is a default option. If you retain this option , Session Manager matches the SIP Firewall rule against all incoming SIP Traffic • SIP UA Connection: If this option is selected, Session Manager matches the SIP Firewall rule against the incoming SIP traffic from entities that are not the Trusted SIP Entity, as defined by the Routing Policy. This option is suitable for creating SIP Firewall filtering rules for SIP telephones that are directly connected to Session Manager. • NRP SIP Entity: If this option is selected, Session Manager matches the SIP Firewall rule against the incoming SIP traffic from SIP entities. • NRP Trusted SIP Entity: If this option is selected, Session Manager matches the SIP Firewall rule against the incoming SIP traffic from entities that are marked as Trusted SIP Entity in the Routing Policy. • NRP Untrusted SIP Entity: This option is for entities such as a Session Border Controller (SBC). You can set a firewall rule to monitor traffic coming through an SBC which might have higher thresholds than SIP UA connections.

Button	Description
Cancel	Cancels the defining of the rule
Commit	Saves the defined rule when the SIP firewall configuration is saved

Related Links

Creating a new SIP Firewall rule on page 445

SIP Firewall Status page field descriptions

Button	Description
Reset	Resets all the processing counters of selected Session Managers and Branch Session Managers to zero, except for *Loop Detection* counters. Also, resets all the Rule matching counts to zero. **Note:** After a reset operation, the system updates the counts from the last reset time.
Audit	Performs sanity audit of the Session Manager Rule Set assignments. The Audit process also checks for Rule Set upgrades and imports pending default Rule Sets.
Configure	Navigates to the *SIP Firewall Configuration* page.

Name	Description
Details	Displays the detailed SIP Firewall processing status, for each Rule, of the selected Session Manager. *Rule Matching table* Name: Description Rule: The name of the Rule. Match: For the selected Session Manager, shows the matched count of the Rule. Drop: For the selected Session Manager, shows the dropped count of the Rule.
SM	The name of the Session Manager.
Type	Specifies the Session Manager type.
Rule Sets	The name of the Rule Set assigned to Session Manager.
Reset Time	The last reset time of the SIP Firewall processing counts. **Note:** Only Session Manager and Branch Session Manager of release 6.3.4 and later shows the reset time.

Table continues…

Name	Description
Processing Counts	Shows the summary of counts for Rules, Whitelist, Blacklist, and Loop Detection. Loop Detection counts do not reset. To view the exact counts, hover your mouse over the **Processing Counts** column. **Note:** Only Session Manager and Branch Session Manager of release 6.3.4 and later show the processing counts.

Related Links

Viewing SIP Firewall status on page 449

Device and Location Configuration

Device Settings Groups

Device Settings Groups

Using Device Settings Groups, you can manage some of the configuration data for Avaya terminals. These device settings are associated in groups or in a default group and can be assigned to one or more terminals or locations. Device Settings Groups of type Location Groups can be associated with Locations while Device Settings Groups of type Terminal Groups can only be associated with a terminal respectively having a Terminal Group ID. When the terminal is set up for the first time, the terminal is set up with a pre-provisioned group called Default Group, which provides the global settings across locations and terminals.

A terminal can be individually associated with a set of Device Settings that are downloaded and set as per the following criteria:

- The configuration of a terminal is set as *Default Device Settings* if the terminal:
  - does not belong to an *Routing Policy Location*
  - does not belong to the *Network Routing Policy Location* , where the terminal is located has no specific set of Personal Profile Manager (PPM) attributes
  - is not associated with a specific set of Personal Profile Manager (PPM) attributes
- The configuration of a terminal is set as the set of attributes defined for a *Routing Policy Location* , if the terminal
  - is located in that *Routing Policy Location*
  - is not individually associated with a specific set of PPM attributes

- The configuration of a terminal is set as a specific set of PPM attributes, if the terminal
  - is individually associated with a set of PPM attributes
  - the selected set of PPM attributes does still exist

Priority ordering of usage of the Device Settings data is as follows:

- Terminal group data – highest priority; used if a terminal group is configured in the endpoints
- Location based settings. Have priority over default settings
- Default service settings

PPM supports device settings on a per location basis. Session Manager notifies an endpoint when Device Settings are modified. This includes the following:

- Timers: Registration, Subscription
- QoS parameters: for Video, Audio and call control
- VLAN ID

Viewing Device Settings Groups

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Device and Location Configuration** > **Device Settings Groups** to open Device Settings Groups page. The Device Settings Groups page displays the list of Device Settings Groups.

Related Links

Device Settings Groups field descriptions on page 463

Creating a Device Settings Group - Location Group

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Device and Location Configuration** > **Device Settings Groups** to open Device Settings Groups page. The Device Settings Groups page displays the list of Device Settings Groups.
3. Click **New** > **Location Group** to open the Device Settings Group screen.
4. On the Device Settings Group screen, enter the appropriate information about the Location Group.
5. Click **Save** to create a Location Group.
6. Click **Restore** to restore the default values of the parameters.

Related Links

Device Settings Groups field descriptions on page 463
Device Settings Group - Location Group field descriptions on page 467

Modifying a Device Settings Group - Location Group

About this task

You can modify only one Location Device Settings Group at a time.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Device and Location Configuration** > **Device Settings Groups** to open Device Settings Groups page. The Device Settings Groups page displays the list of Device Settings Groups.
3. Select a Location Group and click **Edit** to open the Device Settings Group page.
4. On the Device Settings Group page, modify the appropriate information to update the Location Group details.
5. Click **Save** to save the changes to the Location Group.
6. Click **Restore** to restore the default values of the parameters.

Related Links

Device Settings Groups field descriptions on page 463
Device Settings Group - Location Group field descriptions on page 467

Removing Device Settings Groups - Location Groups

About this task

You cannot delete the default Location Device Settings Group.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Device and Location Configuration** > **Device Settings Groups** to open Device Settings Groups page. The Device Settings Groups page displays the list of Device Settings Groups.
3. Select one or more Location Groups and click **Delete** to delete one or more Location Groups.

Related Links

Device Settings Groups field descriptions on page 463
Device Settings Group - Location Group field descriptions on page 467

Creating a Device Settings Group - Terminal Group

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Device and Location Configuration** > **Device Settings Groups** to open Device Settings Groups page. The Device Settings Groups page displays the list of Device Settings Groups.

3. Click **New** > **Terminal Group** to open the Device Settings Group page.
4. On the Device Settings Group page, enter the appropriate information of the new Terminal Group.
5. Click **Save** to create a new Terminal Group.
6. Click **Restore** to restore the default values of the parameters.

Related Links

Device Settings Groups field descriptions on page 463
Device Settings Group - Terminal Group field descriptions on page 470

Modifying a Device Settings Group - Terminal Group

About this task

You can modify only one Terminal Device Settings Group at a time.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Device and Location Configuration** > **Device Settings Groups** to open Device Settings Groups page. The Device Settings Groups page displays the list of Device Settings Groups.
3. Select an Terminal Device Setting Group and click **Edit** to open the Device Settings Group page.
4. On the Device Settings Group page, modify the appropriate information.
5. Click **Save** to save the changes to the Terminal Device Setting Group.
6. Click **Restore** to restore the default values of the parameters.

Related Links

Device Settings Groups field descriptions on page 463
Device Settings Group - Terminal Group field descriptions on page 470

Removing Device Settings Group - Terminal Group

About this task

You cannot delete the default Terminal Device Settings Group.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Device and Location Configuration** > **Device Settings Groups** to open Device Settings Groups page. The Device Settings Groups page displays the list of Device Settings Groups.
3. Select one or more Terminal Groups and click **Delete** to delete one or more Terminal Device Settings Groups.

Related Links

Device Settings Groups field descriptions on page 463
Device Settings Group - Terminal Group field descriptions on page 470

Purpose and usage of SIP subscriptions

SIP Subscription and Notification requests update connected SIP endpoints on state changes related to services that the endpoints consume. For example, when a new voice message arrives in a mailbox, Session Manager sends a SIP notification request to notify the related endpoints about the arrival of a new voice mail message.

For an endpoint to receive SIP notifications, it first needs to subscribe to the relevant subscription package. Each subscription package is related to a specific service that the network delivers to the endpoint. The SIP endpoints automatically establish all required subscriptions upon logging into the network.

When a subscription to an event package or service, is established, SIP subscription is assigned with a subscription expiration timer. The endpoint continues to receive notifications as long as the expiration timer does not expire. The endpoints automatically refresh any subscriptions before their expiration timer expires. A lower subscription expiration timer generates more SIP traffic related to subscription refresh events. Refreshing a subscription updates the state of the subscription.

Session Manager allows administration of the subscription expiration timer for each type of event package.

Device Settings Groups field descriptions

Use the Device Settings Groups page to enable a user to create and manage device configuration groups.

Button	Description
Default Group	Opens the Device Settings Group page that allows you to modify the Default Group.

Terminal Groups

Button	Description
New	Opens the Device Settings Group page that allows you to create a new Terminal Device Settings Group.
Edit	Opens the Device Settings Group page that allows you to modify the selected Terminal Device Settings Group.
Delete	Allows you to delete the selected Terminal Device Settings Group.

Name	Description
Name	Shows the name of the Terminal Device Settings Group.
Terminal Group Number	Specifies a numeric ID for this group. Using a group ID you can identify different phones on your network for ease of administration. With the exception of the field Group ID, Group parameters are the same as those for common phone parameters. Numeric IDs must be between 0 and 999.
Description	Shows the details of Terminal Device Settings Group.

Location Groups

Button	Description
New	Opens the Device Settings Group page that allows you to create a new Location Device Settings Group.
Edit	Opens the Device Settings Group page that allows you to modify the selected Location Device Settings Group.
Delete	Allows you to delete the selected Location Device Settings Group.

Name	Description
Name	Shows the name of the Location Device Settings Group.
Description	Shows the details of Location Device Settings Group.

Related Links

Viewing Device Settings Groups on page 460
Creating a Device Settings Group - Location Group on page 460
Modifying a Device Settings Group - Location Group on page 461
Removing Device Settings Groups - Location Groups on page 461
Creating a Device Settings Group - Terminal Group on page 461
Modifying a Device Settings Group - Terminal Group on page 462
Removing Device Settings Group - Terminal Group on page 462

Device Settings Group - Default Group field descriptions

General section

Name	Description
Name	Specifies a non–editable field as Default Group.

Table continues…

Name	Description
Description	Specifies a non–editable field as Default Group.
Group Type	Specifies a non–editable field as Location Group
Terminal Group Number	Specifies a non–editable field.

Server Timer section

Name	Description
Subscription Expiration Timer (secs)	Specifies the maximum duration as 86400 and minimum duration as 60 seconds for a SIP server to keep a SIP client as subscribed.
Registration Expiration Timer (secs)	Specifies the maximum duration as 3600 and minimum duration as 60 seconds for a SIP server to keep a SIP client as registered.

Endpoint Timer section

Name	Description
Line Reservation Timer (secs)	Specifies a required field and specifies the maximum duration, range is 30 to 240 seconds, for a SIP server that a SIP line appearance can be reserved for. If no value is entered, the default value is 30 seconds.
Reactive Monitoring Interval (secs)	Specifies the duration, in seconds, after which the phone attempts to Register with a proxy server when it is not reachable or available. Range is 10 to 3600 seconds. The default time is 60 seconds.
Timer B (sec)	Specifies the duration, in seconds, that the phone waits for a provisional response after transmitting a SIP INVITE to a proxy server and after not receiving any response from proxy being unavailable or unreachable, proceeds to another proxy. The range is 0 to 32 seconds. 0 disables this feature. The default value is 2.

Maintenance Settings section

Name	Description
IP Address For SNMP Queries	Specifies the IP address of a server that can query the phone for SNMP messages. This server must have the correct community string. If this field is blank, any server can query the phone.
SNMP Community	Specifies the SNMP community name. This string is both a challenge and a response for the server specified in the IP addresses for SNMP Queries field and the phone. If a server IP address is specified,

Table continues…

Name	Description
	both the server and the phone must have the same community name administered. Only alphabetic characters are allowed and length cannot exceed 32 characters.
Station Admin Password	Specifies the code that an administrator must enter on a SIP phone to log in and administer the phone. Only numeric values are accepted as code and length cannot exceed 32 digits.
Quick Login Status	Specifies the whether users must enter a password when logging in to the phone. There are two choices: Password Entry Required and Quick Login Allowed

VoIP Monitoring Manager section

Name	Description
IP Address	Specifies the IP address of the Avaya Voice over IP Monitoring Manager server.
Port	Specifies the port used by the Avaya Voice over IP Monitoring Manager server. The range is 1 through 65,535. The default port is 5005.
Reporting Period	Specifies how often an endpoint should send its RTCP packets of endpoints to the Avaya Voice over IP Monitoring Manager server. The range is 5 through 30 seconds. The default value is 5.

Volume Settings section

Name	Description
Receiver Volume	Sets the volume in the handset rather than the speaker. This is a required field and range is 0-10. The default value is 5.
Ringer Cadence	Sets the cadence of the ring tone. This is a required field and range is 1-8. The default value is 3.
Ringer Volume	Sets the ringer setting for the stations bridged appearance buttons. This is a required field and range is 1-10. The default value is 5.
Speaker Volume	Sets the volume on the speaker rather than the handset. This is a required field and the range is 0-10. The default value is 5.

VLAN Parameters section

Name	Description
VLAN Supported?	Indicates whether VLAN is supported. VLAN ID field disappears if unchecked.

DIFFSERV/QOS Parameters section

Name	Description
Call Control PHB Value	This is a required field and the range is 0-63. The default value is 46.
Audio PHB Value	This is a required field and the range is 0-63. The default value is 46.
Video PHB Value	This is a required field and the range is 0-63. The default value is 46.

802.1 P/Q Parameters section

Name	Description
Call Control 802.1p Priority	This is a required field and range is 0-7. The default value is 6.
Audio 802.1p Priority	This is a required field and range is 0-7. The default value is 6.
Video 802.1p Priority	This is a required field and range is 0-7. The default value is 5.

Button	Description
Restore	Restores the earlier device settings.
Cancel	Cancels the modified device settings.
Save	Saves the modified device settings.

Device Settings Group - Location Group field descriptions

General section

Name	Description
Name	Shows the name of the Location Device Settings Group.
Description	Shows Location Device Settings Group details.
Group Type	Shows a non-editable field specifying the type of Device Setting as Location Group

Server Timer section

Name	Description
Subscription Expiration Timer (secs)	Specifies the maximum duration as 86400 and minimum duration as 60 seconds for a SIP server to keep a SIP client as subscribed.
Registration Expiration Timer (secs)	Specifies the maximum duration as 3600 and minimum duration as 60 seconds for a SIP server to keep a SIP client as registered.

Assigned Location section

Name	Description
Name	Is the name of the location to which the Device Group Settings is associated.

Endpoint Timer section

Name	Description
Line Reservation Timer (secs)	Specifies a required field and specifies the maximum duration for a SIP server that a SIP line appearance can be reserved for. The range of line reservation timer field is 30–240 seconds. If no value is entered, the default value is 30 seconds.
Reactive Monitoring Interval (secs)	Specifies the duration after which (in seconds) the phone attempts to REGISTER with a proxy server when it is not reachable/available. Range is 10 to 3600 seconds. The default is 60 seconds.
Timer B (sec)	Specifies the duration (in seconds) that the phone waits for a provisional response after transmitting a SIP INVITE to a proxy server and after not receiving any response from proxy being unavailable or unreachable, proceeds to another proxy. The range is 0 to 32 seconds. (0 disables this feature.) The default value is 2.

Maintenance Settings section

Name	Description
IP Address For SNMP Queries	Specifies the IP address of a server that can query the phone for SNMP messages. This server must have the correct community string. If this field is blank, any server can query the phone.
SNMP Community	Specifies the SNMP community name. This string is both a challenge and a response for the server specified in the IP addresses for SNMP Queries field and the phone. If a server IP address is specified, both the server and the phone must have the same community name administered. Only alphabetic characters are allowed and length cannot exceed 32 characters.
Station Admin Password	Specifies the code that an administrator must enter on a SIP phone to log in and administer the phone. Only numeric values are accepted as code and length cannot exceed 32 digits.
Quick Login Status	Specifies the whether users must enter a password when logging in to the phone. There are two choices: Password Entry Required and Quick Login Allowed

VoIP Monitoring Manager section

Name	Description
IP Address	Specifies the IP address of the Avaya Voice over IP Monitoring Manager server.
Port	Specifies the port used by the Avaya Voice over IP Monitoring Manager server. The range is 1 through 65,535. The default is 5005.
Reporting Period	Specifies how often an endpoint should send its RTCP packets to the Avaya Voice over IP Monitoring Manager server. The range is 5 through 30 seconds. The default is 5.

Volume Settings section

Name	Description
Receiver Volume	Sets the volume in the handset rather than the speaker. This is a required field and range is 0-10. The default value is 5.
Ringer Cadence	Sets the cadence of the ring tone. This is a required field and range is 1-8. The default value is 3.
Ringer Volume	Sets the ringer setting for the stations bridged appearance buttons. This is a required field and range is 1-10. The default value is 5.
Speaker Volume	Sets the volume on the speaker rather than the handset. This is a required field and range is 0-10. The default value is 5.

VLAN Parameters section

Name	Description
VLAN Supported?	Indicates whether VLAN is supported. VLAN ID field disappears if unchecked.

DIFFSERV/QOS Parameters section

Name	Description
Call Control PHB Value	This is a required field and range is 0-63. The default value is 46.
Audio PHB Value	This is a required field and range is 0-63. The default value is 46.
Video PHB Value	This is a required field and range is 0-63. The default value is 46.

802.1 P/Q Parameters section

Name	Description
Call Control 802.1p Priority	This is a required field and range is 0-7. The default value is 6.
Audio 802.1p Priority	This is a required field and range is 0-7. The default value is 6.
Video 802.1p Priority	This is a required field and range is 0-7. The default value is 5.

Button	Description
Restore	Restores the earlier device settings.
Cancel	Cancels the modified device settings.
Save	Saves the modified device settings.

Related Links

Creating a Device Settings Group - Location Group on page 460
Modifying a Device Settings Group - Location Group on page 461
Removing Device Settings Groups - Location Groups on page 461

Device Settings Group - Terminal Group field descriptions

General section

Name	Description
Name	Specifies the name of the Terminal Device Settings Group.
Description	Specifies Terminal Device Settings Group details.
Group Type	Specifies a non editable field specifying the type of Device Setting as Terminal Group
Terminal Group Number	Specifies the Device Settings Group number

Endpoint Timer section

Name	Description
Line Reservation Timer (secs)	Specifies a required field and specifies the maximum duration for a SIP server that a SIP line appearance can be reserved for. The Line Reservation Timer range is 30 to 240 seconds. If no value is entered, the default value is 30 seconds.
Reactive Monitoring Interval (secs)	Specifies the duration, in seconds, after which the phone attempts to REGISTER with a proxy server when it is not reachable/available. Range is 10 to 3600 seconds. The default is 60 seconds.

Table continues…

Name	Description
Timer B (sec)	Specifies the duration, in seconds, that the phone waits for a provisional response after transmitting a SIP INVITE to a proxy server and after not receiving any response from proxy being unavailable or unreachable, proceeds to another proxy. The range is 0 to 32 seconds. 0 disables this feature. The default value is 2.

Maintenance Settings section

Name	Description
IP Address For SNMP Queries	Specifies the IP address of a server that can query the phone for SNMP messages. This server must have the correct community string. If this field is blank, any server can query the phone.
SNMP Community	Specifies the SNMP community name. This string is both a challenge and a response for the server specified in the IP addresses for SNMP Queries field and the phone. If a server IP address is specified, both the server and the phone must have the same community name administered. Only alphabetic characters are allowed and length cannot exceed 32 characters.
Station Admin Password	Specifies the code that an administrator must enter on a SIP phone to log in and administer the phone. Only numeric values are accepted as code and length cannot exceed 32 digits.
Quick Login Status	Specifies the whether users must enter a password when logging in to the phone. There are two choices: Password Entry Required or Quick Login Allowed

VoIP Monitoring Manager section

Name	Description
IP Address	Specifies the IP address of the Avaya Voice over IP Monitoring Manager server.
Port	Specifies the port used by the Avaya Voice over IP Monitoring Manager server. The range is 1 through 65,535. The default is 5005.
Reporting Period	Specifies how often an endpoint should send its RTCP packets to the Avaya Voice over IP Monitoring Manager server. The range is 5 through 30 seconds. The default is 5.

Volume Settings section

Name	Description
Receiver Volume	Sets the volume in the handset rather than the speaker. This is a required field and range is 0-10. The default value is 5.
Ringer Cadence	Sets the cadence of the ring tone. This is a required field and range is 1-8. The default value is 3.
Ringer Volume	Sets the ringer setting for the stations bridged appearance buttons. This is a required field and range is 1-10. The default value is 5.
Speaker Volume	Sets the volume on the speaker rather than the handset. This is a required field and range is 0-10. The default value is 5.

VLAN Parameters section

Name	Description
VLAN Supported?	Indicates whether VLAN is supported. VLAN ID field disappears if unchecked.

DIFFSERV/QOS Parameters section

Name	Description
Call Control PHB Value	This is a required field and the range is 0-63. The default value is 46.
Audio PHB Value	This is a required field and the range is 0-63. The default value is 46.
Video PHB Value	This is a required field and the range is 0-63. The default value is 46.

802.1 P/Q Parameters section

Name	Description
Call Control 802.1p Priority	This is a required field and the range is 0-7. The default value is 6.
Audio 802.1p Priority	This is a required field and the range is 0-7. The default value is 6.
Video 802.1p Priority	This is a required field and the range is 0-7. The default value is 5.

Button	Description
Restore	Restores the earlier device settings.
Cancel	Cancels the modified device settings.
Save	Saves the modified device settings.

Related Links

Creating a Device Settings Group - Terminal Group on page 461
Modifying a Device Settings Group - Terminal Group on page 462
Removing Device Settings Group - Terminal Group on page 462

Location Settings

Location Settings

Using the Location Settings functionality, you can assign a Device Settings Group to a Location.

Viewing location settings

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Device and Location Configuration** > **Location Settings** to open Location Settings page.

   The Location Settings page displays the list of location settings.

Related Links

Location Settings field descriptions on page 473

Modifying Location Settings

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Device and Location Configuration** > **Location Settings** to open Location Settings page.
3. Associate a location with the respective Device Settings Group.
4. Click **Save** to save the changes.

Related Links

Location Settings field descriptions on page 473

Location Settings field descriptions

Button	Description
Save	Saves the Location Settings.

Name	Description
Name	Name of the Location.
Device Setting Group	Name of the Device Setting Group.

Related Links

Modifying Location Settings on page 473
Viewing location settings on page 473

Application Configuration

Applications

Applications

Session Manager uses media-based filtering when invoking a set of sequenced applications for an originating or terminating call. Before invoking an application, Session Manager ensures the application supports the media type requested in the session request. If an application does not support the requested media, Session Manager skips that application in an application sequence.

The administrator defines the media attributes for each application.

Related Links

Application Sequences on page 480

Filtering of sequenced applications based on media attributes

Prior to invoking a provisioned originating or terminating sequenced application, Session Manager checks for the value of the “Enable Media Filtering” flag of the application.

- If the flag is set, Session Manager applies application filtering based on the provisioned media attributes conditions and the media types requested in the SDP. Session Manager invokes the sequenced application only if it passes the filter condition.
- If the “Media Filtering” flag is not set, Session Manager unconditionally invokes the sequenced application.

Session Manager applies the media based filtering for both orig-side and term-side applications.

For filtering the requests, Session Manager compares the SDP of the SIP request against the following attributes of the sequenced application: Audio, Video, Text, MatchType, and “If SDP Missing”.

Following table shows some of the possible examples for analysis of the media based filtering treatment:

Audio	Video	Text	MatchType	If SDP Missing	Description
Y	Y	Not Only	Exact	Allowed	Enables: {A,V,T} , {A,V} and request

Table continues…

					with no SDP only.
Y	Y	Not Only	Exact	Skip	Enables: {A,V,T} and {A,V} only. (Does not allow requests without SDP)
N	N	Not Only	Exact	Allowed	Invalid combination.
N	Not Only	Not Only	Not Exact	Skip	Invalid combination. At least one attribute must be Yes.
Y	Y	Not Only	Not Exact	Skip	Enables: {A}, {V}, {A, V}, {A,T}, {V, T}, {A,V,T}
Y	N	Not Only	Not Exact	Skip	Enables: {A} {A,T}

For an application with *Mandatory* condition in an application sequence:

If the “Enable Media Filtering” flag is enabled for an application, Session Manager does application filtering based on media irrespective of the “Mandatory” condition defined for the application.

Consider the following case:

1. Setup details
   - An application sequence vector seq-vector-abc consists of three applications app-a, app-b, and app-c in sequence.
   - Only app-a and app-b have “Mandatory” conditions defined.
   - The media based applicable filtering is enabled for seq-vector-abc. app-a and app-c support audio whereas app-b does not support audio.
2. Call processing details

   Upon receiving an originating audio request from a user of seq-vector-abc, Session Manager removes app-b from the list based on the media attribute filter processing. Even though “Mandatory” condition is defined for app-b, Session Manager shall not invoke app-b because app-b does not meet the media attribute filter condition. Session Manager shall invoke app-a followed by app-c in sequence. If the request fails when Session Manager invokes app-a, Session Manager shall not proceed with the request because app-a has “Mandatory” condition.

In survivable condition:

While in the survivable mode, for the requests that either originate from or targeted to the branch SIP endpoint and meet the media attribute filter conditions, Branch Session Manager shall invoke

LSP as the sequenced application. If the request does not meet the filter condition of LSP, Branch Session Manager shall skip the sequenced application invocation step.

Viewing applications

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Applications** to open the Applications page.

   The Applications page displays the list of applications.

Creating an application

Before you begin

Creating a new application entry requires that a non-Session Manager SIP entity first be administered. See the topic “Creating SIP entities” to create the SIP entity.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Applications** to open the Applications page.
3. Click **New**. The system displays the Application Editor page .
4. Enter the appropriate information for the new application.
5. Click **Commit** to create the application.

Related Links

Applications field descriptions on page 477
Application Editor field descriptions on page 478

Modifying an application

About this task

You can modify only one application at a time.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Applications** to open the Applications page.
3. Select an application and click **Edit** to open the Application Editor page.
4. On the Application Editor screen, modify the appropriate information.
5. Click **Commit** to save the changes.

Related Links

Applications field descriptions on page 477
Application Editor field descriptions on page 478

Removing applications

About this task

You cannot delete an application if the application is a part of an Application Sequence. If you try to delete the application, the system displays a warning , and the application entry remains.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Applications** to open the Applications page.
3. Select one or more applications and click **Delete** . The system displays the Delete Confirmation screen appears.
4. On the Delete Confirmation screen, click **Delete** to remove the application entries.

Related Links

Applications field descriptions on page 477

Applications field descriptions

Use each field to sort or filter records by enabling or disabling filter feature. Records are filtered on the basis of partial string match and as a combination of one or more fields.

Button	Description
New	Enables creating a new application entry.
Edit	Enables modifying the selected application entry.
Delete	Enables deleting the selected application entry.

Name	Description
Application Name	Name of the application.
SIP Entity	Name of the associated SIP Entity.
Media Filtering	Shows the status of media filtering for this application entry.
Description	Provides details about the application.

Related Links

Creating an application on page 476
Modifying an application on page 476
Removing applications on page 477

Application Editor field descriptions

Application section

Name	Description
Name	Name of the application entries. This is a mandatory field.
SIP Entity	List of previously provisioned SIP entities. This is a mandatory field.
CM System for SIP Entity	Select the Communication Manager (CM) system corresponding to the selected CM SIP entity.
Description	Provides details of the application.

Application Attributes (optional) section

Name	Description
Application Handle	A unique handle for the application. This handle is inserted in the Route header sent by Session Manager when it sequences a call to an application. Application handle is mainly used to distinguish between multiple applications running on the same host.
URI Parameters	List of URI parameters.

Application Media Attributes section

Name	Description
Enable Media Filtering	Indicates whether media filtering shall be applied to this sequenced application. If this check box is cleared, then all the fields in this section become disabled. This suggests that “Media Filtering” is disabled for this Application and that the Application will always be invoked irrespective of the media requested in the session requests.
Audio	Specifies whether this Application supports audio media Valid choices: YES, NO, NOT_ONLY Specifies whether this sequenced application supports audio media or not. The NOT_ONLY choice specifies that audio may be present with either text or video but not as an audio only media stream.
Video	Specifies whether this Application supports video media. Valid choices: YES, NO, NOT_ONLY Specifies whether this sequenced application supports video media or not. The NOT_ONLY choice

Table continues…

Name	Description
	specifies that video may be present with either audio or text but not as a video only media stream.
Text	Specifies whether this Application supports text media. Valid choices: YES, NO, NOT_ONLY Specifies whether this sequenced application supports text media or not. The NOT_ONLY choice specifies that text may be present with either audio or video but not as a text only media stream.
Match Type	The valid choices for this field are EXACT, NOT_EXACT • An "EXACT" entry in this field indicates that the SDP for this message must contain all of the media type specified with a "YES" and none of the media types specified with a "NO". • A "NOT_EXACT" entry in this field indicates that the SDP for this message must contain at least one of the media types specified with a "YES". • A "NOT_APPLICABLE" entry in this field indicated that SDP matches for this Application need not be done as the Application is to always be invoked.
If SDP Missing	Specifies whether or not the Application is to be invoked in the event that there is no SDP present in the INVITE. Valid choices: SKIP, ALLOW • If the SDP is not present and this field is set to “Allow” then the application is invoked. • If the SDP is not present and this field is set to “Skip” then the application is skipped. • If the SDP is present this field is ignored. If the SDP is present this field is ignored.

Button	Description
Cancel	Cancels the changes made to the application entry.
Commit	Saves the changes made to the application entry.

Related Links

Creating an application on page 476
Modifying an application on page 476

Application Sequences

Application Sequences

Application Sequence enables defining and managing an ordered set of applications used in call sequencing. These application sets can be associated as the originating and terminating application templates for a registered user's "Communication Profile" in the User Management module and enable routing every incoming, outgoing, or combined call for that user. Applications are assigned based on the user's needs and are not related to the location or the device used.

Session Manager provides the capability to create a profile for third party PBX users and add applications to be applied to these users to provide services, such as block calls based on user preferences, direct calls to these users when they move across the enterprise, and augment caller ID information for incoming and outgoing calls without upgrades or code modifications to existing third party PBX-equipment.

Related Links

Applications on page 474

Viewing application sequences

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Application Sequences** to open the Application Sequences page.

   The Application Sequences page displays the list of Application Sequences.

Related Links

Application Sequences field descriptions on page 482

Creating an Application Sequence

About this task

An Application Sequence can contain a maximum of up to 10 applications.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Application Sequences** to open the Application Sequences page.

   The Application Sequences page displays the list of Application Sequences.
3. Click **New**. The Application Sequence Editor page appears.
4. Enter the appropriate information.
5. Click **Commit** to create the Application Sequence.

Related Links

Application Sequences field descriptions on page 482
Application Sequence Editor field descriptions on page 483

Modifying an Application Sequence

About this task

You can modify only one Application Sequence at a time.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Application Sequences** to open the Application Sequences page.
3. Select an application sequence and click **Edit** . The system displays the Application Sequence Editor page.
4. On the Application Sequence Editor screen, modify the appropriate information.
5. Click **Commit** to save the changes.

Related Links

Application Sequences field descriptions on page 482
Application Sequence Editor field descriptions on page 483

Removing Application Sequences

About this task

You cannot delete an Application Sequence, if it is defined as an originating or terminating application set of a communication profile.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Application Sequences** to open the Application Sequences page.

   The Application Sequences page displays the list of Application Sequences.
3. Select one or more application sequence and click **Delete** . Delete Confirmation page appears.
4. Click **Delete** to remove the selected application sequences.

Related Links

Application Sequences field descriptions on page 482

Rearranging Applications in an Application Sequence

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.

2. In the left navigation pane, click **Application Configuration** > **Application Sequences** to open the Application Sequences page.
3. Select an Application Sequence and click **Edit** to open the Application Sequence Editor page.
4. In the section **Applications in this Sequence** do the following:
   - Click the buttons in the top panel to move selected Applications to the front or back of the Application Sequence or to remove Applications from the Application Sequence.
   - Click the buttons under **Sequence Order (first to last)** to change the relative sequence order of the Applications or to remove Applications from the Application Sequence.

Related Links

Application Sequence Editor field descriptions on page 483

Adding Applications in an existing Application Sequence

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Application Sequences** to open the Application Sequences page.
3. Select an application sequence and click **Edit** to open the Application Sequence Editor page.
4. In the section *Available Applications*, click the + button to add the application to the application sequence at the end.

Related Links

Application Sequence Editor field descriptions on page 483

Application Sequences field descriptions

Use the Application Sequence screen to add, edit, or remove sequences of applications.

Button	Description
New	Enables creating a new application sequence.
Edit	Enables modifying the selected application sequence.
Delete	Enables deleting the selected application sequence.

Name	Description
Name	Name of the application sequence.
Description	Details about the application sequence.

Related Links

Viewing application sequences on page 480
Creating an Application Sequence on page 480
Modifying an Application Sequence on page 481

Removing Application Sequences on page 481

Application Sequence Editor field descriptions

Sequence Name section

Name	Description
Name	Name of the application sequence. This is a mandatory field.
Description	Details of the application sequence .

Applications in this Sequence section

Button	Description
Move First	Move selected applications to become the first invoked in the sequence.
Move Last	Move selected applications to become the last invoked in the sequence.
Remove	Remove the selected applications from the sequence.

Name	Description
Sequence Order (first to last)	Change the relative sequence order of the applications or to remove applications from the application sequence.
Name	Name of the selected application.
SIP Entity	Name of the SIP entity associated with the selected application
Mandatory	Specifies whether the application is mandatory or not. If Session Manager fails to reach the application during the sequencing, Session Manager will stop sequencing and send an error response upstream. If the “Enable Media Filtering” flag is enabled for an application, Session Manager does application filtering based on media irrespective of the “Mandatory” condition. Session Manager skips the application if the request does not pass the media attribute filters irrespective of the “Mandatory” condition. For the requests that pass the application media attribute filter condition, Session Manager does application sequencing as per “Mandatory” condition. See the topic “Filtering of sequenced applications based on media attributes” for a related scenario.
Description	Description of the selected application

Available Applications section

Name	Description
+	Adds the selected application to the application sequence in the table Application in this Set above.
Name	Name of the application.
SIP Entity	Name of the SIP entity associated with the application
Description	Description of the application

Button	Description
Commit	Saves the changes made to the application sequence.
Cancel	Cancels the changes made to the application sequence.

Related Links

Creating an Application Sequence on page 480
Modifying an Application Sequence on page 481
Rearranging Applications in an Application Sequence on page 481
Adding Applications in an existing Application Sequence on page 482

Conference Factory URI

About Conference Factory URI

Conference Factory URI feature enables seamless integration of the conference capabilities provided by the conference products, such as Multimedia Collaboration Solution (MMCS), Meeting Exchange (MX), Communication Manager (CM) and the SIP endpoints like the Avaya Desktop Video Device (ADVD) with Session Manager (SM). This feature provides enhanced experience for conferences participants and enables richer collaboration when using voice, video, and text conference systems.

A Conference Factory Set is a collection of Conference Factory URI mappings having a unique URI referred as Conference Factory URI. In a Conference Factory URI mapping, a Conference Factory URI is associated with a respective Entity Name (Conference server name), Audio-Video-Text media attributes, Match Type parameters, and SDP parameters. On the User management page, you can associate a Conference Factory Set with Session Manager Communication Profile of a user.

Session Manager receives a REQUEST URI in the INVITE and compares the Request URI of the Invite with the provisioned Well Known Conference URI list. Then, Session Manager selects the Conference Factory Set and routes the call towards the associated Conference Server to create a new ad-hoc conference.

How the Conference Factory feature works

The Well Known Conference URI is a unique SIP address used by the endpoint to initiate a conference, while the Conference Factory URI is a unique SIP address of the Conference Server. An Avaya phone receives the “Well Known Conference URI ” from the settings file.

Session Manager contains a list of all provisioned Well Known Conference URIs and Conference Factory URIs in the database. Thus, Session Manager easily resolves the participant who wants to initiate the conference, and to which conference server the call has to be routed based on the user's Conference Factory Set (as specified in Session Manager Communication Profile of the user) as follows:

1. When the first participant wants to initiate a conference, the participant presses the conference button on the phone or by dragging the additional contacts into the spotlight (as applicable for some conferencing products).
2. The endpoint then sends an INVITE to Session Manager with the REQUEST URI set to the Well Known Conference URI.
3. Session Manager receives the INVITE, reads the Well Known Conference URI, and runs the originating application sequence.
4. Session Manager then compares the REQUEST URI of the INVITE with the provisioned Well Known Conference URI list.
5. If the URI does not match, Session Manager proceeds with the normal routing process.
6. If the URI matches, Session Manager runs the following process to route the call towards an appropriate conference server based on the priority level setting of the Conference Factory URI mappings:
    a. Session Manager identifies the Conference Factory Set defined in Session Manager Communication Profile of the originator and matches the provisioned Conference Factory Sets for evaluation.
    b. Session Manager compares the media type contained in the INVITE (SDP) with the media criteria specified for the first Conference Factory URI mapping of the Conference Factory Set.
    c. If the media types match the media attributes, Session Manager replaces the REQUEST URI of the INVITE with the respective Conference Factory URI and routes the call to the respective Conference Server that is the SIP Entity identified in the current Conference Factory URI mappings.
    d. If the media types do not match the media attributes, Session Manager compares the media type with the media attributes specified for the next Conference Factory URI mappings in the matched Conference Factory Set and so on.
    e. If there is no match between the endpoint media types in the INVITE and the media attributes specified for other Conference Factory URI mappings, Session Manager denies the conference initiation request and send back 403 response to the upstream SIP element.

f. In case SDP is not present in the INVITE message, Session Manager, based on the **If SDP Missing** field setting in the Conference Factory Set Web page, routes the call as per the following method:

- If the SDP is not present and this field is set to **Allow**, then Session Manager routes the call to the conference server as indicated in the Conference Factory URI mapping.
- If the SDP is not present and this field is set to **Deny**, then Session Manager does not route the call to the conference server as indicated in the Conference Factory URI mapping. In fact, Session Manager skips this conference server and goes to the next Conference Factory URI mappings until Session Manager finds SDP status as **Allow**.
- If the SDP is present, Session Manager ignores the **If SDP Missing** field

Depending on the conferencing needs of the enterprise, you can create multiple Conference Factory Sets in Session Manager. However, you cannot create more than 10 Well Known Conference URIs. You can add multiple Conference Factory URI mappings in the Conference Factory Set. To each Conference Factory URI mapping, you can assign particular URI, Entity Name (Conference server name), Audio-Video-Text media attributes, Match Type parameters, and SDP parameters. A conference server (defined as a SIP entity in the Conference Factory URI mapping) can be associated with multiple Conference Factory Sets. You can import and export these Conference Factory Sets and Well Known URIs using Bulk Importing and Exporting feature. Furthermore, you can assign Conference Factory Sets to the conference servers using Communication Profile Editor feature.

Session Manager replicates the Well Known Conference URIs table and the Conference Factory URIs table to all the core Session Manager instances and the associated Branch Session Manager (BSMs) instances. When, due to any reason, Branch Session Manager is cut off from the core Session Manager instances, BSM compares the Well Known Conference URI from the REQUEST URI of the INVITE with the provisioned Well Known Conference URI list on the BSM. Then, BSM routes the call to the appropriate conference server (SIP entity) that matches the associated user's feature server (LSP) or local trunk gateway.

Adding a new Well Known Conference URI

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Conference Factories**.
3. On the Conference Factories page, in **Well Known Conference URIs** tab, click **Add**.
4. In the **Well Known Conference URIs** column, click the cell and type an appropriate entry for the Well Known Conference URI as per the following specifications.

Note:

- The Well Known Conference URI name must contain at least two characters and must not exceed 255 characters.
- Do not use <, >, $, %, \, ^,*, and # characters.

- You may use characters from the UTF-8 character set.
- Do not include the sip: or sips: prefix when entering the Well Known Conference URI.
- Follow the RFC 3261 for more information on SIP URI format.

5. In **Description** column, click the cell and type a general description of the Well Known Conference URI.
6. Click **Commit** to save the Well Known Conference URI entry to the Session Manager database.
7. Click **Refresh** to refresh the list of URIs.

Caution:

Do not click **Refresh** before saving the field entries. You must click **Commit** to save the Well Known Conference URI record.

Note:

You can add a maximum of 10 Well Known Conference URIs. If you attempt to enter more than 10 Well Known Conference URI entries, Session Manager displays a message indicating that you cannot add more than 10 Well Known Conference URIs.

Place the cursor on **Well Known Conference URIs** column header. Click the arrow that appears on the right hand side of the column header, to sort the Well Known Conference URIs in alphabetical order.

Related Links

Conference Factories Field Description on page 491

Editing the Well Known Conference URI entry

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Conference Factories**.
3. On the Conference Factories page, in **Well Known Conference URIs** tab, click the Well Known Conference URI that you want to edit.
4. In **Well Known Conference URIs** column, click the cell to make the changes.

Note:

- The Well Known Conference URI name must contain at least two characters and must not exceed 255 characters.
- Do not use <, >, $, %, \, ^,*, and # characters.
- You may use characters from the UTF-8 character set.
- Do not include the sip: or sips: prefix when entering the Well Known Conference URI.
- Follow the RFC 3261 for more information on SIP URI format.

5. In **Description** column, click the cell to change the description.
6. Click **Commit** to update the modifications in Session Manager database.
7. Click **Refresh** to refresh the list of URIs.

Caution:

Do not click **Refresh** before saving the field entries. You must click **Commit** to save the Well Known Conference URI record.

Note:

Place the cursor on **Well Known Conference URIs** column header. Click the arrow that appears on the right hand side of the column header, to sort the Well Known Conference URIs in alphabetical order.

Related Links

Conference Factories Field Description on page 491

Removing the Well Known Conference URI entry

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Conference Factories**.
3. On the Conference Factories page, in **Well Known Conference URIs** tab, select the respective check box for the Well Known Conference URI you need to remove.

   You can select and remove multiple Well Known Conference URIs simultaneously.
4. Click **Remove**.
5. Click **Commit** to update the information in Session Manager database.
6. Click **Refresh** to refresh the list of URIs.

Caution:

Do not click **Refresh** before saving the URI entries. You must click **Commit** to update the Well Known Conference URI record.

Related Links

Conference Factories Field Description on page 491

Adding a new Conference Factory Set and setting the respective parameters

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Conference Factories**.
3. On the Conference Factories page, in **Conference Factory Set** tab, click **Add**.

4. On the Conference Factory Set page, enter the appropriate information as follows:
   - **Factory Set Name**: Enter a name for the Factory set.
   - **Description** : Enter a general description of the Factory set.
5. To add a conference factory URI mappings, under Conference Factory URI section, click **Add**.
   a. Click the row cell and enter an appropriate Conference Factory URI name.
   b. In **SIP Entity** field, from the drop-down list box, select an appropriate SIP entity that you need to assign for Conference Factory URI .
   c. In **Audio** field, select an appropriate option from the drop down list box to specify if this URI mapping supports voice conference.
      - Select **YES** to specify that this Conference Factory URI mapping supports voice conferencing.
      - Select **NO** to specify that this Conference Factory URI mapping does not support voice conferencing.
   d. In **Video** field, from the drop down list box, select an appropriate option to specify if this URI mapping supports video conference.
      - Select **YES** to specify that this Conference Factory URI mapping supports video conferencing.
      - Select **NO** to specify that this Conference Factory URI mapping does not support video conferencing.
   e. In **Text** field, from the drop down list box, select an appropriate option to specify whether this URI mapping supports text conference.
      - Select **YES** to specify that this Conference Factory URI mapping supports text conferencing.
      - Select **NO** to specify that this Conference Factory URI does not support text conferencing.
   f. In **Match Type** field, from the drop down list box, select an appropriate option to specify whether this URI mapping supports selected media types.
      - Select **EXACT** to indicate that SDP for this message should contain all the media types specified with **YES** and none of the media types specified with **NO**.
      - Select **NOT_EXACT** to indicate that SDP for this message should contain at least one media type specified with **YES**.
   g. In **If SDP Missing** field, from the drop down list box, select an appropriate option to specify whether Session Manager should route the INVITE to the Conference Factory URI when SDP is not present.
      - If the SDP is not present and this field is set to **ALLOW**, then Session Manager routes the call to the conference server as indicated in the Conference Factory URI mapping.

- If the SDP is not present and this field is set to **DENY**, then Session Manager does not route the call to the conference server as indicated in the Conference Factory URI mapping. In fact, Session Manager skips this conference server, goes to the next Conference Factory URI mappings until Session Manager finds SDP status as **ALLOW**.
- If the SDP is present, Session Manager ignores the **If SDP Missing** field.

h. In **Priority** field, set the priority to evaluate INVITE order evaluation. Move up to determine higher priority and move down to determine lower priority.

6. Click **Commit** to save the information.
7. On the Conference Factories page, click **Refresh** to refresh the list of Conference Factory Sets.

Related Links

Conference Factories Field Description on page 491
Conference Factory Set Page Field Description on page 493

Viewing the Conference Factory Set

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Conference Factories**.
3. On the Conference Factories page, click the **Conference Factory Set** tab.
4. On the Conference Factory Set page, select the respective check box for the Conference Factory Set you need to view.
5. Click **View** to view the details of the selected Conference Factory Set.
6. Click **Cancel** to return to the previous page.

Related Links

Conference Factories Field Description on page 491
Conference Factory Set Page Field Description on page 493

Editing the Conference Factory Set

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Conference Factories**.
3. On the Conference Factories page, click the **Conference Factory Set** tab.
4. On the Conference Factory Set page, select the respective check box for the Conference Factory Set you need to edit.
5. Click **Edit**.

6. Enter the appropriate information as follows:
   - **Factory Set Name** : Modify the name for the Conference Factory set.
   - **Description** : Modify a general description of the Conference Factory set.
   - In the Conference Factory URI section, add or remove the Conference Factory URI mappings or change other parameters.
7. Click **Commit** to update the information.
8. On the Conference Factories page, click **Refresh** to refresh the list of administered Conference Factory Sets.

Related Links

Conference Factories Field Description on page 491
Conference Factory Set Page Field Description on page 493

Deleting the Conference Factory Set

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Application Configuration** > **Conference Factories**.
3. On the Conference Factories page, click the **Conference Factory Set** tab.
4. On the Conference Factory Set page, select the respective check box for the Conference Factory Set you need to delete.

   You can delete more than one Conference Factory Set simultaneously.
5. Click **Delete**.
6. On the delete confirmation notice, click **OK**.
7. On the Conference Factories page, click **Refresh** to refresh the list of administered Conference Factory Sets.

Related Links

Conference Factories Field Description on page 491
Conference Factory Set Page Field Description on page 493

Conference Factories Field Description

Well Known Conference URI tab

Button	Description
Add	Adds a new entry of Well Known Conference URI to the table.
Remove	Removes the selected Well Known Conference URI entry from the table.

Table continues…

Button	Description
Reset	Discards the changes made and restores the saved Well Known URI values.
Commit	Saves the Well Known Conference URI entry in the Session Manager database.
Refresh	Refreshes the information in theSession Manager database

Field	Description
Well Known Conference URI	Displays a list of the provisioned Well Known Conference URIs.
Description	Displays a brief description of the Well Known Conference URI.

Conference Factory Set Tab

Button	Description
Add	Navigates you to the Conference Factory Set page using which you can add new Conference Factory Set.
View	Navigates you to the Conference Factory Set page using which you can view the details of the selected Conference Factory Set.
Edit	Navigates you to the Conference Factory Set page using which you can edit the details of the selected Conference Factory Set.
Delete	Deletes the Conference Factory Set entry from the Session Manager database.

Field	Description
Factory Set Name	Displays a name of the provisioned Conference Factory Sets.
Communication Profiles	Number of users with Session Manager Communication Profile references to this Conference Factory Set.
Description	Displays a brief description of the selected Conference Factory Set.

Related Links

Adding a new Well Known Conference URI on page 486
Editing the Well Known Conference URI entry on page 487
Removing the Well Known Conference URI entry on page 488
Adding a new Conference Factory Set and setting the respective parameters on page 488
Viewing the Conference Factory Set on page 490

Editing the Conference Factory Set on page 490
Deleting the Conference Factory Set on page 491

Conference Factory Set Page Field Description

Fields	Description
Factory Set Name	Name of the Conference Factory Set. The following section defines the collection of Conference Factory URI mappings for this Factory Set.
Description	Details of the Factory Set.

Conference Factory URIs

Button	Description
Add	Adds a new entry for Conference Factory URI in the table.
Remove	Removes the selected entry of the Conference Factory URI from the table.

Fields	Description
Priority	Sets the order to evaluate INVITE for a match.
Conference Factory URI	Indicates the Conference Factory URI without "sip:" or "sips:" prefix.
SIP Entity	Indicates the Conference Server SIP Entity linked to this Conference Factory URI.
Audio	Specifies whether or not this Conference Factory URI supports voice conference. • Select **Yes** to specify that this Conference Factory URI mapping supports voice conferencing. • Select **No** to specify that this Conference Factory URI mapping does not support voice conferencing.
Video	Specifies whether or not this Conference Factory URI supports video conference. • Select **Yes** to specify that this Conference Factory URI mapping supports video conferencing. • Select **No** to specify that this Conference Factory URI mapping does not support video conferencing.
Text	Specifies whether or not this Conference Factory URI supports text conference. • Select **Yes** to specify that this Conference Factory URI mapping supports text conferencing.

Table continues…

Fields	Description
	• Select **No** to specify that this Conference Factory URI does not support text conferencing.
Match Type	Specifies whether or not this Conference Factory URI needs to match all the media types. **Exact** indicates that SDP for this message must contain all the media types specified with **Yes** and none of the media types specified with **No**. **Not Exact** indicates that SDP for this message should contain at least one media type specified with **Yes**.
If SDP missing	Specifies the condition whether Session Manager will route the INVITE to the Conference Factory URI in case when SDP is not present in the Conference Factory URI. • If the SDP is not present and this field is set to **Allow**, then Session Manager routes the call to the conference server as indicated in the Conference Factory URI mapping. • If the SDP is not present and this field is set to **Deny**, then Session Manager does not route the call to the conference server as indicated in the Conference Factory URI mapping. In fact, Session Manager skips this conference server, go to the next Conference Factory URI mappings until Session Manager finds SDP status as **Allow**. • If the SDP is present, Session Manager ignores the **If SDP Missing** field.

Button	Description
Commit	Saves the Conference Factory Set in the Session Manager database.
Reset	Discards the changes made and restores the saved Conference Factory Set.
Cancel	Returns to the Conference Factories page without saving any changes.

Related Links

Adding a new Conference Factory Set and setting the respective parameters on page 488
Viewing the Conference Factory Set on page 490
Editing the Conference Factory Set on page 490
Deleting the Conference Factory Set on page 491

Implicit Users

Implicit Users

Use Implicit Users functionality to administer certain dial patterns for users, who do not register or connect with Session Manager. You can use this functionality to provision a set of originating and terminating sequenced applications for such users.

SIP User Implicit Sequencing

You can apply origination and termination application sequencing for SIP (explicit) users based on implicit user application sequencing definitions.

During origination, Session Manager sequences through explicit, then implicit origination applications.

During termination, Session Manager sequences through implicit, then explicit termination applications.

For backwards compatibility, implicit sequencing for SIP users is **disabled** by default.

Implicit sequencing for a SIP user is performed from the user's Session Manager only. For non-SIP users, any Session Manager can perform implicit sequencing.

Implicit sequencing can route-through to an alternate Session Manager to reach an application. For a SIP user, route-through is limited to the Session Managers in the user's community.

Viewing Implicit User Rules

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. Click **Application Configuration** > **Implicit Users** to open Implicit Users page.

   The Implicit Users page displays the list of Implicit User rules.

Related Links

Implicit User Rules field descriptions on page 496

Creating an Implicit User Rule

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. To open Implicit Users page, click **Application Configuration** > **Implicit Users**
3. Click **New**.

   The system displays the Implicit User Rule Editor page.
4. On the Implicit User Rule Editor page, enter the appropriate information.
5. Click **Commit** to create a new Implicit User rule.

Related Links

Implicit User Rules field descriptions on page 496
Implicit User Rule Editor field descriptions on page 497

Modifying an existing Implicit User Rule

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. To open Implicit Users page, click **Application Configuration** > **Implicit Users** .
3. To open the Implicit User Rule Editor page, select an Implicit User rule and click **Edit**.
4. On the Implicit User Rule Editor page, modify the appropriate information.
5. Click **Commit** to save the changes to the Implicit User rule.

Related Links

Implicit User Rules field descriptions on page 496
Implicit User Rule Editor field descriptions on page 497

Removing existing Implicit User Rules

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. To open Implicit Users page, click **Application Configuration** > **Implicit Users** .
3. Select one or more Implicit User rules and click **Delete** to delete one or more Implicit User rules respectively.

   The system displays the Delete Confirmation screen.
4. On the Delete Confirmation screen, click **Delete** to remove the selected Implicit User rules.

Related Links

Implicit User Rules field descriptions on page 496

Implicit User Rules field descriptions

Button	Description
New	Enables creating a new Implicit User Rule.
Edit	Enables modifying the selected Implicit User Rule.
Delete	Enables deleting the selected Implicit User Rule.

Name	Description
Pattern	Dial pattern with the same pattern format as the Routing Policy Dial pattern.
Min	Minimum value of the dial pattern matching. Valid values are from 1 to 36.

Table continues…

Name	Description
Max	Maximum value of the dial pattern matching. Valid values are from 1 to 36.
SIP Domain	Associated SIP Domain.
Origination Application Sequence	Origination Application Sequence.
Termination Application Sequence	Termination Application Sequence.
Description	Description of the Rule.

Related Links

Viewing Implicit User Rules on page 495
Creating an Implicit User Rule on page 495
Modifying an existing Implicit User Rule on page 496
Removing existing Implicit User Rules on page 496

Implicit User Rule Editor field descriptions

Use the Implicit User Rule Editor screen to define a new pattern rule or to modify an existing pattern rule.

Name	Description
Pattern	Shows a dial pattern with the same pattern format as the Routing Policy Dial pattern. This field is a mandatory field.
Min	Shows the minimum value of the dial pattern matching. Valid values are 1-36. This field is a mandatory field. The value must be higher than the pattern length.
Max	Shows the maximum value of the dial pattern matching. Valid values range from 1 to 36. This field is a mandatory field.
Description	Shows the description of the Rule.
SIP Domain	Shows the name of the SIP Domain
Origination Application Sequence	Shows the name of the Origination Application Sequence
Termination Application Sequence	Shows the name of the Termination Application Sequence

Button	Description
Cancel	Cancels the changes made to the Implicit User Rule.
Commit	Saves the changes made to the Implicit User Rule.

Related Links

Creating an Implicit User Rule on page 495
Modifying an existing Implicit User Rule on page 496

Administering Implicit Applications for SIP users

By default, the **Enable Implicit User Applications for the SIP users** checkbox is not selected.

Procedure

1. On the System Manager web console home page, under **Elements**, click **Session Manager > Session Manager Administration**.
2. Under the **Global Settings** section, enable or disable **Enable Implicit User Applications for SIP users**.

Session Manager Network Connect Service

NRS Proxy Users

Session Manager Network Connect Service (NCS) provides routing services to VoIP endpoints based on Avaya Communication Server 1000 (CS1000). This service is similar to the services provided by Nortel Network Routing Service (NRS). The NRS provides following three services:

- SIP Proxy Server (SPS): SPS performs two roles in CS1000-based configuration. These roles are SIP routing proxy and SIP registrar.
- Network Connect Server (NCS): NCS supports the centralized CS1000 solution for IP clients, that is, IP phones.
- H.323 Gatekeeper (GK): GK provides typical H.323 gatekeeper functions to H.323 endpoints in the solution.

Session Manager provides both the SIP Proxy Server (SPS) and Network Connect Server (NCS) functionality that are provided by Nortel NRS.

Session Manager provides the following information to each UNIStim phone:

- Primary signaling server
- Secondary signaling server
- Branch Office, Survivable Media Gateway or Survivable Remote Gateway

Session Manager NCS provides network redirection services for UNIStim phones for several CS1000 network features, such as geographic redundancy, virtual office, branch office, and Survivable Remote Gateway. You can define user patterns that are administered as a NRS Proxy User Rule in Session Manager, and associate user patterns with up to three CS 1000 Terminal Proxy Servers in priority order. Since a large number of users share the same server set, you can administer a range for the user pattern to match a large set of users.

Redirecting UNIStim Phones

About this task

In normal conditions, all UNIStim phones in the system should be configured with their Primary Connect Server, Primary CS 1000, pointing to the local Primary Session Manager and the Secondary Connect Server, Secondary CS 1000, pointing to the Secondary Session Manager.

Following are the administration steps:

Procedure

1. Point each SIP Signaling Gateway from the SIP Proxy Server (SPS) to the Session Manager. See CS1000 documentation.
2. Reconfigure NCS pointing to Session Manager. See CS1000 documentation.
3. Create Terminal Proxy Server instances for Primary signaling server and Secondary signaling server as per your system requirement.
4. Create Terminal Proxy Server instances for each Branch Office, Survivable Media Gateway, or Survivable Remote Gateway 50.
5. Create an NRS Proxy User Rule.

Related Links

Creating Terminal Proxy Server instance on page 499
Creating a NRS Proxy User Rule on page 499

Creating Terminal Proxy Server instance

Procedure

1. On System Manager Web Console, click **Elements** > **Inventory**.
2. From the left navigation pane, click **Inventory** > **Manage Elements**.
3. On the Manage Elements page, click **New** and select a “CS 1000 Terminal Proxy Server” entity instance.
4. On the New CS 1000 Terminal Proxy Server page, enter the following details:
   - In the **Name** field, enter the H323 ID value of the Main or Primary Signaling Server.
   - Enter the Node IP address of the Main or Primary Signaling Server.
5. Click **Commit**.

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

Creating a NRS Proxy User Rule

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. To open the NRS Proxy Users page, click **Application Configuration** > **NRS Proxy Users** .
3. Click **New** and enter the appropriate information for the new NRS Proxy User Rule.
4. Click **Commit**.

Note:

Terminal Proxy Server should be administered using **Elements** > **Inventory** > **Manage Elements**.

Related Links

NRS Proxy Users field descriptions on page 501
NRS Proxy User Rule Editor field descriptions on page 501

Modifying NRS Proxy User Rule

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. To open the NRS Proxy Users page, click **Application Configuration** > **NRS Proxy Users**.
3. Select the NRS Proxy User Rule to be modified and click **Edit**.
4. On the NRS Proxy User Rule Editor page, modify the information and click **Commit** to save the changes.

Note:

Terminal Proxy Server must be administered using **Elements** > **Inventory** > **Manage Elements**.

Related Links

NRS Proxy Users field descriptions on page 501
NRS Proxy User Rule Editor field descriptions on page 501

Deleting NRS Proxy User rule

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. To open NRS Proxy Users page, click **Application Configuration** > **NRS Proxy Users**.
3. Select one or more NRS Proxy User rule from the list and click **Delete**.
4. On the Delete Confirmation screen, click **Delete** to delete the selected NRS Proxy User rules.

Related Links

NRS Proxy Users field descriptions on page 501
Delete Confirmation page field descriptions on page 500

Delete Confirmation page field descriptions

Button	Description
Cancel	Cancels the deletion of the selected NRS Proxy User rule.
Delete	Deletes the selected NRS Proxy User rule.

Related Links

Deleting NRS Proxy User rule on page 500

NRS Proxy Users field descriptions

Button	Description
New	Adds a new entry.
Edit	Saves the changes of the modified entry.
Delete	Deletes the selected entry.

Name	Description
Pattern	User Pattern type.
Primary Terminal Proxy Server	Administered Terminal Proxy Server. This field is a required field.
Secondary Terminal Proxy Server	Administered Terminal Proxy Server.
Survivable Terminal Proxy Server	Administered Terminal Proxy Server.

Related Links

Creating a NRS Proxy User Rule on page 499
Modifying NRS Proxy User Rule on page 500
Deleting NRS Proxy User rule on page 500

NRS Proxy User Rule Editor field descriptions

Name	Description
Pattern	Specifies the User Pattern. This field is a required field. The prefix can include the numbers 0 to 9, and the hash (#), the hyphen (-), and the question mark (?) symbols. The prefix can have a length of up to 30 characters, but the first character must be numeric. Routing entries can be categorized in the following way: • Basic digits: Any number of digits can be used to make a simple entry. For example, 570 • Range of digits: Two basic digit entries can be used to build a range entry. The range will have a dash between the two ranges and each range will have the same number of digits. For example, 467 – 486 is valid but 467 – 4866 is invalid. • Length delimited: A basic digit entry can be terminated with the hash "#" symbol to force a specific length match. For example, 5703360#.

Table continues…

Name	Description
	• Wild card: The wild card digit character "?" can be appended to a basic digit entry. Multiple wild cards may be appended, but each wild card character matches only one digit. For example, 57033??.
Primary Terminal Proxy Server	Select an administered Terminal Proxy Server. This field is a required field.
Secondary Terminal Proxy Server	Select an administered Terminal Proxy Server.
Survivable Terminal Proxy Server	Select an administered Terminal Proxy Server.

Button	Description
Commit	Saves the changes made to the NRS Proxy User Rule.
Cancel	Cancels the changes made to the NRS Proxy User Rule.

Related Links

Creating a NRS Proxy User Rule on page 499
Modifying NRS Proxy User Rule on page 500

System Status

Session Manager SIP Entity Monitoring

SIP Entity Monitoring provides background detection for monitored connections to improve alternative routing and to minimize the call setup time due to SIP link failures. The SIP Monitor periodically tests the status of the SIP proxy servers. If a proxy fails to reply, SIP messages are no longer routed to that proxy. As a result, call delays are reduced since calls are not routed to the failed servers. The SIP Monitor continues to monitor the failed SIP entity. When the proxy replies, SIP messages are again routed over that link.

SIP monitoring sends OPTIONS requests to SIP entities to determine whether these are in up, partially up, down or deny new service state. An entity is considered up if all of the addresses associated with it are up. An entity is down if all of its addresses are down. An entity is partially up if some, but not all, of its addresses are up. An address is considered down if the response of address to OPTIONS is:

- 408 Request Timeout
- 500 Server Internal Error: Destination Unreachable
- 503 Service Unavailable (with no parenthetical text)
- 503 Service Unavailable (no media resources)

- 504 Server Timeout

All other responses (including "503 Service Unavailable") with other parenthetical text, such as "503 Service Unavailable (Signaling Resources Unavailable)" results in the address to be considered up.

Note:

Any 503 response is displayed as a 500 response on the SIP Monitoring GUI. SIP container converts 503 to 500 before passing the response to Session Manager.

You can turn the monitoring on or off for a given SIP entity. If monitoring is turned off, the SIP entity is not monitored by any instance.

You can also turn monitoring on or off for an entire instance. If monitoring is turned off, none of the SIP entities are monitored by that instance. If monitoring for the instance is turned on, only those SIP entities for which monitoring is turned on are monitored.

SIP Monitoring can only report problems if the Security Module is functional.

SIP Monitoring setup is administered using the SIP Entity and the Session Manager Administration pages on System Manager. See the sections *SIP Entities*, *Session Manager Administration* and *SIP Responses to an OPTIONS Request* from the book *Administering Avaya Aura® Session Manager*.

Related Links

Handling SIP responses on page 247
SIP Responses to an OPTIONS Request on page 297

Viewing the SIP Monitoring Status Summary page

About this task

The SIP Entity Link Monitoring Status Summary page displays the status of the entity links for all the administered Session Manager instances. An entity link consists of one or more physical connections between a Session Manager server and a SIP entity.

If all connections are up, then the entity link status is **up**. If one or more connections are down but there is at least one connection up, the link status is **partially down**. If all of the connections are down, the entity link status is **down**. If the connection denies any new service, the entity link status is **deny new service**.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **SIP Entity Monitoring**

   The **SIP Entity Link Monitoring Status Summary** page displays the SIP Entity Link monitoring status for all Session Manager instances.

SIP Entity Link Monitoring Status Summary page field descriptions

SIP Entities Status for ALL Monitoring Session Manager Instances

Button	Description
Run Monitor	Starts asynchronous demand monitor test for the selected Session Manager or Branch Session Manager instances.
Refresh	Refreshes the status of the entity links for all administered Session Manager instances.

Field	Description
Session Manager	Name of the Session Manager instance. Clicking any of Session Manager servers in the list opens the Session Manager Entity Link Connection Status page that displays detailed connection status for all entity links from Session Manager. **Note:** An entity link consists of one or more physical connections between a Session Manager server and a SIP entity. If all of these connections are up, then the entity link status is *up*. If one or more connections are down, but there is at least one connection up, then the entity link status is *partially down*. If all the connections are down, the entity link status is *down*.
Type	Instances of type Session Manager and Branch Session Manager.
Monitored Entities / Down	Entity links for Session Manager that are down out of the total number of entity links for Session Manager.
Monitored Entities / Partially Up	Entity links for Session Manager that are partially up.
Monitored Entities / Up	Entity links for Session Manager that are up out of the total number of entity links for Session Manager.
Monitored Entities / Not Monitored	SIP entities that are not monitored, because they are not administered to be monitored by Session Manager.
Monitored Entities / Deny	Number of Deny New Service Entity Links.
Monitored Entities / Total	Number of total Entity Links for a SIP Entity.

All Monitored SIP Entities

Button	Description
Run Monitor	Starts asynchronous demand monitor test for the selected SIP entities. Clicking any of the entities in the list opens the SIP Entity, Entity Link Connection

Button	Description
	Status page that displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Session Manager Entity Link Connection Status page field descriptions

All Entity Links with connections to Session Manager

Field	Description
SIP Entity Name	Name of the SIP Entity.
SIP Entity Resolved IP	Resolved IP address of the SIP entity.
Port	Port used for the connection.
Protocol	Protocol used.
Deny	Deny new service status.
Conn. Status	Connection status.
Reason Code	Reason for the failure. This field explains how the status of a connection is determined irrespective of whether the status is “up” or “down”.
Link Status	Status of the Entity Link.

Button	Description
Summary View	Returns to the SIP Entity Link Monitoring Status Summary page.
Refresh	Refreshes and displays the detailed connection status for all entity links from the selected Session Manager instance.

Details

Field	Description
Time Last Down	Time when the entity link was last down.
Time Last Up	Time when the entity link was last up.
Last Message Sent	Port used for the connection.
Last Message Response	Duration of the last response latency (ms).

SIP Entity, Entity Link Connection Status page field descriptions

All Entity Links to SIP Entity

Field	Description
Session Manager Name	Name of the Session Manager instance.
SIP Entity Resolved IP	Resolved IP address of the SIP entity

Table continues…

Field	Description
Port	Port used for the connection
Protocol	Protocol used
Deny	Deny new service status.
Conn. Status	Connection status
Reason Code	Reason for the failure. This field explains how the status of a connection is determined irrespective of whether the status is “up” or “down”.
Link Status	Status of the Entity Link.

Button	Description
Summary View	Returns to the SIP Entity Link Monitoring Status Summary page.
Refresh	Refreshes and displays the detailed connection status for all entity links from all Session Manager instance to a single SIP entity.

Details

Field	Description
Time Last Down	Time when the entity link was last down
Time Last Up	Time when the entity link was last up
Last Message Sent	Port used for the connection
Last Message Response	Duration of the last response latency (ms)

Managed Bandwidth

The Managed Bandwidth Usage page displays Managed Bandwidth (Call Admission Control) real-time data. Bandwidth usage measurements help administrators to manage networks with multimedia calls. The Managed Bandwidth Usage page displays a table containing one row for each administered location and provides details on actual call counts and bandwidth usage for audio and video calls respectively.

You can expand each row to display a breakdown of usage and capacity by Session Manager, which can help troubleshoot network utilization or the distribution algorithm. If no bandwidth management is administered, the table contains no data.

Viewing Managed Bandwidth Usage

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Managed Bandwidth Usage**.

The Managed Bandwidth Usage screen displays system-wide bandwidth usage information for locations where usage is managed.

3. Click **Show** under Details column to view the bandwidth usage information per Session Manager in that location. You can click **Hide** to close this table.
4. On the Managed Bandwidth Usage screen, click **Refresh** to refresh the data.

Managed Bandwidth Usage page field descriptions

The Manage Bandwidth Usage page displays system-wide bandwidth usage information for locations where usage is managed. If there is no bandwidth management implemented, this table has no information.

Field	Description
Details	Shows the breakdown of usage among the administered Session Managers in the enterprise. You can click the Show or Hide arrow on any row in **Details** to show or hide the detailed usage for that location.
Location	Displays the locations that you have administered in the Routing Policy.
Audio Call Count	Indicates sum of audio calls of Session Manager in a given location.
Audio BW Used	Indicates sum of bandwidth used for audio calls of Session Managers in a given location.
Multimedia Call Count	Indicates sum of multimedia calls of Session Managers in a given location.
Multimedia BW Used	Indicates sum of bandwidth used for multimedia calls of Session Managers in a given location.
Multimedia BW Allow	Administered value, if any, of multimedia Bandwidth for a given location.
Multimedia BW %Used	Indicates sum of bandwidth used for multimedia calls into or out of a given location divided by the value in the "Multimedia BW Allow" column.
Total BW Used	Indicates sum of audio and multimedia bandwidth into or out of a given location
Total BW Allow	Administered value, if any, of "Total Bandwidth" for a given location.
Total BW %Used	Indicates sum of audio and multimedia bandwidth for calls into or out of a given location divided by the value in the "Total BW Allow" column.

Field	Description
Session Manager	Name of the instance.

Table continues…

Field	Description
Audio Call Count	Number of audio calls terminated by the selected Session Manager for the given location.
Audio BW Used	Sum of bandwidth used by audio calls terminated by the selected Session Manager for the given location.
Multimedia Call Count	Number of multimedia calls terminated by the selected Session Manager for the given location.
Multimedia BW Used	Indicates sum of bandwidth used by multimedia calls terminated by the selected Session Manager for the given location.

Security Module Status

About Security Module Status

Use the Security Module Status page to view the status of the security module for each administered Session Manager and to perform certain actions on the security module.

You can view the status of the security module, such as the IP address of security module, default gateway, the interface that a security module uses, the VLAN that it is associated with, the QOS priority, trusted hosts configured for that security module, and the certificate authority.

You can also reset and synchronize the security module or assign a certificate authority.

Security Module Status actions

Use the Security Module Status page to perform the following actions:

- **Refresh**: Refreshes the statistics for all of the administered Session Manager instances.
- **Reset** : Resets the security module for the selected Session Manager. You may choose to reset the security module when a connection cannot be made to the security module.

  Warning:

  The Session Manager cannot process calls while the security module is being reset. See *Administering Avaya Aura® Session Manager* for details on how to disable the Session Manager prior to resetting the security module.
- **Synchronize**: Verifies that the administered configuration matches the actual configuration stored on the security module. This action should be performed anytime the values in the security module statistics table do not match the administered data.
- **Connection Status**: Shows the view of the current status of inbound and outbound links between the Session Manager security module and external hosts. Connection Status enables general-purpose monitoring and debugging activities, such as:
  - identifying if the Session Manager is required to be taken out of service
  - determining if links are secured or not

- viewing link details and statistics

Investigating Security Module status

Possible causes for the Security Module status to be **Down** include:

- The security module may have recently been reset. A reset can take several minutes to complete.
- The security module may not have received security module configuration information from System Manager System Manager.

Procedure

1. On the System Manager Web Console, under **Services**, click **Replication** to display the **Replica Group** associated with the Session Manager instance.
2. If the **Synchronization Status** is not **Synchronized** for the Session Manager instance:
   a. Select the affected Replica Group.
   b. Click **View Replica Nodes**.
   c. On the Replica Nodes page, verify the **Replica Node Host Name** is correct.
   d. If the **Replica Node Host Name** is incorrect, click **Repair**.
3. Click **Refresh** to see the latest status.
4. On the Security Module Status page, if the status is **Down**, synchronize the security module to trigger an update:
   a. Click the button in front of the appropriate Session Manager instance from the Session Manager list.
   b. Click **Synchronize**.
   c. Click **Refresh** to see the latest status.
5. If the status is still **Down**, reset the security module:
   a. Select the appropriate Session Manager instance from the Session Manager list.
   b. Click **Reset**.

      Warning:

      The Session Manager cannot process calls while the security module is being reset.
6. Select **Refresh** to see the latest status.

Security Module Status page field descriptions

Button	Description
Reset	Opens the Security Module Reset Confirmation page.
Synchronize	Synchronizes the security module of the selected Session Manager and displays the Confirm Security Module Synchronize page.
Connections Status	Displays the connection status information for the selected Session Manager instance.

Name	Description
Details	Displays detailed information about the selected Session Manager instance. **Note:** Details are available only in certain releases or if additional features are enabled.
Session Manager	Displays the name of the Session Manager instance.
Type	Displays the type of Session Manager instance (SM or BSM).
Status	Displays the status of the Security Module deployed for the Session Manager (up or down).
Connections	Displays the total number of connections for the Security Module.
IP Address	Displays the IP address of the security module used for SIP traffic. This field should match the address administered on the SIP Entity form for the Session Manager instance.
VLAN	Displays the VLAN ID associated with the security module. This field should match the VLAN ID administered on the Session Manager instance form.
Default Gateway	Displays the default Gateway used by the security module. This value should match the default gateway administered on the Session Manager instance form.
NIC Bonding	Displays if NIC bonding is “enabled” or “disabled”.
Entity Links (expected / actual)	Displays the expected and actual number of Entity Links. The expected value is the number of SIP Entities configured in the Routing Policy that have Entity Links to the Session Manager. The actual value is the number of Entity Links currently configured on the security module. If these values do not match, perform the Synchronize action.
Certificate Used	Displays the details of the certificate type used.

Related Links

SIP Firewall status on page 443

Confirm Security Module Reset page field descriptions

Button	Description
Confirm	Resets the security module for the selected Session Manager instance. , Session Manager cannot process the calls while the security module is being reset.
Cancel	Cancels the resetting of the security module for the selected Session Manager

About Connection Status

Connection Status allows administrator to view current status of inbound and outbound links between Session Manager security module and external hosts. Use Connection Status to perform general-purpose monitoring and debugging activities, such as:

- Identification of whether Session Manager is required to be taken out of service
- Determination of whether links are secured or not
- Viewing of link details and statistics

Monitoring Connection Links

Procedure

1. On the System Manager console, under **Elements**, click **Session Manager**.
2. Click **System Status** > **Security Module Status** to open the Security Module Status page.
3. Select a system and click **Connection Status** to open the Connection Status page.
4. Apply the required filters using the **Connection Filter** section. Select the **Non-Compliant NIST TLS Only** check box to display only the TLS connections that are not compliant with NIST standards.
5. Under **Connection List**, click **Apply Filter** to display the list of connection links.
6. Select a row and click **Show** to view the detailed information about the selected connection.
7. Click **Return** to return to the Security Module Status page.

Connections Status field descriptions

Summary section

The Summary section displays the total number of Active Connections and the number of connections that are incoming, outgoing, TCP, and TLS.

Connection Filter section

Use the Connect Filter section to define a filter and to display the connection list based on the defined filters. A filter can be an FQDN or an IP Address and mask.

If you select the **Non-compliant NIST TLS Only** check box, the screen displays only the TLS connections having an algorithm that is not compliant with the NIST SP800-131A recommendation.

Connection List section

The Connection List table displays basic information of all the active connections. The following definitions apply to several of the fields:

- **A**: Acceptable. The algorithm and key length are safe to use. No security risk is currently known.
- **D**: Deprecated. The use of the algorithm and key length is allowed, but the user must accept some risk.
- **X**: Disallowed.
- **N**: Not approved.
- **R**: Restricted. The use of the algorithm or key length is deprecated, and there are additional restrictions required to use the algorithm or key length for applying cryptographic protection to data.
- **U**: Unknown. The system cannot determine the status.

Name	Description
Details	Show or hide the detailed information of the selected connection link.
Dir	Link direction (inbound or outbound).
Local Port	Local Security Module port.
Remote IP	Remote IP address.
Remote Port	Remote port.
Remote FQDN/IP	Remote FQDN or IP address.
Transport	Transport protocol (UDP, TCP, TLS).
Policy	Security Policy (Trusted, Default, Instance)
Cert Sign	Certificate Signature. Digital signature algorithms (for example, RSA or DSA) and the cryptographic hash function (for example, SHA) of the certificate in use by the TLS connection.
Key Exch	Key exchange algorithm (for example, RSA, DSA, Diffie-Hellman,) and key bit length (for example, 1024, 2048) to establish symmetric keys between the endpoints on the TLS connection.
Encryption	Cryptographic operation that provides confidentiality of the data being carried on the TLS connection.
MAC	Message Authentication Code algorithm (for example, SHA) that authenticates the TLS data and provides integrity and authenticity assurance on the message.

Connection Details section

The Connection Details section displays detailed information for the selected connection.

Name	Description
Direction	Link direction.
Creation time	Link creation time.
Last message received	Last message received time.
Last message sent	Last message sent time.
Messages/Bytes Received	Received message count and byte count.
Messages/Bytes Transmitted	Transmitted message count and byte count.
Messages/Bytes Dropped	Dropped message count and byte count.
Subject	The subject field identifies the entity associated with the public key stored in the subject public key field of the X.509 certificate.
Alt Subject	Alt subject is an extension to X.509 that allows various values to be associated with a security certificate.
CA	The issuer who signed the certificate.
Cipher	The negotiated TLS cipher suite. The cipher suite includes the Key Exchange, Encryption and MAC algorithms.
Public Key Algorithm	The encryption algorithm of the public key (e.g. RSA, DSA or Diffie-Hellman).
Key Size (bits)	The Public Key length.
q bits size	For DSA public keys, this represents the q parameter size.
Signature Algorithm	The identifier for the cryptographic algorithm used by the CA to sign this certificate.
MAC Algorithm	The Message Authentication Code (MAC) algorithm to verify data integrity.

SIP Firewall Status

Viewing SIP Firewall status

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **SIP Firewall Status** to open the SIP Firewall Status page.

Result

The SIP Firewall Status page shows the SIP Firewall processing status for each Session Manager and Branch Session Manager instances.

Auditing Firewall configuration

About this task

You can perform periodic audit of Firewall configuration to ensure the functioning state of the SIP Firewall. The audit operation checks for Rule Set upgrades and imports the latest default Rule Sets. The system also performs the audit operation automatically at every 5 minutes.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **SIP Firewall Status** to open the SIP Firewall Status page.
3. Click **Audit** to open the Rule Set Audit and Repair Results page.
4. Click **Done**.

Result

Rule Set Audit and Repair Results page shows the details of the SIP Firewall configuration state for all Session Manager and Branch Session Manager instances.

SIP Firewall Status page field descriptions

Button	Description
Reset	Resets all the processing counters of selected Session Managers and Branch Session Managers to zero, except for *Loop Detection* counters. Also, resets all the Rule matching counts to zero. **Note:** After a reset operation, the system updates the counts from the last reset time.
Audit	Performs sanity audit of the Session Manager Rule Set assignments. The Audit process also checks for Rule Set upgrades and imports pending default Rule Sets.
Configure	Navigates to the *SIP Firewall Configuration* page.

Name	Description
Details	Displays the detailed SIP Firewall processing status, for each Rule, of the selected Session Manager. *Rule Matching table* Name: Description Rule: The name of the Rule.

Table continues…

Name	Description
	Match: For the selected Session Manager, shows the matched count of the Rule. Drop: For the selected Session Manager, shows the dropped count of the Rule.
SM	The name of the Session Manager.
Type	Specifies the Session Manager type.
Rule Sets	The name of the Rule Set assigned to Session Manager.
Reset Time	The last reset time of the SIP Firewall processing counts. **Note:** Only Session Manager and Branch Session Manager of release 6.3.4 and later shows the reset time.
Processing Counts	Shows the summary of counts for Rules, Whitelist, Blacklist, and Loop Detection. Loop Detection counts do not reset. To view the exact counts, hover your mouse over the **Processing Counts** column. **Note:** Only Session Manager and Branch Session Manager of release 6.3.4 and later show the processing counts.

Related Links

Viewing SIP Firewall status on page 449

Registration Summary

Registration Summary

Use Registration Summary module to view the registration status for all Avaya SIP Telephony (AST) devices registered for the selected Session Manager Instance. These AST devices are reloaded or rebooted based on the following actions:

- Reset of endpoints
- Full reload of endpoints
- Partial reload of endpoints
- Failback of endpoints to the primary controller

Viewing Registration Summary

About this task

This module provides the ability to view the basic registration information for a particular device.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Registration Summary** to open the Registration Summary page.

   The Registration Summary page displays the list of registered devices per Session Manager.
3. Click **Refresh** to retrieve the latest Device Summary results.

Rebooting of selected AST devices

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Registration Summary** to open the Registration Summary page.

   The Registration Summary page displays the list of registered devices.
3. Select the AST Device and click **Reboot**.

   The system displays the Confirm Reboot Notification page.
4. On the Confirm Reboot Notification page, click **Confirm**.

   After user confirmation, a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

Reloading of selected AST devices

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Registration Summary** to open Registration Summary page.
3. Click the rows to select SIP AST devices and perform one of the following tasks:
   a. Click **Reload** > **Reload Complete** to force complete reload of selected SIP AST devices that includes maintenance data, configuration data, and a complete data reload.

      On the Confirm Reload Complete Notification page, click **Confirm**.

      After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.
   b. Click **Reload** > **Reload Config** to reload only configuration details of selected SIP AST subscribed devices.

On the Confirm Reload Config Notification page, click **Confirm**.

After user confirmation, the system displays a status page showing the detailed information regarding the current state of scheduled and running endpoint actions.

c. Click **Reload** > **Reload Contacts** to reload only contact details of selected SIP AST subscribed devices.

On the Confirm Reload Contacts Notification page, click **Confirm**.

After user confirmation, the system displays the status page showing the detailed information regarding the current state of scheduled and running endpoint actions.

Failback of selected AST devices

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Registration Summary** to open the Registration Summary page.

   The Registration Summary page displays the list of registered devices.
3. Click to select the AST Devices and click **Failback**.

   The system displays the Confirm Failback Notification page.
4. On the Confirm Failback Notification page, click **Confirm**.

Result

This enables failback to the primary Session Manager.

Advanced Searching

Procedure

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
Advanced Search Criteria	In the Advanced Search Criteria section, perform the following steps: a. Define the search criterion by performing the following steps: a. Select the search criterion from the first drop-down list box. b. Select the operator from the second drop-down list box. c. Enter the search value in the third field. b. If you want to add another search condition, click the plus sign (+). c. If you want to delete a search condition, click the minus sign (-) . d. Click **Clear** to clear the fields. e. Click **Search** to search as per the set search criteria. f. Click **Close** to contract the **Advanced Search Criteria** section.

Registration Summary field descriptions

Button	Description
Reboot	Reboots the selected Avaya SIP Telephony (AST) devices.
Reload Complete	Forces complete reload of the selected AST devices.
Reload Config	Reloads only configurations of the selected AST devices.
Reload Contacts	Reloads only contacts of the selected AST devices.
Failback	Ensures that devices failback to Primary Session Manager.

Name	Description
Session Manager	Name of the Session Manager instance.
Type	Either as Session Manager or Branch Session Manager (BSM).
Primary Registered	Number of users registered to this Session Manager as the primary Session Manager.
Primary AST	Number of PPM subscriptions to this Session Manager for users as the primary Session Manager.
Primary Admin	Number of users administered to use this Session Manager as the primary Session Manager. **Note:** Session Manager of type **BSM** does not have any registration status entries in the Primary column group and the system displays the status as “---”.
Secondary Registered	Number of users registered to this Session Manager as the secondary Session Manager.
Secondary AST Failover	Number of PPM subscriptions to this Session Manager for users as the secondary Session Manager. This also indicates the failover users since failover users subscribe to the secondary Session Manager.
Secondary Admin	Number of users administered to use this Session Manager as the secondary Session Manager.
Total Registered	Sum of fields **Primary Registered** and **Secondary Registered**.
Total AST	Sum of fields **Primary AST** and **Secondary AST Failover**.
Total Admin	Sum of fields **Primary Admin** and **Secondary Admin**.

User Registrations

User Registrations

The User Registrations module sends notification to the selected SIP AST devices and displays the summary of the user registration status for the SIP AST Device based on the following actions:

- Forced termination of registrations for selected devices
- Reset of selected devices
- Full reload of selected devices
- Only reload configuration for selected devices
- Only reload contacts for selected devices
- Failback of devices to the primary controller

Viewing User Registrations

About this task

Use the User Registrations module to view the basic registration information for a particular user or groups of users.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open User Registrations page.

   The User Registrations page displays the list of registered users.
3. To view the User Registration status based on the following view options, click **View** and select the one of the viewing options.

User	For viewing current default view.
Time Detail	For viewing diagnosis of endpoint registration oriented problems.
Device	For viewing all available device specific information.
Active Controller	For viewing more detailed registration time view.
SM	For viewing that Session Managers are associated with the user registration.
Customized	For viewing custom views.
Create Customized	For customizing the display columns for viewing the user registration details.

4. To view individual row details, click the **Show** or **Hide** link under **Details** column to display or hide the details that have the following tabbed panes:

User	For viewing user specific details.

Registration	For viewing the registration specific details.
Device	For viewing device specific details.
Simultaneous	For viewing details of simultaneous registered devices.
History	For viewing the details of current and past AST devices associated with this user.

5. Click **Refresh** to retrieve the latest user registration summary results.

Customizing column display

About this task

You can customize the column display on the User Registrations page. Use any of the following methods to customize a column display:

- Select the columns you need to get displayed in the table
- Order the appearance of the columns
- Reset the column appearance to the default columns

Note:

The customization settings are valid for the current user session, that is, after the user logs out, the customization settings revert to the default appearance.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open User Registrations page.
3. Click **Customize** link to view this section.
4. Select columns in **Available Columns** and click the **Move** link to move the selected columns to **Display Columns** list. Click **Move All** link to move all columns to be displayed.
5. Click **Remove** and **Remove All** links to remove selected or all columns from displayed columns.
6. To rearrange the selected columns under **Display Columns**, perform the following steps:
   a. Click the **Top** link to move the selected column to the top of the list.
   b. Click the **Up** link to move the selected column one position up on the list.
   c. Click the **Down** link to move the selected column one position down on the list.
   d. Click the **Up** link to move the selected column to the bottom of the list.
7. Click **Default** to restore the default settings.
8. Click **Apply** to save the changed settings.
9. Click **Close** to close the customization section.

Forcing unregistration of device registration

About this task

This feature enables forced unregistration of any registered device and is not limited to only AST devices. These devices respond based on device settings.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open the User Registrations page.

   The User Registrations page displays the list of registered devices.
3. Select the device and click **Force Unregister**.

   The system displays the Confirm Force Unregister Notification page.
4. On the Confirm Force Unregister Notification page, click **Confirm**.

   After user confirmation, a status page appears showing the detailed information of the unregistration action.

Rebooting of selected AST devices

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open User Registrations page.

   The User Registrations page displays the list of registered users.
3. Click to select the AST Devices and click **Reboot**. The Confirm Reboot Notification page appears.
4. On the Confirm Reboot Notification page, click **Confirm**.

   After user confirmation, a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

Reloading of selected AST devices

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open User Registrations page.
3. Click the rows to select the SIP AST Devices and do one of the following:
   a. Click **Reload** > **Reload Complete** to force complete reload of selected SIP AST Devices that includes maintenance data, configuration data, and a complete data reload.

On the Confirm Reload Complete Notification page, click **Confirm**.

After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

b. Click **Reload** > **Reload Config** to reload only configuration details of selected SIP AST subscribed devices.

On the Confirm Reload Config Notification page, click **Confirm**.

After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

c. Click **Reload** > **Reload Contacts** to reload only contact details of selected SIP AST subscribed devices.

On the Confirm Reload Contacts Notification page, click **Confirm**.

After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

Failback of selected AST devices

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open User Registrations screen. The User Registrations screen displays the list of registered users.
3. Click to select the AST Devices and click **Failback**. The Confirm Failback Notification page appears.
4. On the Confirm Failback Notification page, click **Confirm**.

Result

This enables failback to the primary Session Manager.

Advanced Searching

Procedure

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
Advanced Search Criteria	In the Advanced Search Criteria section, perform the following steps: a. Define the search criterion by performing the following steps: a. Select the search criterion from the first drop-down list box. b. Select the operator from the second drop-down list box. c. Enter the search value in the third field. b. If you want to add another search condition, click the plus sign (+). c. If you want to delete a search condition, click the minus sign (-) .

Table continues…

	d. Click **Clear** to clear the fields. e. Click **Search** to search as per the set search criteria. f. Click **Close** to contract the **Advanced Search Criteria** section.

User Registrations field descriptions

Customize Column Display section

List	Description
Available Columns	Shows the list of available columns.
Display Columns	Shows the list of selected columns.

Link	Description
Customize	Expands **Customize Column Display** section.
Move	Moves selected items from **Available Columns** list to the **Display Columns** list.
Move All	Moves all items from **Available Columns** list to the **Display Columns** list.
Remove	Removes selected items from the **Display Columns** list.
Remove All	Moves all items from the **Display Columns** list.
Top	Moves the selected items of **Display Columns** list to the top of the list.
Up	Moves the selected items of **Display Columns** list to one position up in the list.
Down	Moves the selected items of **Display Columns** list to one position down in the list.
Bottom	Moves the selected items of **Display Columns** list to the bottom of the list.

Button	Description
Default	Reverts back to the default column settings of **Available Columns** and **Display Columns** lists.
Apply	Applies the changes made in the column customizing lists to the **AST Device Notifications** section.
Close	Collapses **Customize Column Display** section.

AST Device Notifications: section

The **As of (time)** label indicates the time of the last update of information for the **AST Device Notifications** section.

Button	Description
View > **Default**	For viewing current default view.
View > **User**	For viewing the user specific information.
View > **Time Detail**	For viewing diagnosis of endpoint registration oriented problems.
View > **Device**	For viewing all available device specific information.
View > **Active Controller**	For viewing registration information of the actively controller Session Manager for AST devices.
View > **SM**	For viewing which Session Managers are associated with the user registration.
View > **Customized**	For viewing custom views.
View > **Create Customized**	For customizing the display columns for viewing the user registration details.
Force Unregister	Forces termination of registrations for selected devices.
Reboot	Reboots selected AST devices.
Reload Complete	Forces complete reload of selected AST devices.
Reload Config	Reloads configurations of selected AST devices.
Reload Contacts	Reloads contacts of selected AST devices.
Failback	Enable devices to failback to Primary Session Manager.

Default View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
First Name	Shows the administered first login name.
Last Name	Shows the administered last login name.
Actual Location	Name of the registration location.
IP Address	Indicates numeric IP address of the end point.
Remote Office	Shows whether the incoming IP Address has been correlated with an administered "Remote Office - SIP Proxy Mapping".
Shared Control	Indicates that this registration, like Avaya OneX Communicator, controls another endpoint.
Simultaneous Devices	Number of devices registered and the maximum administered devices.
AST Device	Indicates an AST device.

Table continues…

Name	Description
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

User View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
First Name	Shows the administered first login name.
Last Name	Shows the administered last login name.
Home Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
IP Address	Indicates numeric IP address of the end point.
Simultaneous Devices	Number of devices registered and the maximum administered devices.
AST Device	Indicates an AST device.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

Time Detail View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
IP Address	Indicates numeric IP address of the end point.
PPM Subscription Time (AC)	Indicates the subscription time for PPM services of AST endpoint.
Registration Time Prim	Indicates the registration time for the Primary Session Manager.
Registration Interrupted Prim	Indicates the last time when the registration was interrupted for the Primary Session Manager.
Registration Time Sec	Indicates the registration time for the Secondary Session Manager.

Table continues…

Name	Description
Registration Interrupted Sec	Indicates the last time when the registration was interrupted for the Secondary Session Manager.
Registration Time Surv	Indicates the registration time for the Survivable Session Manager.
Registration Interrupted Surv	Indicates the last time when the registration was interrupted for the Survivable Session Manager.

Device View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
IP Address	Indicates numeric IP address of the end point.
Remote Office	Indicates whether the incoming IP address correlates with an administered Remote Office — SIP Proxy Mapping.
MAC Address	MAC address of the endpoint.
Device Vendor	Device information from PPM.
Device Type	Device information from PPM.
Device Model	Device information from PPM.
Device Version	Device information from PPM.
Simult. Devices	Number of devices registered to the maximum number administered.

Active Controller View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
Actual Location	Name of the registration location.
Active Controller	Name of the Active Controller
Registration Time (AC)	Indicates the registration time for the Active Controller.
Registration Interrupt Time (AC)	Indicates the time duration since the last interruption occurred for the Active Controller.
Registration Interrupted (AC)	Indicates the last time when the registration was interrupted for the Active Controller.

Table continues…

Name	Description
AST Device	Indicates an AST device.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

SM View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
Home Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
Actual Location	Name of the registration location.
Active Controller	Name of the Active Controller
Primary SM	Primary Session Manager of the user profile.
Secondary SM	Secondary Session Manager of the user profile.
Survivable SM	Survivable Session Manager of the user profile.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

Customized View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
First Name	Shows the administered first login name.
Last Name	Shows the administered last login name.
Home Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
IP Address	Indicates numeric IP address of the end point.
Simultaneous Devices	Number of devices registered and the maximum administered devices.
AST Device	Indicates an AST device.
Registered Prim	Indicates as primary registration.

Table continues…

Name	Description
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

`Create Customized view is same as Customize Column Display section as shown above.`

Details section

User Tab:

Name	Description
First Name	Shows the administered first login name.
Last Name	Shows the administered last login name.
Login Name	Shows the administered user login name.
Registration Address	The Communication Address/handle user logged in with.
All Addresses	All of the SIP Communication Addresses the user has administered.
Home Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
Actual Location	Name of the registration location.
Primary SM	Primary Session Manager of the user profile.
Secondary SM	Secondary Session Manager of the user profile.
Survivable SM	Survivable Session Manager of the user profile.
Simultaneous Devices	Number of devices registered to the maximum number administered.
ELIN Number	The ELIN sent from ELIN server associated with the primary controller for a user.
ELIN Last Updated	The date and time that the ELIN was last updated by ELIN server based on the location of Session Manager. Format is: www mmm dd hh:mm:ss TMZ yyyy", where: • www implies day of the week • mmm implies month • dd implies date • hh:mm:ss implies hour (military time):minutes:seconds • TMZ implies time zone • yyyy implies year For example, Fri Feb 11 15:56:36 MST 2011.

Registration Tab:

Name	Description
Registration Address	The Communication Address/handle user logged in with.
IP Address	Indicates numeric IP address of the end point.
Active Controller	Session Manager currently serving the endpoint SIP signaling and event subscriptions.
PPM Subscription Time (AC)	Indicates the subscription time for PPM services of AST endpoint.
Event Subscriptions	Event subscription details.
Instance Id	SIP User Agent Instance Id as URN (Uniform Resource Name):UUID (Universally Unique IDentifier).
Primary Registration Time	Indicates the registration time for the Primary Session Manager.
Primary Registration Interrupted Time	Indicates the time duration since the last interruption occurred for the Primary Session Manager.
Primary Registration Interrupted	Indicates the last time when the registration was interrupted for the Primary Session Manager.
Secondary Registration Time	Indicates the registration time for the Secondary Session Manager.
Secondary Registration Interrupted Time	Indicates the time duration since the last interruption occurred for the Secondary Session Manager.
Secondary Registration Interrupted	Indicates the last time when the registration was interrupted for the Secondary Session Manager.
Survivable Registration Time	Indicates the registration time for the Survivable Session Manager.
Survivable Registration Interrupted Time	Indicates the time duration since the last interruption occurred for the Survivable Session Manager.
Survivable Registration Interrupted	Indicates the last time when the registration was interrupted for the Survivable Session Manager.

Device Tab:

Name	Description
MAC Address	MAC address of the endpoint.
IP Address	Indicates numeric IP address of the end point.
Remote Office	Indicates whether the incoming IP address correlates with an administered Remote Office — SIP Proxy Mapping.
Remote Office SIP Proxy Name	Name of the SIP Proxy.

Table continues…

Name	Description
Active Controller	Name of the Active Controller
Event Subscriptions	Event subscription details.
AST Device	Indicates an AST device.
Device Vendor	Device information from PPM.
Device Type	Device information from PPM.
Device Model	Device information from PPM.
Device Version	Device information from PPM.

Simultaneous Tab:

Shows all other registrations associated with this user.

Name	Description
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
IP Address	Indicates numeric IP address of the end point.
MAC Address	MAC address of the endpoint.

History Tab:

Shows up to 10 of the last device registrations performed by this user.

Name	Description
MAC Address	MAC address of the endpoint.
Vendor	Device information.
Type	Device information.
Model	Device information.
Version	Device information.

Session Counts

SIP sessions count

Session Manager Element Manager collects, monitors, and logs the number of concurrent SIP sessions in the system. As the total number of session licenses used is equal to the number of concurrent SIP sessions, you can use the SIP sessions count feature to monitor and report the number of session licenses used by the system.

The system raises an alarm in the following conditions:

- In the case of a single occurrence of an event where the number of concurrent SIP INVITE sessions exceeds the authorized number of session licenses.

- If the number of concurrent SIP INVITE sessions in use continues to exceed the number of authorized licenses. In this condition, the system raises a new alarm once every 24 hours until either the number of concurrent SIP INVITE sessions is reduced below the number of authorized licenses or the number of authorized licenses is increased to be equal to or greater than the number of concurrent SIP INVITE sessions.

  Note:

  The system raises an alarm if a valid license file is not installed on the system.

SIP sessions count functionality enables historical analysis of SIP sessions count data for the system or the selected Session Manager instance and allows:

- The generation of graphs of the analyzed data.
- The export of the analyzed data as a report in the comma separated value (CSV) or XML format.

Using the generated reports, you can conduct a time based analysis of the license usage of the system.

Viewing Session Count data

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Session Counts** to open the Session Counts page.
3. In the **Session Manager** field, select the Session Manager instance.
4. Specify the date and time for the required period of the session counts data.
5. Click **Generate Graphs** for viewing the data in graphical format.

Exporting analyzed Session Count data

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Session Counts** to open the Session Counts page.
3. Select the required Session Manager instance.
4. Specify the date and time for the required period of the session counts data.
5. Specify **Export Data Range** and **Export Data Format**.
6. Click **Download Data** to save a copy of the generated report.

Session Counts field descriptions

Name	Description
Global Session Status as of	Indicates when the session count data was last updated.
Sessions Used	The number of SIP sessions currently used by the system.
Sessions Available	The number of SIP sessions authorized for usage by the system.
Session Manager	The Session Manager instance or all Session Manager instances for which session count data is desired.
Data Available	The period for which session count data is available.
Date and Time	The period of the session count data. Predefined values: 1. all dates and times • last month • last week • today • yesterday 2. Last: 1-99 Days or Hours 3. Between: Specified Date Range
Generate Graphs	Generates session count graphs based on specified parameters.
Export Data Range	The period for which session count data must be exported: • All – Retrieve all data for specified Session Manager. • Selected Range – Retrieve data based on the Date and Time field selection.
Export Data Format	The format of downloaded session count data: CSV or XML.
Download Data	Exports session count data based on the specified parameters.

User Data Storage status and Call History management

Use the User Data Storage status screen to manage, monitor, backup, and restore User Data Storage on Session Managers.

User Data Storage only stores the call logs of a user.

Note:

The User Data Storage backup is *not* related in any way to the System Manager backup.

Viewing the User Data Storage Status screen

Procedure

On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.

Data Server Status field descriptions

The Data Server Status screen displays the status of the User Data Storage data server.

The User Data Storage **Status** on the Session Manager can be one of the following states:

- Normal Operation
- Auditing: Call History information is being audited and obsolete data is being removed.
- Restoring: User Data Storage is being restored from a backup server file.
- Backing Up: An on-demand or automated backup is in progress.
- Needs Repair: A Restore action has failed.

Name	Description
Details	Show or hide the details of the last action that was performed on the Session Manager.
SM	Name of the core Session Manager.
Status	Current state of the User Data Storage on the Session Manager.
Connect Test	Status of the maintenance connection test to the User Data Storage server.
Last Action	The last action performed on the User Data Storage server. An action can be: • Audit • Backup • Restore • Recreate
Last Action Status	Result of the last action performed (Complete or Failed).
Last Action Time	The requested or completion time of the **Last Action** .
Disk Usage	Cumulative disk usage for data storage.

User Data Storage backup

Backups and audits run on a daily basis at 1:15 AM local time on the Session Manager. The backup server audit removes extra backup files at 2:15 AM local time on the System Manager.

The User Data Storage backup feature:

- is *not* related in any way to the System Manager backup.
- does not pre-allocate space. The administrator must administer a location for backup files. 4 GB of space is adequate for this release, but more space will need to be allocated over time.
- makes a backup directly from the Session Manager to the backup location.
- backs up call history data only.

If the user does not configure a backup server:

- a warning message displays until the user configures a backup server location.
- no backups are made.
- the status page displays that no backup server is configured.

Backup and Restore field descriptions

Use this screen to configure and monitor User Data Storage backups and recoveries. The backup server must be in place before configuring the backup information.

The fields display **- -**:

- If the system cannot retrieve the status of a Session Manager.
- If the Session Manager is running a release earlier than 6.3.8.

Backup Host	Name of the backup server.
File Transport	Type of file transport in use.
Directory	Location on the backup server to store the backup files.
Directory Disk Used	Amount of disk space used for the backup file
Retained Copies	Number of backup copies saved on the backup server per Session Manager.

Button	Description
Backup	Start the backup process on the selected Session Managers.
Restore	Start the restore process on the selected Session Managers.
Configure Backup	Configure backup server location and directory for backup file storage.
Audit Backup	Audit the backup configuration, status, and directory. Provides an option to remove unnecessary files to reclaim disk space.

Name	Description
Details	Show or hide the backup file details for a selected Session Manager (File Name, Backup Date, File Size, Session Manager Release).
SM	The name of the core Session Manager.
Backup Status	Indicates the status of the last backup (Complete or Failed).
Backup Files	The number of backup files that are stored on the backup server for the selected Session Manager.
Last Backup Time	The time a backup was last run on the selected Session Manager.
Last Restore Status	The status of the last Restore request on the selected Session Manager (Complete or Failed).
Last Restore Time	The time a restore request was last run on the selected Session Manager.

Administering Backup Storage Configuration

Use the Backup Storage Configuration screen to create or change the backup server configuration information.

Backups and audits run on a daily basis at 1:15 AM local time on the Session Manager. The backup server audit removes extra backup files at 2:15 AM local time on the System Manager.

Important:

The backup server must support the SSH2 protocol.

Warning:

If you change the server or backup file location directory using this screen, existing backup files are not automatically moved to the new location and are not available for restoring. The user must move the backup files to the new location and remove files from the unused location.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Backup and Restore**.
3. Click **Configure Backup**.
4. Enter the required information. See Backup Storage Configuration field descriptions on page 536.
5. Do one of the following:
   - Click **Commit** to save the configuration changes.
   - Click **Test Connection** to verify the configuration information is correct.
   - Click **Cancel** to cancel the configuration request.

Backup Storage Configuration field descriptions

Button	Description
Commit	Accept and store the configuration changes to the database.
Test Connection	Test the SSH connection, directory access for the login, and write/delete permissions.
Cancel	Do not make any changes to the existing configuration information.

Name	Description
Hostname or IP Address	Hostname or IP address of the SSH-accessible server.
Login	The login that has SSH privileges and can gain access to the server.
Password **Confirm Password**	The password associated with the login.
Backup File Transfer	The default is **SFTP**. **SCP** is a slightly faster transport but can be affected by interrupts.
SSH Port	The default is 22.
Directory	The directory location where backup files are stored on the backup server.
Retained backup copies per SM	The maximum number of backup file copies retained for each Session Manager on the backup location.

Backing up User Data Storage

Run the backup immediately. Running the backup on demand does not alter the nightly backup schedule.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Backup and Restore**.
3. Select the Session Manager or multiple Session Managers on which to run the backup.
4. Click **Backup**.
5. Click **Confirm** to start the backup process, or **Cancel** to cancel the backup request.

Restoring User Data Storage

The restore operation:

- Only restores call history information that exists in a backup file.
- Deletes call history information that exists only in the database.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Backup and Restore**.
3. Select the Session Manager on which to run the restore operation.
4. Click **Restore**.
5. In the **Restore File** column, select the appropriate file you want to restore from the drop-down menu.
6. Do one of the following:
   - Click **Commit** to accept the selection.
   - Click **Reset** to reload the **Restore File** selection list.
   - Click **Cancel** to cancel the restore request and return to the User Data Storage screen.
7. Click **Confirm** to send a request to each Session Manager to begin the restore operation using the selected file, or click **Cancel** to cancel the restore request.

Auditing a Backup Storage Location

The audit runs on the backup server and provides a summary status of the backup server and files.

The Audit Backup Storage Location screen also displays the files which will be removed in the next nightly audit. If not enough disk space is currently available, the administrator can click **Remove Pending** to immediately remove the pending files on the backup server.

Backups and audits run on a daily basis at 1:15 AM local time on the Session Manager. The backup server audit removes extra backup files at 2:15 AM local time on the System Manager.

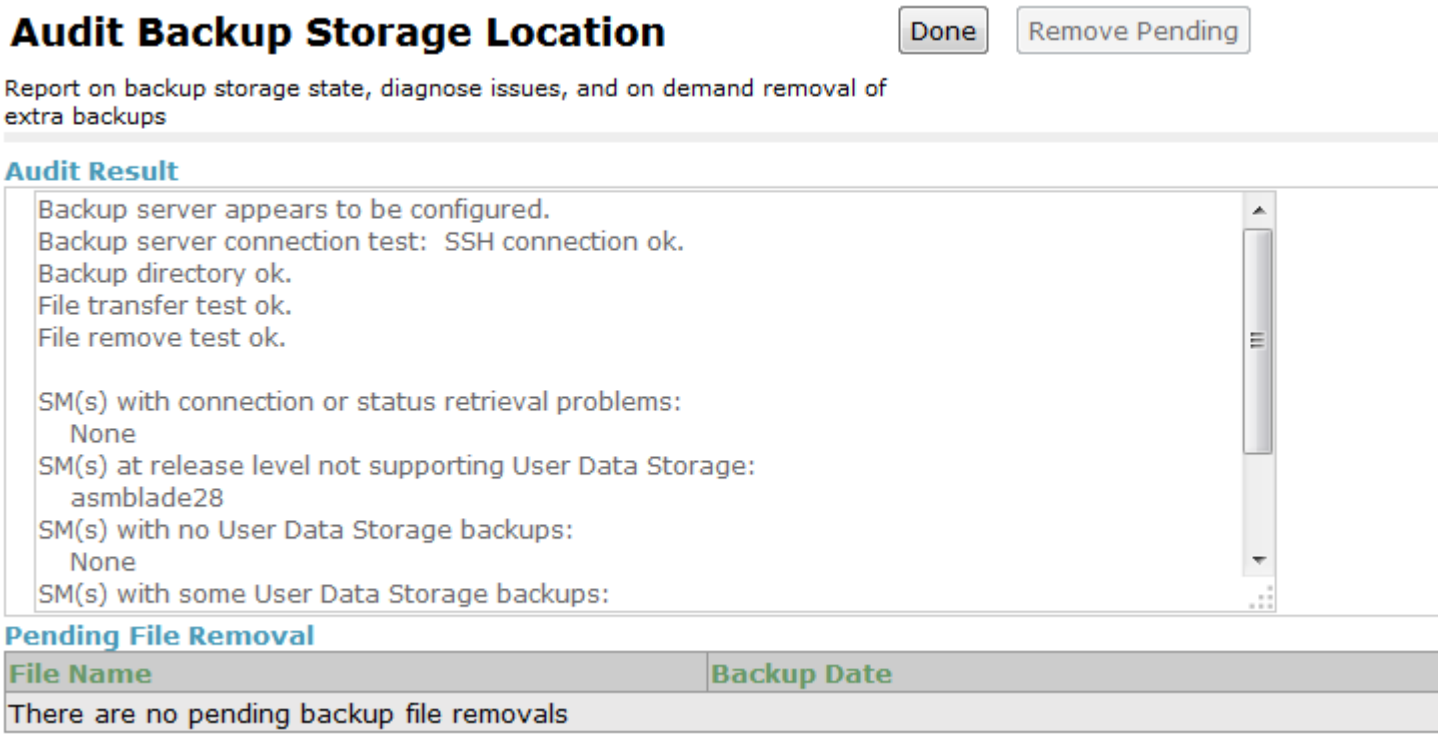
Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Backup and Restore**.
3. Select a Session Manager from the **SM** list.
4. Click **Audit Backup**.

   The system displays the results of the audit.
5. To immediately remove any files listed under **Pending File Removal**, click **Remove Pending**.
6. Click **Done**.

Example

The audit displays results similar to the following:



Call History

Starting with Session Manager Release 6.3.8, logged out missed call information is saved for both H.323 and SIP endpoints.

- For H.323 endpoints, Communication Manager stores logged out missed calls and downloads the Call History logs when the endpoint logs in.
- For SIP endpoints, the primary Session Manager stores all call logs and downloads the logs to the endpoint during login. The endpoint maintains the logs locally while logged in. Call logs are only stored on the primary Session Manager of the user. No call logs are stored on the secondary Session Manager for the user. Call log storage is not redundant..

You control Call History logging for the SIP user by selecting or deselecting the **Enable Centralized Call History** check box on the Session Manager Communication Profile screen. The check box is deselected by default (disabled). The maximum number of call logs for each Communication Profile is 100. You cannot configure the maximum number of call logs.

Administering Call History

Enable or disable call history collection for a user.

Warning:

When a user logs in for the first time after the **Centralized Call History** check box is selected for that user, all calls that were made or received by that user before enabling **Centralized Call History** are lost.

Procedure

1. On the home page of the System Manager Web Console, under **Users**, click **User Management** > **Manage Users**.
2. Do one of the following:
   - If you are adding a new user, click **New** and add the information for the new user.
   - If you are enabling/disabling call history collection for a current user, select the user and click **Edit**.
3. On the User profile Edit: screen, click the **Communication Profile** tab.
4. Select the **Session Manager Profile** checkbox.
5. Under the **Call History Settings** section, select (enable) or clear (disable) the **Enable Centralized Call History?** check box.
6. Click **Commit**.

Administering Call History for SIP users with the Communication Profile Editor

You can bulk enable or disable the call history collection for all SIP users or selected SIP users.

Warning:

When a user logs in for the first time after the **Centralized Call History** check box is selected for that user, all calls that were made or received by that user before enabling **Centralized Call History** are lost.

Procedure

1. On the System Manager web console home page, under **Elements**, click **Session Manager** > **Communication Profile Editor**.
2. Select a user, select multiple users, or select **All**.
3. In the **New Communication Profile Values** section, under **Call History Settings**, select a value from the **Enable Centralized Call History** drop-down menu.
4. Click **Commit**.

Viewing the Call History Status screen

Use this screen to manage and monitor call history tables in the User Data Storage database.

An audit runs every night at 1:15 a.m. local time to the Session Manager. The audit deletes the call history logs of a user who is permanently deleted or is assigned to another Session Manager.

The audit compacts the table storage after it completes.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Call History Status**.

Call History Status field descriptions

Button	Description
Audit	Audit the call history and remove entries for deleted users, users with deleted Session Manager Communication Profiles, and users who have been reassigned to another Session Manager. Compact the data storage table after removing the affected files.

Name	Description
Details	Show or hide the Call Log Table details for a selected Session Manager.
SM	The name of the core Session Manager.
Last Audit	The time when an audit process last ran. Audits run nightly or on-demand.
Call Log Records	The total number of records in the Call Log table.
Call Id Records	The total number of records in the Call Log Id table.
Primary SIP Users	Number of SIP users assigned to the Primary Session Manager.
Call History Users	The number of users who have Call History enabled in their Session Manager Communication Profile.

System Tools

Session Manager maintenance tests

Use the Maintenance Tests page to perform tests on the System Manager server and the configured Session Managers. The tests verify functionality such as network connectivity, data replication, and database operation. The system runs the tests periodically to monitor the status of system components. You can also run the tests on demand.

Note:

Tests can fail if the server under test is out of service or is not responding.

Maintenance Tests page field descriptions

Name	Description
Select System Manager or Session Manager to test:	Select a System Manager or a Session Manager from the drop-down menu on which to perform the maintenance tests.

Button	Description
Execute Selected Tests	Run the selected maintenance tests on the selected System Manager or Session Manager.
Execute All Tests	Run all the maintenance tests on the selected System Manager or Session Manager.

Name	Description
Test Description	Description of the test.
Test Result	The outcome of executing the test (pass or fail).
Test Result Time Stamp	The last time the test was run.

Note:

The system loads Maintenance test data asynchronously in the background. The system displays the message **Loading..** when data is loading in the background. The system displays the message **Loading Complete** when data loading finishes. If the wait time exceeds a certain limit, the system displays the message **Loading failure. Please try again.** and requests the user to try again later.

Running maintenance tests

Run the maintenance tests on the current System Manager or any configured Session Manager.

Procedure

1. On the System ManagerWeb Console, under **Elements**, select **Session Manager** > **System Tools** > **Maintenance Tests**.
2. In the **System Manager or a Session Manager to test** field, select **System Manager** or a Session Manager instance from the drop-down menu.
3. To run all of the tests, select **Execute All Tests**.
4. To run only certain tests:
   a. Select the test to run from the test list.
   b. Click **Execute Selected Tests**.
5. Verify the tests pass.

Maintenance Test descriptions

Test Call Processing status

This test checks the call processing functionality for a particular Session Manager instance. If call processing is working correctly, the test passes. If the test fails, contact Avaya Technical Support.

Test data distribution and redundancy link

This test only runs on Session Manager. This test verifies the Session Manager data share mechanism is functioning properly by sending a test string to each configured Session Manager. Each Session Manager saves the test string Session Manager within its respective database. After a short wait, the system queries each Session Manager for the test string value.

The test passes if each Session Manager returns the correct value.

A test failure indicates a potential failure of link redundancy and Session Manager pass-through capabilities that could impact call processing and Call Admission Control.

The test does not run on a Session Manager if the state of the Session Manager is **Deny New Service**.

Test host name resolution of each Session Manager

This test only runs on System Manager. The test verifies that the DNS server can resolve the host name of each configured Session Manager.

If the DNS server can resolve the host name for each Session Manager, the test passes. Otherwise, the test fails. Check for the following possible causes:

- The Session Manager host name is incorrect on the DNS server.
- The Session Manager host name is missing on the DNS server.

Test management link functionality

This test checks the administrative link to the Session Manager. If the test fails, administrative changes cannot take effect on Session Manager. .

Test Postgres database sanity

This test runs on either System Manager or aSession Manager.

System Manager tests the functionality of the master database.

The Session Manager tests the functionality of the local instance database.

If the test fails, contact Avaya Technical Support.

Test sanity of Secure Access Link (SAL) agent

This test can run on either System Manager or Session Manager. It checks if the Security Access Link agent is running or not on the server. If the link is up and running, the test passes.

If the test fails, run the **statapp** command and other corrective actions for associated alarms on Session Manager before escalating to Avaya Technical Support.

Test Security Module Status

This test queries the status of the Security Module on a specified Session Manager. If the query is successful, the test passes. Otherwise, the test fails.

Test network connections to each Session Manager

The Network Connections test runs only on System Manager. This test verifies the connectivity to each administered Session Manager.

If connectivity is up for each Session Manager, the test passes. If connectivity is down, the test fails. The following are possible causes of test failure:

1. An upgrade or install is in progress.
2. The server might be out of service. Check the log for an event code, then check the Log Event Codes in *Maintaining and Troubleshooting Avaya Aura® Session Manager* for the appropriate troubleshooting action.
3. The network might be out of service. Run a ping test between System Manager and the failing Session Manager to verify network connectivity.

Test User Data Storage sanity

Note:

This test is not available for:

- Branch Session Managers
- Session Managers that are running a release earlier than 6.3.8.

This test checks the status of the **Cassandra** application and the connectivity to the **Cassandra** database. The test passes if the application and the connectivity are operating correctly. The test fails otherwise.

SIP Tracer Configuration

About Tracer Configuration

You can use the Tracer Configuration page to configure the tracing of SIP messages incoming through the security module, SIP messages outgoing from the security module, and also messages dropped by ASSET proxy or by the SIP firewall.

You can also filter these messages based on the user or the call. Session Manager logs all the traced messages to a file based on the configuration.

Tracer Configuration page field descriptions

Tracer Configuration

Name	Description
Tracer Enabled	SIP message tracing is enabled by default.
Trace All Messages	SIP message tracing is enabled for all SIP messages. In this case, other fields get disabled.
From Network to Security Module	SIP message tracing is enabled for ingress calls sent to the Session Manager instance from the network.
From Security Module to Network	SIP message tracing is enabled for egress calls originating from the Session Manager instance and sent to the network.
From Server to Security Module	Local SIP messages originating from Session Manager.
From Security Module to Server	Local SIP messages originating from the security module.
Trace Dropped Messages	SIP message tracing is enabled to trace messages from calls dropped by the SIP firewall as well as by the SM100 proxy.
Max Dropped Message Count	Shows the value for the maximum number of traced dropped messages, if Dropped check box is activated.
Send Trace to a Remote Server	Enables or disables SIP Tracing to an external host . This enables Session Manager to send all the (decrypted) SIP traffic out to an external host. Session Manager uses Syslog protocol for sending the SIP traffic (as used currently for SIP Tracing).
Remote Server FQDN or IP Address	FQDN or IP address of the remote syslog server.
Send Trace Method	Method used to transfer syslogs either using Stunnel (encrypted TCP) or Syslog (unsecure UDP) as mentioned below: • Syslog (unsecured UDP) : Traffic is send without being encrypted to remote server as specified in the “Remote Server FQDN or IP Address” to default syslog port. • Stunnel (encrypted TCP) : Traffic is send as encrypted (using stunnel) to remote server that is specified in the “Remote Server FQDN or IP Address” to the port specified in the input field ”Stunnel Port”.
Stunnel Port	Port number that remote server's stunnel is listening on. Stunnel provides several modes for far end certificate validation.

User Filter

Button	Description
New	Create a new filter for filtering SIP messages based on the users. You can define a maximum of three user filters.
Delete	Delete a selected user filter or filters.

Name	Description
From	Filter SIP messages based on the user from whom the message is sent. Type the user string. For example, a rule to trace all messages from user “pqr”: to=”” from=”pqr” stop-count=50
To	Filter SIP messages based on the user to whom the message is sent. Type the user string. For example, a rule to trace all messages to user “xyz”: to=”xyz” from=”” stop-count=50
Source	Filter SIP messages based on the source address.
Destination	Filter SIP messages based on the destination address.
Max Message Count	Value for maximum number of messages matching the filter that Session Manager should trace. Default is 25 messages.

Call Filter

Button	Description
New	Create a new filter for filtering all SIP messages that start a new call. You can define a maximum of three call filters.
Delete	Delete a selected call filter or filters.

Name	Description
From	Filter SIP messages from a specific user. Call tracing identifies a call by capturing the Call ID from the first message that matches the From filter, thereafter tracing all the messages that have the matching call ID. For example, a rule to trace all messages related to a CALL from user “pqr”: to=”” from=”pqr” request-uri=”” stop-count=50

Table continues…

Name	Description
To	Filter SIP messages based on the user to whom the message is sent. Call tracing identifies a call by capturing the Call ID from the first message that matches the To filter, thereafter tracing all the messages that have the matching call ID. For example, a rule to trace all messages related to a CALL to user “xyz”: to=”xyz” from=”” request-uri=”” stop-count=50
Source	Filter SIP messages based on the source address.
Destination	Filter SIP messages based on the destination address.
Max Call Count	Value for maximum number of messages matching the filter that Session Manager should trace. Default is 25 messages.
Request URI	Filter calls based on the called party (URI address). A valid Request URI format, for example, is .@192.111.11.111.

Session Manager Instances

Name	Description
Name	Select one or more configured Session Managers for which the specific filters should be used. **Note:** If you select only one Session Manager from this list, the **Read** button is activated. Click this button to retrieve the current Trace Configuration details for the selected Session Manager and display that within the Trace Configuration page. After displaying the configuration, Session Manager closes the display so that no older configuration data is displayed.

Button	Description
Commit	Save the configuration changes.
Read	Retrieves the current Trace Configuration details for the selected Session Manager and display that within the Trace Configuration page.

SIP Trace Viewer

About SIP Tracing

Use the SIP tracer to trace SIP messages exchanged between the Session Manager server and remote SIP entities. SIP messages that are dropped by any of the SM100 components such as SIP Firewall are also logged by the SIP tracer. You can trace all the messages belonging to a user, for a call, or for a selected Session Manager instance. The SIP tracer provides statistics of SIP messages within the SM100 framework. SIP tracer is located under Session Manager on the System Manager Common Console navigation pane. SIP tracer user interface has the following components:

- Tracer Configuration defines the characteristics of messages to be traced for the capturing engine in the security module.
- Trace Viewer displays the captured SIP messages.

For details, refer to the section Tracing in *Maintaining and Troubleshooting Avaya Aura® Session Manager* (03-603325)

Trace Viewer page field descriptions

Use the From and To fields to specify a range of days or time as follows:

Filter

Name	Description
From: Date	Date from which you want to filter the trace logs.
From: Time	Time from which you want to filter the trace logs.
From: Time Zone	Time Zone for the From date that you want to use for filtering trace logs.
To: Date	Date up to which you want to filter the trace logs.
To: Time	Time up to which you want to filter the trace logs.
To: Time Zone	Time Zone for the To date that you want to use for filtering trace logs.
Name	Name of the Session Manager instance.

Trace Viewer

Button	Description
Dialog Filter	Filters trace log entries. Select a trace log and click **Dialog Filter**. This option filters trace log entries and displays entries for the same Call ID, From, and To fields as the trace log that you select.

Table continues…

Button	Description
	Note: You can also click Filter: **Enable** to filter log entries based on a value or to sort them based on selected columns.
Clear Dialog Filter	Clears the filtering of the trace using Dialog Filter and displays all trace log entries.
Hide dropped messages	Hides dropped messages from the trace log entries.
More Actions > Export Trace Viewer Overview	Creates a tabulator-separated plain text file with all of the overview columns of the Trace Viewer page. You can open this file with editors such as Wordpad and Excel. The **More Actions** button is active only if trace records are listed. The retrieved Trace Viewer list can be saved into a file at the client side.
More Actions > Export Trace Viewer Details	Creates a plain text file with the details of the Trace View records. The **More Actions** button is active only if trace records are listed. The retrieved Trace Viewer list can be saved into a file at the client side.

Name	Description
Details	Displays the complete message. Click the Show arrow to view the message.
Time	Timestamp when the trace record was written. This timestamp entry also displays the date and time zone.
Tracing Entity	Host name of the system where Security Module logged the trace.
From	URI from where the traced SIP message originated.
Action	Action of the traced SIP message such as INVITE, ACK, or BYE. The SIP message action is surrounded by an arrow to indicate the direction of the action. For example, -- INVITE -> or <- BYE --. Dropped messages have a leading DROPPED, for example, -- DROPPED ACK ->
To	URI to which the traced SIP message was sent.
Protocol	Protocol that was used by the traced SIP message such as TCP, UDP, or TLS.
Call ID	Call ID of the traced SIP message.

Button	Description
View	Generates the trace log output for the selected Session Managers from the Session Manager list for

Table continues…

Button	Description
	the selected date range. This output displays the following details: **Note:** Number of retrieved records shows the number of records that matched the filter criteria. If Session Manager displays fewer records than this number, it means that not all the matching records are displayed. Usually this is done to avoid problems caused by running out of memory. In such cases, you can further configure or refine the filter criteria in such a way that all the log entries are displayed.
Clear	Clears all the selections made in the Trace Viewer page.

Call Routing Test

About Call Routing Testing

Use the call routing tests to test routing of a SIP INVITE based on the current Session Manager administration options that you select. You can use it to verify that you have administered the Session Manager as intended before placing it into service, or to get feedback on why a certain type of call is not being routed as expected. The testing of call routing using Session Manager does not send any “real” SIP messages. It invokes call processing in the debug mode to test routing.

Call Routing Test page field descriptions

Name	Description
Calling Party URI	SIP URI of the calling party. You must specify a handle and a domain, for example, 5552000@domain.com. You can also specify a full URI such as sip:5555555@domain.com:5060;sometag=3;othertag=4. You can also copy a URI recorded in a SIP trace and use it.
Calling Party Address	IP address or host name from which the INVITE is received.
Called Party URI	SIP URI of the called party. You must specify a handle and a domain, for example, sip:5551000@companydomain.com. You can also specify a full URI such as sip:5555555@domain.com:5060;sometag=3;othertag=4. You can also copy a URI recorded in a SIP trace and use it.

Table continues…

Name	Description
Session Manager Listen Port	Port on which the called Session Manager Instance receives the INVITE.
Day of Week	Day of the week. Call times can influence routing policies.
Time (UTC)	Time. Call times can influence routing policies.
Transport Protocol	The transport protocol used by the calling party, which may impact routing options. This is used in testing the routing based on entity links.
Called Session Manager Instance	The Session Manager instance that receives the initial INVITE from the calling party. **Note:** These are only core Session Manager instances.

Button	Description
Execute Test	Carries out the routing test based on the parameters that you provide. The Routing Decisions box displays the result of the routing test. This result displays one line per destination choice. For a destination that has alternate routing choices available, the result displays one line per alternate routing choice and the lines are in the same order that the test attempted the destinations. Each line displays not only where the INVITE would be routed, but also what the adapted digits and domain would be. The Routing Decision Process box contains details about how Session Manager made the routing decisions. This tool allows you to test your routing administration.

SNMP MIB

SNMP MIB Download

Administrators can download a zip archive file containing the definitions of Session Manager supported SNMP MIBs, alarm traps, and informs. SNMP MIBs can be used by Network Management Systems (NMS) supporting any version of Session Manager. MIBs downloaded from a Session Manager 6.3.2 Element Manager can be used by an NMS supporting earlier software version such as Session Manager 6.2.

An important condition of the feature is that the version of System Manager must always be equal to or greater than the software version of each of the Session Managers in the system.

The downloaded Session Manager SNMP MIBs zip archive file contains the current versions of the following MIB files:

- Standard MIBs
  - HOST-RESOURCES-MIB.my
  - If-mib.my
  - INADS-MIB.my
  - SNMPv2-MIB.my
  - Tcp-mib.my
  - Udp-mib.my
- Session Manager enterprise specific MIBs
  - SM-CommonAlarmDef-Data.my
  - SmSecMod-CommonAlarmDef-Data.my
  - SmSIPAS-CommonAlarmDef-Data.my
  - SmThirdPrty-CommonAlarmDef-Data.my
  - SMELEM-CommonAlarmDef-Data.my

For information about the SNMP support for Session Manager, see Maintaining and troubleshooting Avaya Aura® Session Manager.

Downloading SNMP MIBs

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Tools** > **SNMP MIB**.
3. In the SNMP MIB Download page, click **Download**.

   The system prompts you to save the Session Manager SNMP MIB zip archive file containing all the MIBs currently supported by the Session Managers in the system.
4. In the **Save As** dialog box, specify the file name and the location for saving the MIB zip archive file.

   The system displays the message that the MIB file is successfully saved in the specified location. In case of error, the system displays the reason for the unsuccessful download attempt.

SNMP MIB Download page field descriptions

Name	Description
File Name	The name of the Download file.
Description	The details of the file.
Action	Download the file.

Performance

Call Counts

Use the call count data of a selected SIP entity to:

- Generate graphs of the analyzed data.
- Export the analyzed data as a report in CSV (comma separated value) or XML format.

You can use the generated reports for capacity planning, system diagnostics, and so on.

Note:

- Performance data can be collected for Session Manager 6.1 and later releases.
- The system collects performance data based on a sample frequency of 5 minutes for the displayed parameters.

Related Links

Call Counts Report Types on page 553

Viewing call counts data

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Performance** > **Call Counts** to open the Call Counts page.
3. Select the required SIP entity.
4. Specify the date and time for the required period of the call counts data.
5. Select the required tab and click **Generate Graphs** for viewing the data in graphical format.

Related Links

Call Counts field descriptions on page 553

Exporting analysed call counts data

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Performance** > **Call Counts** to open the Call Counts page.
3. Select the required SIP entity.
4. Specify the date and time for the required period of the call counts data.
5. Select the required tab and specify the **Export Data Range** and **Export Data Format**.
6. Click **Download Data** to save a copy of the generated report.

Related Links

Call Counts field descriptions on page 553

Call Counts Report Types

Report Name	Report Details
SIP call count	• Active “other” SIP calls per SIP entity. • Active fax SIP calls per SIP entity. • Active text SIP calls per SIP entity. • Active video SIP calls per SIP entity. • Active audio SIP calls per SIP entity. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Related Links

Call Counts on page 552

Call Counts field descriptions

Name	Description
SIP Entity	SIP Entity for which call counts data is desired.
Data Available	Period for which performance data is available.
Date and Time	Period for which call counts data should be retrieved: 1. Predefined Values: • all dates and times • last month • last week • today

Table continues…

Name	Description
	• yesterday 2. Last: 1-99 Days or Hours 3. Between: Specified Date Range
Generate Graphs	Generates call counts graphs based on specified parameters.
Export Data Range	Period for which call counts data should be exported: • All – Retrieve all data for specified SIP entity. • Selected Range – Retrieve data based on the **Date and Time** field selection.
Export Data Format	Format of downloaded call counts data: CSV or XML.
Download Data	Export call counts data based on specified parameters.

Related Links

Viewing call counts data on page 552
Exporting analysed call counts data on page 553

Location Performance

Use the bandwidth usage information for the selected location to:

- Generate graphs of the analyzed data.
- Export the analyzed data as a report in CSV (comma separated value) or XML format.

You can use the generated reports for capacity planning, system diagnostics, and so on.

Note:

- Performance data can be collected for Session Manager 6.1 and later releases.
- The system collects performance data based on a sample frequency of 5 minutes for the displayed parameters.

Related Links

Location Performance Report Types on page 555

Viewing location performance data

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Performance** > **Location Performance** to open the Location Performance page.
3. Select the required location.

4. Specify the date and time for the required period of the bandwidth usage data for the selected location.
5. Select the required tab and click **Generate Graphs** for viewing the data in graphical format.

Related Links

Location Performance field descriptions on page 556

Exporting analyzed location performance data

Procedure

1. On the System Manager Web Console, under **Elements**, click **Session Manager**.
2. Click **Performance** > **Location Performance** to open the Location Performance page.
3. Select the required location.
4. Specify the date and time for the required period of the location performance data.
5. Select the required tab and specify the **Export Data Range** and **Export Data Format**.
6. Click **Download Data** to save a copy of the generated report.

Related Links

Location Performance field descriptions on page 556

Location Performance Report Types

Report Name	Report Details
Bandwidth Usage	• Multimedia bandwidth allocated per location. • Audio bandwidth allocated per location. • Total bandwidth available per location. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Bandwidth Available	• Total bandwidth available per location. • Multimedia bandwidth available per location. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Call Counts	• Count of calls totally rejected or denied due to insufficient bandwidth per location. • Count of downgraded calls where quality was reduced due to insufficient bandwidth per location. • Count of completed calls per location.

Table continues…

Report Name	Report Details
	The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Related Links

Location Performance on page 554

Location Performance field descriptions

Name	Description
Location	Location for which bandwidth usage data is desired.
Data Available	Period for which performance data is available.
Date and Time	Period for which bandwidth usage data should be retrieved: 1. Predefined Values: • all dates and times • last month • last week • today • yesterday 2. Last: 1-99 Days or Hours 3. Between: Specified Date Range
Generate Graphs	Generates bandwidth usage graphs based on specified parameters.
Export Data Range	Period for which bandwidth usage data should be exported: • All : Retrieve all data for specified location. • Selected Range : Retrieve data based on the **Date and Time** field selection.
Export Data Format	Format of downloaded bandwidth usage data: CSV or XML.
Download Data	Export bandwidth usage data based on specified parameters.

Related Links

Viewing location performance data on page 554
Exporting analyzed location performance data on page 555

SIP Performance

Use the Session Manager SIP performance data to:

- Generate graphs of the analyzed data
- Export the analyzed data as a report in CSV (comma separated value) or XML format.

You can use the generated reports for capacity planning, system diagnostics, and so on.

Note:

- Performance data can be collected for Session Manager 6.1 and later releases.
- The system collects performance data based on a sample frequency of 5 minutes for the displayed parameters.

Performance report acronym definitions

The SIP performance reports use the following acronyms:

- Mps – Messages per second
- GMps – giga Messages per second (10^9)
- MMps – mega Messages per second (10^6)
- kMps – kilo Messages per second (10^3)
- mMps – milli Messages per second (10^-3)
- uMPS – micro Messages per second (10^-6)
- nMps – nano Messages per second (10^-9)

Related Links

SIP Performance Report Types on page 558

Viewing SIP performance data

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Performance** > **SIP Performance** to open the SIP Performance page.
3. Select the required Session Manager instance.
4. Specify the date and time for the required period of the SIP performance data.
5. Select the required tab and click **Generate Graphs** for viewing the data in graphical format.

Related Links

SIP Performance field descriptions on page 561

Exporting analysed SIP performance data

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Performance** > **SIP Performance** to open the SIP Performance page.
3. Select the required Session Manager instance.
4. Specify the date and time for the required period of the SIP performance data.
5. Select the required tab and specify the **Export Data Range** and **Export Data Format**.
6. Click **Download Data** to save a copy of the generated report.

Related Links

SIP Performance field descriptions on page 561

SIP Performance Report Types

Total Tab

Report Name	Report Details
Trusted SIP Entities – SIP traffic	• Total SIP messages transmitted from a trusted SIP entity per Session Manager. • Total SIP messages received by a trusted SIP entity per Session Manager. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Trusted SIP Entities – SIP requests and responses	• Total SIP requests transmitted from a trusted SIP entity per Session Manager. • Total SIP requests received by a trusted SIP entity per Session Manager. • Total SIP responses transmitted from trusted SIP entity per Session Manager. • Total SIP Responses received by trusted SIP entity per Session Manager. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Trusted SIP Entities – SIP errors	• Total Security Module drops on trusted SIP entity per Session Manager

Table continues…

Report Name	Report Details
	• Total Transmission Errors on trusted SIP entity per Session Manager The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Default Policy SIP devices – SIP traffic	• Total SIP messages transmitted from an untrusted SIP entity per Session Manager. • Total SIP messages received by an untrusted SIP entity per Session Manager. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Default Policy SIP devices – SIP requests and responses	• Total SIP requests transmitted from an untrusted SIP entity per Session Manager. • Total SIP requests received by an untrusted SIP entity per Session Manager. • Total SIP responses transmitted from an untrusted SIP entity per Session Manager. • Total SIP Responses received by an untrusted SIP entity per Session Manager. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Default Policy SIP devices – SIP errors	• Total Security Module drops on an untrusted SIP entity per Session Manager. • Total Transmission Errors on an untrusted SIP entity per Session Manager. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
SIP call count	• Active “other” SIP calls per Session Manager. • Active fax SIP calls per Session Manager. • Active text SIP calls per Session Manager. • Active video SIP calls per Session Manager. • Active audio SIP calls per Session Manager. The report shows the maximum, minimum and average values in the selected time period for each

Table continues…

Report Name	Report Details
	of the displayed parameters at the bottom of graphs as part of the graph legend.

SIP Entity Tab

Report Name	Report Details
SIP traffic	• Total SIP messages transmitted per SIP Entity. • Total SIP messages received per SIP Entity. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
SIP requests and responses	• Total SIP Requests transmitted per SIP Entity. • Total SIP Requests received per SIP Entity. • Total SIP Responses transmitted per SIP Entity. • Total SIP Responses received per SIP Entity. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
SIP errors	• Total Security Module drops per SIP Entity. • Total Transmission Errors per SIP Entity. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

SIP Per IP Tab

Report Name	Report Details
SIP traffic	• Total SIP messages transmitted per SIP IP Address. • Total SIP messages received per SIP IP Address. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
SIP requests and responses	• Total SIP Requests transmitted per SIP IP Address. • Total SIP Requests received per SIP IP Address.

Table continues…

Report Name	Report Details
	• Total SIP Responses transmitted per SIP IP Address. • Total SIP Responses received per SIP IP Address. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
SIP errors	• Total Security Module drops per SIP IP Address. • Total Transmission Errors per SIP IP Address. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Related Links

SIP Performance on page 557

SIP Performance field descriptions

Name	Description
Session Manager	Session Manager whose SIP performance data is desired.
Data Available	Period for which performance data is available.
Date and Time	Period for which SIP performance data should be retrieved: 1. Predefined Values: • all dates and times • last month • last week • today • yesterday 2. Last: 1-99 Days or Hours 3. Between: Specified Date Range
Generate Graphs	Generates SIP performance graphs based on specified parameters.
Export Data Range	Period for which SIP performance data should be exported: • All : Retrieve all data for specified Session Manager.

Table continues…

Name	Description
	• Selected Range : Retrieve data based on the **Date and Time** field selection.
Export Data Format	Format of downloaded SIP performance data: CSV or XML.
Download Data	Export SIP performance data based on specified parameters.

Related Links

Viewing SIP performance data on page 557
Exporting analysed SIP performance data on page 558

System Performance

Use Session Manager platform performance data to:

- Generate graphs of the analyzed data
- Export the analyzed data as a report in CSV (comma separated value) or XML format.

You can use the generated reports for capacity planning, system diagnostics, and so on.

Note:

- Performance data can be collected for Session Manager 6.1 and later releases.
- The system collects performance data based on a sample frequency of 5 minutes for the displayed parameters.

Related Links

System Performance Report Types on page 563

Viewing system performance data

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Performance** > **System Performance** to open the System Performance page.
3. Select the required Session Manager instance.
4. Specify the date and time for the required period of the system performance data.
5. Select the required tab and click **Generate Graphs** for viewing the data in graphical format.

Related Links

System Performance field descriptions on page 565

Exporting analysed system performance data

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **Performance** > **System Performance** to open the System Performance page.
3. Select the required Session Manager instance.
4. Specify the date and time for the required period of the System Performance data.
5. Select the required tab and specify the **Export Data Range** and **Export Data Format**.
6. Click **Download Data** to save a copy of the generated report.

Related Links

System Performance field descriptions on page 565

System Performance Report Types

CPU Tab

Report Name	Report Details
CPU Usage	• User : CPU occupancy for normal processes executing in user mode. • System : CPU occupancy for processes executing in kernel mode. • Idle : CPU occupancy when system is idle. • IO Wait : CPU occupancy of waiting for I/O to complete. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Memory Tab

Report Name	Report Details
Physical Memory	• Total :Total usable RAM (physical ram minus a few reserved bits and the kernel binary code). • Free : Sum of LowFree + HighFree (overall stat). • Used : RAM used by the system. • Cached : Memory in the pagecache (diskcache) — SwapCache. The report shows the maximum, minimum and average values in the selected time period for each

Table continues…

Report Name	Report Details
	of the displayed parameters at the bottom of graphs as part of the graph legend.
Swap Memory	• Swap Total : Total amount of physical swap memory. • Swap Free : Total amount of swap memory free. • Swap Used : Total amount of swap memory used. • Swap In :Total amount of swap memory swapped in. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Disk Tab

Report Name	Report Details
Disk Usage	• Total Session Manager disk space used. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Network eth0/ eth2 Tab

Report Name	Report Details
Network Bytes	• Total Network bytes received (rxbytes) • Total Network bytes transmitted (txbytes) The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Network Packets	• Total Network packets received (rxpackets) • Total Network packets transmitted (txpackets) The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Network Errors	• Total received network errors (rxerr) • Total received network drops (rxdrop) • Total transmitted network errors (txerr) • Total transmitted network drops (txdrop)

Table continues…

Report Name	Report Details
	The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Temperature Tab

Report Name	Report Details
Temperature	• Chassis Temperature **Note:** When Session Managers are installed on a System Platform based platform, then temperature related information is not displayed. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Related Links

System Performance on page 562

System Performance field descriptions

Name	Description
Session Manager	Session Manager whose System performance data is desired.
Data Available	Period for which performance data is available.
Date and Time	Period for which System performance data should be retrieved: 1. Predefined Values: • all dates and times • last month • last week • today • yesterday 2. Last: 1-99 Days or Hours 3. Between: Specified Date Range
Generate Graphs	Generates System performance graphs based on specified parameters.

Table continues…

Name	Description
Export Data Range	Period for which System performance data should be exported: • All – Retrieve all data for specified Session Manager. • Selected Range – Retrieve data based on the **Date and Time** field selection.
Export Data Format	Format of downloaded System performance data: CSV or XML.
Download Data	Export System performance data based on specified parameters.

Related Links

Viewing system performance data on page 562
Exporting analysed system performance data on page 563

Performance Data Collection

Use this module to monitor and manage performance data collection from Session Manager instances. Performance data information includes collection, sampling interval information and utilization of the performance disk slice dedicated to performance data storage.

This module provides the following features:

- Indicates valid range of collected data that can be displayed for Session Manager.
- Shows general status information on performance processing and disk usage.
- Ability to force collection now, able to test repair of collection system or get performance data up to date after outage to a particular Session Manager.
- Ability to disable or enable collection from all Session Managers, selected Session Managers.
- Specifies performance data storage location, which can be either the existing performance data disk partition that resides on System Manager or an external Network File System (NFS) disk partition. By default, the data storage location is set to Local, the 30 GB partition on System Manager.

Using NFS disk space for Performance Data storage

When using remote storage, the NFS partition should be 30 GB or more, with the recommended size being 80 GB.

Note:

Remote NFS storage should be used for large capacity configurations to ensure adequate space is available for performance data storage.

Before you begin

Start an SSH session.

Procedure

1. Log in to System Manager using SSH as a non-root user.
2. Mount NFS share.

   Run the script **`mountNFS_PerfData.sh server:directory`** , where

   - server is the Hostname, IP address or fully qualified domain name of the NFS server
   - directory is the path to the shared directory on the NFS server
3. Disable performance data collection for all Session Managers.
   a. On the System Manager Web Console, click **Elements** > **S ession Manager**.
   b. In the left navigation pane, click **Performance** > **Data Collection** to open the Data Collection page.
   c. Click **Disable All** on the **Per Session Manager Collection** table at the bottom of the page.
4. Move existing performance data to the remote storage location.
   a. Run the script **`move_to_perfdata-remote.sh`** from SSH session.
   b. Successful completion of the move is indicated by returning to the command prompt without an error message being displayed. After the move is completed, the performance data can no longer be accessed in the old storage location.
5. Change the storage location
   a. On System Manager Web Console, click **Elements** > **Session Manager**.
   b. In the left navigation pane, click **Performance** > **Data Collection** to open the Data Collection page.
   c. Click **Change Data Storage**.

      Click **OK** and acknowledge the warning message. The warning states that existing performance data should be moved from the current storage location to the new location in order to prevent loss of data.
   d. After the warning message is acknowledged, the Performance Data Storage Location window is displayed.
   e. Select **Remote (NFS) storage** and click **Commit**.

   Prior to committing the changes when Remote (NFS) is selected, the system validates that the NFS is properly mounted on the local mount point and the NFS server is accessible.

   After committing the changes, the Data Collection page is updated with the new storage location.
6. Enable performance data collection for all Session Managers.
   a. On the System Manager Web Console, click **Elements** > **Session Manager**.
   b. In the left navigation pane, click **Performance** > **Data Collection** to open the Data Collection page.

c. Click **Enable All** on the **Per Session Manager Collection** table at the bottom of the page.

Reverting back to local storage after using remote storage

Before you begin

Start an SSH session.

About this task

This procedure is applicable in the unlikely event that a customer desires to revert back to local storage after using a remote NFS share.

Caution:

If the size of the NFS performance data partition exceeds 30 GB, the data cannot be moved back to the local disk because the local disk partition is limited to 30 GB max.

Procedure

1. Disable performance data collection for all Session Managers.
   a. On System Manager Web Console, click **Elements** > **Session Manager**.
   b. In the left navigation pane, click **Performance** > **Data Collection** to open the Data Collection page.
   c. Click **Disable All** on the **Per Session Manager Collection** table at the bottom of the page.
2. Log in to System Manager using SSH as a non-root user.
3. Move existing performance data from the remote storage location to the local disk.
   a. Run the script `move_to_perfdata.sh` from SSH session.
   b. Successful completion of the move will be indicated by returning to the command prompt without an error message being displayed. After the move is completed, the performance data will no longer be accessible in the old storage location.
4. Change the storage location
   a. On System Manager Web Console, click **Elements** > **Session Manager**.
   b. In the left navigation pane, click **Performance** > **Data Collection** to open the Data Collection page.
   c. Click **Change Data Storage**.

      Click **OK** and acknowledge the warning message. The warning states that existing performance data should be moved from the current storage location to the new location in order to prevent loss of data.
   d. After the warning message is acknowledged, the Performance Data Storage Location window is displayed.
   e. Select **Local** storage and click **Commit**.

After committing the changes, the Data Collection page is updated with the new storage location.

5. Enable performance data collection for all Session Managers.
   a. On System Manager Web Console, click **Elements** > **Session Manager**.
   b. In the left navigation pane, click **Performance** > **Data Collection** to open the Data Collection page.
   c. Click **Enable All** on the **Per Session Manager Collection** table at the bottom of the page.
6. Un-mount NFS share.

   Run the script **`unmountNFS_PerfData.sh`** from SSH session.

Performance Data Collection field descriptions

Button	Description
Refresh	Refreshes performance data collection status information.
Collect Now	Starts data collection from enabled Core Session Managers.
Reinitialize	Restarts entire performance data collection system, force re-retrieval of all data stored on Session Managers. **Warning:** This operation forces complete re-loads from all Session Managers and is very resource intensive. It should only be used if found extremely necessary.
Change Data Storage	Opens the Performance Data Storage Location window where user can change the storage location.

Name	Description
Data collection status	Shows whether data collection is currently running, idle, administratively disabled, or error has occurred. Following are the possible states: • IDLE indicates that the collection process is currently not running. • COLLECTING indicates that the system is currently downloading measurement CSV files and converting to RRD files. • ERROR: disk area problem — indicates that there is a disk area problem that can be serious.

Table continues…

Name	Description
	• ERROR: disabled, disk full — indicates that alarm has been generated for performance partition being full. • COLLECTING: disk use warning — indicates the system is above the warning alarm level.
Last Collection	Date of last collection cycle completed for all enabled Session Managers.
Collection interval minutes	Interval between collection from Session Managers. Collection begins at the top of the hour.
5 Min sample retention days	5 minute sample data retention period.
60 Min sample retention days	Hourly roll up sample data retention period.
CSV file retention days	Raw CSV file retention period on System Manager.
Performance data storage location	Specifies type of storage used for performance data. Valid choices are: • Local • Remote (NFS) Default value is Local.

Per Session Manager Collection

Button	Description
Disable	Turns off data collection for select Session Managers, does not stop Session Manager measurement sampling, just collection from Session Managers.
Enable	Turns on data collection for select Session Managers, does not stop Session Manager measurement sampling, just collection from Session Managers.
Disable All	Stops data collection from all Session Managers, does not stop Session Manager measurement sampling, just collection from Session Managers.
Enable All	Starts data collection from all Session Managers, does not stop Session Manager measurement sampling, just collection from Session Managers.
Reset	Discards changes and restore original values.
Apply	Applies the changes.

Name	Description
Session Manager	Name of administered Session Manager instance.
Release	Session Manager Release Number.

Table continues…

Name	Description
Type	Type of Session Manager instance.
Data Collection	Shows whether data collection is enabled or disabled.
Last Collection	The date and time of the last successful collection from this Session Manager instance.
First Sample	The date and time of the first measurement sample collected.
Last Sample	The date and time of the last measurement sample collected.

Chapter 9: System Tools

Session Manager maintenance tests

Use the Maintenance Tests page to perform tests on the System Manager server and the configured Session Managers. The tests verify functionality such as network connectivity, data replication, and database operation. The system runs the tests periodically to monitor the status of system components. You can also run the tests on demand.

Note:

Tests can fail if the server under test is out of service or is not responding.

Maintenance Tests page field descriptions

Name	Description
Select System Manager or Session Manager to test:	Select a System Manager or a Session Manager from the drop-down menu on which to perform the maintenance tests.

Button	Description
Execute Selected Tests	Run the selected maintenance tests on the selected System Manager or Session Manager.
Execute All Tests	Run all the maintenance tests on the selected System Manager or Session Manager.

Name	Description
Test Description	Description of the test.
Test Result	The outcome of executing the test (pass or fail).
Test Result Time Stamp	The last time the test was run.

Note:

The system loads Maintenance test data asynchronously in the background. The system displays the message **Loading..** when data is loading in the background. The system displays the message **Loading Complete** when data loading finishes. If the wait time exceeds a certain limit, the system displays the message **Loading failure. Please try again.** and requests the user to try again later.

Running maintenance tests

Run the maintenance tests on the current System Manager or any configured Session Manager.

Procedure

1. On the System ManagerWeb Console, under **Elements**, select **Session Manager** > **System Tools** > **Maintenance Tests**.
2. In the **System Manager or a Session Manager to test** field, select **System Manager** or a Session Manager instance from the drop-down menu.
3. To run all of the tests, select **Execute All Tests**.
4. To run only certain tests:
   a. Select the test to run from the test list.
   b. Click **Execute Selected Tests**.
5. Verify the tests pass.

Maintenance Test descriptions

Test Call Processing status

This test checks the call processing functionality for a particular Session Manager instance. If call processing is working correctly, the test passes. If the test fails, contact Avaya Technical Support.

Test data distribution and redundancy link

This test only runs on Session Manager. This test verifies the Session Manager data share mechanism is functioning properly by sending a test string to each configured Session Manager. Each Session Manager saves the test string Session Manager within its respective database. After a short wait, the system queries each Session Manager for the test string value.

The test passes if each Session Manager returns the correct value.

A test failure indicates a potential failure of link redundancy and Session Manager pass-through capabilities that could impact call processing and Call Admission Control.

The test does not run on a Session Manager if the state of the Session Manager is **Deny New Service**.

Test host name resolution of each Session Manager

This test only runs on System Manager. The test verifies that the DNS server can resolve the host name of each configured Session Manager.

If the DNS server can resolve the host name for each Session Manager, the test passes. Otherwise, the test fails. Check for the following possible causes:

- The Session Manager host name is incorrect on the DNS server.
- The Session Manager host name is missing on the DNS server.

Test management link functionality

This test checks the administrative link to the Session Manager. If the test fails, administrative changes cannot take effect on Session Manager. .

Test Postgres database sanity

This test runs on either System Manager or aSession Manager.

System Manager tests the functionality of the master database.

The Session Manager tests the functionality of the local instance database.

If the test fails, contact Avaya Technical Support.

Test sanity of Secure Access Link (SAL) agent

This test can run on either System Manager or Session Manager. It checks if the Security Access Link agent is running or not on the server. If the link is up and running, the test passes.

If the test fails, run the **statapp** command and other corrective actions for associated alarms on Session Manager before escalating to Avaya Technical Support.

Test Security Module Status

This test queries the status of the Security Module on a specified Session Manager. If the query is successful, the test passes. Otherwise, the test fails.

Test network connections to each Session Manager

The Network Connections test runs only on System Manager. This test verifies the connectivity to each administered Session Manager.

If connectivity is up for each Session Manager, the test passes. If connectivity is down, the test fails. The following are possible causes of test failure:

1. An upgrade or install is in progress.
2. The server might be out of service. Check the log for an event code, then check the Log Event Codes in *Maintaining and Troubleshooting Avaya Aura® Session Manager* for the appropriate troubleshooting action.
3. The network might be out of service. Run a ping test between System Manager and the failing Session Manager to verify network connectivity.

Test User Data Storage sanity

Note:

This test is not available for:

- Branch Session Managers
- Session Managers that are running a release earlier than 6.3.8.

This test checks the status of the **Cassandra** application and the connectivity to the **Cassandra** database. The test passes if the application and the connectivity are operating correctly. The test fails otherwise.

SIP Tracer Configuration

About Tracer Configuration

You can use the Tracer Configuration page to configure the tracing of SIP messages incoming through the security module, SIP messages outgoing from the security module, and also messages dropped by ASSET proxy or by the SIP firewall.

You can also filter these messages based on the user or the call. Session Manager logs all the traced messages to a file based on the configuration.

Tracer Configuration page field descriptions

Tracer Configuration

Name	Description
Tracer Enabled	SIP message tracing is enabled by default.
Trace All Messages	SIP message tracing is enabled for all SIP messages. In this case, other fields get disabled.
From Network to Security Module	SIP message tracing is enabled for ingress calls sent to the Session Manager instance from the network.
From Security Module to Network	SIP message tracing is enabled for egress calls originating from the Session Manager instance and sent to the network.
From Server to Security Module	Local SIP messages originating from Session Manager.

Table continues…

Name	Description
From Security Module to Server	Local SIP messages originating from the security module.
Trace Dropped Messages	SIP message tracing is enabled to trace messages from calls dropped by the SIP firewall as well as by the SM100 proxy.
Max Dropped Message Count	Shows the value for the maximum number of traced dropped messages, if Dropped check box is activated.
Send Trace to a Remote Server	Enables or disables SIP Tracing to an external host . This enables Session Manager to send all the (decrypted) SIP traffic out to an external host. Session Manager uses Syslog protocol for sending the SIP traffic (as used currently for SIP Tracing).
Remote Server FQDN or IP Address	FQDN or IP address of the remote syslog server.
Send Trace Method	Method used to transfer syslogs either using Stunnel (encrypted TCP) or Syslog (unsecure UDP) as mentioned below: • Syslog (unsecured UDP) : Traffic is send without being encrypted to remote server as specified in the “Remote Server FQDN or IP Address” to default syslog port. • Stunnel (encrypted TCP) : Traffic is send as encrypted (using stunnel) to remote server that is specified in the “Remote Server FQDN or IP Address” to the port specified in the input field ”Stunnel Port”.
Stunnel Port	Port number that remote server's stunnel is listening on. Stunnel provides several modes for far end certificate validation.

User Filter

Button	Description
New	Create a new filter for filtering SIP messages based on the users. You can define a maximum of three user filters.
Delete	Delete a selected user filter or filters.

Name	Description
From	Filter SIP messages based on the user from whom the message is sent. Type the user string. For example, a rule to trace all messages from user “pqr”:

Table continues…

Name	Description
	to="" from="pqr" stop-count=50
To	Filter SIP messages based on the user to whom the message is sent. Type the user string. For example, a rule to trace all messages to user "xyz": to="xyz" from="" stop-count=50
Source	Filter SIP messages based on the source address.
Destination	Filter SIP messages based on the destination address.
Max Message Count	Value for maximum number of messages matching the filter that Session Manager should trace. Default is 25 messages.

Call Filter

Button	Description
New	Create a new filter for filtering all SIP messages that start a new call. You can define a maximum of three call filters.
Delete	Delete a selected call filter or filters.

Name	Description
From	Filter SIP messages from a specific user. Call tracing identifies a call by capturing the Call ID from the first message that matches the From filter, thereafter tracing all the messages that have the matching call ID. For example, a rule to trace all messages related to a CALL from user "pqr": to="" from="pqr" request-uri="" stop-count=50
To	Filter SIP messages based on the user to whom the message is sent. Call tracing identifies a call by capturing the Call ID from the first message that matches the To filter, thereafter tracing all the messages that have the matching call ID. For example, a rule to trace all messages related to a CALL to user "xyz": to="xyz" from="" request-uri="" stop-count=50
Source	Filter SIP messages based on the source address.
Destination	Filter SIP messages based on the destination address.

Table continues…

Name	Description
Max Call Count	Value for maximum number of messages matching the filter that Session Manager should trace. Default is 25 messages.
Request URI	Filter calls based on the called party (URI address). A valid Request URI format, for example, is .@192.111.11.111.

Session Manager Instances

Name	Description
Name	Select one or more configured Session Managers for which the specific filters should be used. **Note:** If you select only one Session Manager from this list, the **Read** button is activated. Click this button to retrieve the current Trace Configuration details for the selected Session Manager and display that within the Trace Configuration page. After displaying the configuration, Session Manager closes the display so that no older configuration data is displayed.

Button	Description
Commit	Save the configuration changes.
Read	Retrieves the current Trace Configuration details for the selected Session Manager and display that within the Trace Configuration page.

SIP Trace Viewer

About SIP Tracing

Use the SIP tracer to trace SIP messages exchanged between the Session Manager server and remote SIP entities. SIP messages that are dropped by any of the SM100 components such as SIP Firewall are also logged by the SIP tracer. You can trace all the messages belonging to a user, for a call, or for a selected Session Manager instance. The SIP tracer provides statistics of SIP messages

within the SM100 framework. SIP tracer is located under Session Manager on the System Manager Common Console navigation pane. SIP tracer user interface has the following components:

- Tracer Configuration defines the characteristics of messages to be traced for the capturing engine in the security module.
- Trace Viewer displays the captured SIP messages.

For details, refer to the section Tracing in *Maintaining and Troubleshooting Avaya Aura® Session Manager* (03-603325)

Trace Viewer page field descriptions

Use the From and To fields to specify a range of days or time as follows:

Filter

Name	Description
From: Date	Date from which you want to filter the trace logs.
From: Time	Time from which you want to filter the trace logs.
From: Time Zone	Time Zone for the From date that you want to use for filtering trace logs.
To: Date	Date up to which you want to filter the trace logs.
To: Time	Time up to which you want to filter the trace logs.
To: Time Zone	Time Zone for the To date that you want to use for filtering trace logs.
Name	Name of the Session Manager instance.

Trace Viewer

Button	Description
Dialog Filter	Filters trace log entries. Select a trace log and click **Dialog Filter**. This option filters trace log entries and displays entries for the same Call ID, From, and To fields as the trace log that you select. **Note:** You can also click Filter: **Enable** to filter log entries based on a value or to sort them based on selected columns.
Clear Dialog Filter	Clears the filtering of the trace using Dialog Filter and displays all trace log entries.
Hide dropped messages	Hides dropped messages from the trace log entries.
More Actions > Export Trace Viewer Overview	Creates a tabulator-separated plain text file with all of the overview columns of the Trace Viewer page.

Table continues…

Button	Description
	You can open this file with editors such as Wordpad and Excel. The **More Actions** button is active only if trace records are listed. The retrieved Trace Viewer list can be saved into a file at the client side.
More Actions > Export Trace Viewer Details	Creates a plain text file with the details of the Trace View records. The **More Actions** button is active only if trace records are listed. The retrieved Trace Viewer list can be saved into a file at the client side.

Name	Description
Details	Displays the complete message. Click the Show arrow to view the message.
Time	Timestamp when the trace record was written. This timestamp entry also displays the date and time zone.
Tracing Entity	Host name of the system where Security Module logged the trace.
From	URI from where the traced SIP message originated.
Action	Action of the traced SIP message such as INVITE, ACK, or BYE. The SIP message action is surrounded by an arrow to indicate the direction of the action. For example, -- INVITE -> or <- BYE --. Dropped messages have a leading DROPPED, for example, -- DROPPED ACK ->
To	URI to which the traced SIP message was sent.
Protocol	Protocol that was used by the traced SIP message such as TCP, UDP, or TLS.
Call ID	Call ID of the traced SIP message.

Button	Description
View	Generates the trace log output for the selected Session Managers from the Session Manager list for the selected date range. This output displays the following details: **Note:** Number of retrieved records shows the number of records that matched the filter criteria. If Session Manager displays fewer records than this number, it means that not all the matching records are displayed. Usually this is done to avoid problems caused by running out of memory. In such cases, you can further

Table continues…

Button	Description
	configure or refine the filter criteria in such a way that all the log entries are displayed.
Clear	Clears all the selections made in the Trace Viewer page.

Call Routing Test

About Call Routing Testing

Use the call routing tests to test routing of a SIP INVITE based on the current Session Manager administration options that you select. You can use it to verify that you have administered the Session Manager as intended before placing it into service, or to get feedback on why a certain type of call is not being routed as expected. The testing of call routing using Session Manager does not send any “real” SIP messages. It invokes call processing in the debug mode to test routing.

Call Routing Test page field descriptions

Name	Description
Calling Party URI	SIP URI of the calling party. You must specify a handle and a domain, for example, 5552000@domain.com. You can also specify a full URI such as sip:5555555@domain.com:5060;sometag=3;othertag=4. You can also copy a URI recorded in a SIP trace and use it.
Calling Party Address	IP address or host name from which the INVITE is received.
Called Party URI	SIP URI of the called party. You must specify a handle and a domain, for example, sip:5551000@companydomain.com. You can also specify a full URI such as sip:5555555@domain.com:5060;sometag=3;othertag=4. You can also copy a URI recorded in a SIP trace and use it.
Session Manager Listen Port	Port on which the called Session Manager Instance receives the INVITE.
Day of Week	Day of the week. Call times can influence routing policies.

Table continues…

Name	Description
Time (UTC)	Time. Call times can influence routing policies.
Transport Protocol	The transport protocol used by the calling party, which may impact routing options. This is used in testing the routing based on entity links.
Called Session Manager Instance	The Session Manager instance that receives the initial INVITE from the calling party. **Note:** These are only core Session Manager instances.

Button	Description
Execute Test	Carries out the routing test based on the parameters that you provide. The Routing Decisions box displays the result of the routing test. This result displays one line per destination choice. For a destination that has alternate routing choices available, the result displays one line per alternate routing choice and the lines are in the same order that the test attempted the destinations. Each line displays not only where the INVITE would be routed, but also what the adapted digits and domain would be. The Routing Decision Process box contains details about how Session Manager made the routing decisions. This tool allows you to test your routing administration.

SNMP MIB

SNMP MIB Download

Administrators can download a zip archive file containing the definitions of Session Manager supported SNMP MIBs, alarm traps, and informs. SNMP MIBs can be used by Network Management Systems (NMS) supporting any version of Session Manager. MIBs downloaded from a Session Manager 6.3.2 Element Manager can be used by an NMS supporting earlier software version such as Session Manager 6.2.

An important condition of the feature is that the version of System Manager must always be equal to or greater than the software version of each of the Session Managers in the system.

The downloaded Session Manager SNMP MIBs zip archive file contains the current versions of the following MIB files:

- Standard MIBs
  - HOST-RESOURCES-MIB.my
  - If-mib.my
  - INADS-MIB.my
  - SNMPv2-MIB.my
  - Tcp-mib.my
  - Udp-mib.my
- Session Manager enterprise specific MIBs
  - SM-CommonAlarmDef-Data.my
  - SmSecMod-CommonAlarmDef-Data.my
  - SmSIPAS-CommonAlarmDef-Data.my
  - SmThirdPrty-CommonAlarmDef-Data.my
  - SMELEM-CommonAlarmDef-Data.my

For information about the SNMP support for Session Manager, see Maintaining and troubleshooting Avaya Aura® Session Manager.

Downloading SNMP MIBs

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Tools** > **SNMP MIB**.
3. In the SNMP MIB Download page, click **Download**.

   The system prompts you to save the Session Manager SNMP MIB zip archive file containing all the MIBs currently supported by the Session Managers in the system.
4. In the **Save As** dialog box, specify the file name and the location for saving the MIB zip archive file.

   The system displays the message that the MIB file is successfully saved in the specified location. In case of error, the system displays the reason for the unsuccessful download attempt.

SNMP MIB Download page field descriptions

Name	Description
File Name	The name of the Download file.
Description	The details of the file.
Action	Download the file.

Chapter 10: System Status

Session Manager SIP Entity Monitoring

SIP Entity Monitoring provides background detection for monitored connections to improve alternative routing and to minimize the call setup time due to SIP link failures. The SIP Monitor periodically tests the status of the SIP proxy servers. If a proxy fails to reply, SIP messages are no longer routed to that proxy. As a result, call delays are reduced since calls are not routed to the failed servers. The SIP Monitor continues to monitor the failed SIP entity. When the proxy replies, SIP messages are again routed over that link.

SIP monitoring sends OPTIONS requests to SIP entities to determine whether these are in up, partially up, down or deny new service state. An entity is considered up if all of the addresses associated with it are up. An entity is down if all of its addresses are down. An entity is partially up if some, but not all, of its addresses are up. An address is considered down if the response of address to OPTIONS is:

- 408 Request Timeout
- 500 Server Internal Error: Destination Unreachable
- 503 Service Unavailable (with no parenthetical text)
- 503 Service Unavailable (no media resources)
- 504 Server Timeout

All other responses (including "503 Service Unavailable") with other parenthetical text, such as "503 Service Unavailable (Signaling Resources Unavailable)" results in the address to be considered up.

Note:

Any 503 response is displayed as a 500 response on the SIP Monitoring GUI. SIP container converts 503 to 500 before passing the response to Session Manager.

You can turn the monitoring on or off for a given SIP entity. If monitoring is turned off, the SIP entity is not monitored by any instance.

You can also turn monitoring on or off for an entire instance. If monitoring is turned off, none of the SIP entities are monitored by that instance. If monitoring for the instance is turned on, only those SIP entities for which monitoring is turned on are monitored.

SIP Monitoring can only report problems if the Security Module is functional.

SIP Monitoring setup is administered using the SIP Entity and the Session Manager Administration pages on System Manager. See the sections *SIP Entities*, *Session Manager Administration* and *SIP Responses to an OPTIONS Request* from the book *Administering Avaya Aura® Session Manager*.

Related Links

Handling SIP responses on page 247
SIP Responses to an OPTIONS Request on page 297

Viewing the SIP Monitoring Status Summary page

About this task

The SIP Entity Link Monitoring Status Summary page displays the status of the entity links for all the administered Session Manager instances. An entity link consists of one or more physical connections between a Session Manager server and a SIP entity.

If all connections are up, then the entity link status is **up**. If one or more connections are down but there is at least one connection up, the link status is **partially down**. If all of the connections are down, the entity link status is **down**. If the connection denies any new service, the entity link status is **deny new service**.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **SIP Entity Monitoring**

   The **SIP Entity Link Monitoring Status Summary** page displays the SIP Entity Link monitoring status for all Session Manager instances.

SIP Entity Link Monitoring Status Summary page field descriptions

SIP Entities Status for ALL Monitoring Session Manager Instances

Button	Description
Run Monitor	Starts asynchronous demand monitor test for the selected Session Manager or Branch Session Manager instances.
Refresh	Refreshes the status of the entity links for all administered Session Manager instances.

Field	Description
Session Manager	Name of the Session Manager instance. Clicking any of Session Manager servers in the list opens the Session Manager Entity Link Connection Status page that displays detailed connection status for all entity links from Session Manager.

Table continues…

Field	Description
	Note: An entity link consists of one or more physical connections between a Session Manager server and a SIP entity. If all of these connections are up, then the entity link status is *up*. If one or more connections are down, but there is at least one connection up, then the entity link status is *partially down*. If all the connections are down, the entity link status is *down*.
Type	Instances of type Session Manager and Branch Session Manager.
Monitored Entities / Down	Entity links for Session Manager that are down out of the total number of entity links for Session Manager.
Monitored Entities / Partially Up	Entity links for Session Manager that are partially up.
Monitored Entities / Up	Entity links for Session Manager that are up out of the total number of entity links for Session Manager.
Monitored Entities / Not Monitored	SIP entities that are not monitored, because they are not administered to be monitored by Session Manager.
Monitored Entities / Deny	Number of Deny New Service Entity Links.
Monitored Entities / Total	Number of total Entity Links for a SIP Entity.

All Monitored SIP Entities

Button	Description
Run Monitor	Starts asynchronous demand monitor test for the selected SIP entities. Clicking any of the entities in the list opens the SIP Entity, Entity Link Connection Status page that displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Session Manager Entity Link Connection Status page field descriptions

All Entity Links with connections to Session Manager

Field	Description
SIP Entity Name	Name of the SIP Entity.
SIP Entity Resolved IP	Resolved IP address of the SIP entity.
Port	Port used for the connection.
Protocol	Protocol used.
Deny	Deny new service status.
Conn. Status	Connection status.

Table continues…

Field	Description
Reason Code	Reason for the failure. This field explains how the status of a connection is determined irrespective of whether the status is “up” or “down”.
Link Status	Status of the Entity Link.

Button	Description
Summary View	Returns to the SIP Entity Link Monitoring Status Summary page.
Refresh	Refreshes and displays the detailed connection status for all entity links from the selected Session Manager instance.

Details

Field	Description
Time Last Down	Time when the entity link was last down.
Time Last Up	Time when the entity link was last up.
Last Message Sent	Port used for the connection.
Last Message Response	Duration of the last response latency (ms).

SIP Entity, Entity Link Connection Status page field descriptions

All Entity Links to SIP Entity

Field	Description
Session Manager Name	Name of the Session Manager instance.
SIP Entity Resolved IP	Resolved IP address of the SIP entity
Port	Port used for the connection
Protocol	Protocol used
Deny	Deny new service status.
Conn. Status	Connection status
Reason Code	Reason for the failure. This field explains how the status of a connection is determined irrespective of whether the status is “up” or “down”.
Link Status	Status of the Entity Link.

Button	Description
Summary View	Returns to the SIP Entity Link Monitoring Status Summary page.
Refresh	Refreshes and displays the detailed connection status for all entity links from all Session Manager instance to a single SIP entity.

Details

Field	Description
Time Last Down	Time when the entity link was last down
Time Last Up	Time when the entity link was last up
Last Message Sent	Port used for the connection
Last Message Response	Duration of the last response latency (ms)

Managed Bandwidth

The Managed Bandwidth Usage page displays Managed Bandwidth (Call Admission Control) real-time data. Bandwidth usage measurements help administrators to manage networks with multimedia calls. The Managed Bandwidth Usage page displays a table containing one row for each administered location and provides details on actual call counts and bandwidth usage for audio and video calls respectively.

You can expand each row to display a breakdown of usage and capacity by Session Manager, which can help troubleshoot network utilization or the distribution algorithm. If no bandwidth management is administered, the table contains no data.

Viewing Managed Bandwidth Usage

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Managed Bandwidth Usage**.

   The Managed Bandwidth Usage screen displays system-wide bandwidth usage information for locations where usage is managed.
3. Click **Show** under Details column to view the bandwidth usage information per Session Manager in that location. You can click **Hide** to close this table.
4. On the Managed Bandwidth Usage screen, click **Refresh** to refresh the data.

Managed Bandwidth Usage page field descriptions

The Manage Bandwidth Usage page displays system-wide bandwidth usage information for locations where usage is managed. If there is no bandwidth management implemented, this table has no information.

Field	Description
Details	Shows the breakdown of usage among the administered Session Managers in the enterprise. You can click the Show or Hide arrow on any row in **Details** to show or hide the detailed usage for that location.
Location	Displays the locations that you have administered in the Routing Policy.
Audio Call Count	Indicates sum of audio calls of Session Manager in a given location.
Audio BW Used	Indicates sum of bandwidth used for audio calls of Session Managers in a given location.
Multimedia Call Count	Indicates sum of multimedia calls of Session Managers in a given location.
Multimedia BW Used	Indicates sum of bandwidth used for multimedia calls of Session Managers in a given location.
Multimedia BW Allow	Administered value, if any, of multimedia Bandwidth for a given location.
Multimedia BW %Used	Indicates sum of bandwidth used for multimedia calls into or out of a given location divided by the value in the "Multimedia BW Allow" column.
Total BW Used	Indicates sum of audio and multimedia bandwidth into or out of a given location
Total BW Allow	Administered value, if any, of "Total Bandwidth" for a given location.
Total BW %Used	Indicates sum of audio and multimedia bandwidth for calls into or out of a given location divided by the value in the "Total BW Allow" column.

Field	Description
Session Manager	Name of the instance.
Audio Call Count	Number of audio calls terminated by the selected Session Manager for the given location.
Audio BW Used	Sum of bandwidth used by audio calls terminated by the selected Session Manager for the given location.
Multimedia Call Count	Number of multimedia calls terminated by the selected Session Manager for the given location.
Multimedia BW Used	Indicates sum of bandwidth used by multimedia calls terminated by the selected Session Manager for the given location.

Security Module Status

About Security Module Status

Use the Security Module Status page to view the status of the security module for each administered Session Manager and to perform certain actions on the security module.

You can view the status of the security module, such as the IP address of security module, default gateway, the interface that a security module uses, the VLAN that it is associated with, the QOS priority, trusted hosts configured for that security module, and the certificate authority.

You can also reset and synchronize the security module or assign a certificate authority.

Security Module Status actions

Use the Security Module Status page to perform the following actions:

- **Refresh**: Refreshes the statistics for all of the administered Session Manager instances.
- **Reset** : Resets the security module for the selected Session Manager. You may choose to reset the security module when a connection cannot be made to the security module.

  Warning:

  The Session Manager cannot process calls while the security module is being reset. See *Administering Avaya Aura® Session Manager* for details on how to disable the Session Manager prior to resetting the security module.
- **Synchronize**: Verifies that the administered configuration matches the actual configuration stored on the security module. This action should be performed anytime the values in the security module statistics table do not match the administered data.
- **Connection Status**: Shows the view of the current status of inbound and outbound links between the Session Manager security module and external hosts. Connection Status enables general-purpose monitoring and debugging activities, such as:
  - identifying if the Session Manager is required to be taken out of service
  - determining if links are secured or not
  - viewing link details and statistics

Investigating Security Module status

Possible causes for the Security Module status to be **Down** include:

- The security module may have recently been reset. A reset can take several minutes to complete.

- The security module may not have received security module configuration information from System Manager System Manager.

Procedure

1. On the System Manager Web Console, under **Services**, click **Replication** to display the **Replica Group** associated with the Session Manager instance.
2. If the **Synchronization Status** is not **Synchronized** for the Session Manager instance:
   a. Select the affected Replica Group.
   b. Click **View Replica Nodes**.
   c. On the Replica Nodes page, verify the **Replica Node Host Name** is correct.
   d. If the **Replica Node Host Name** is incorrect, click **Repair**.
3. Click **Refresh** to see the latest status.
4. On the Security Module Status page, if the status is **Down**, synchronize the security module to trigger an update:
   a. Click the button in front of the appropriate Session Manager instance from the Session Manager list.
   b. Click **Synchronize**.
   c. Click **Refresh** to see the latest status.
5. If the status is still **Down**, reset the security module:
   a. Select the appropriate Session Manager instance from the Session Manager list.
   b. Click **Reset**.

      Warning:

      The Session Manager cannot process calls while the security module is being reset.
6. Select **Refresh** to see the latest status.

Security Module Status page field descriptions

Button	Description
Reset	Opens the Security Module Reset Confirmation page.
Synchronize	Synchronizes the security module of the selected Session Manager and displays the Confirm Security Module Synchronize page.
Connections Status	Displays the connection status information for the selected Session Manager instance.

Name	Description
Details	Displays detailed information about the selected Session Manager instance. **Note:** Details are available only in certain releases or if additional features are enabled.
Session Manager	Displays the name of the Session Manager instance.
Type	Displays the type of Session Manager instance (SM or BSM).
Status	Displays the status of the Security Module deployed for the Session Manager (up or down).
Connections	Displays the total number of connections for the Security Module.
IP Address	Displays the IP address of the security module used for SIP traffic. This field should match the address administered on the SIP Entity form for the Session Manager instance.
VLAN	Displays the VLAN ID associated with the security module. This field should match the VLAN ID administered on the Session Manager instance form.
Default Gateway	Displays the default Gateway used by the security module. This value should match the default gateway administered on the Session Manager instance form.
NIC Bonding	Displays if NIC bonding is “enabled” or “disabled”.
Entity Links (expected / actual)	Displays the expected and actual number of Entity Links. The expected value is the number of SIP Entities configured in the Routing Policy that have Entity Links to the Session Manager. The actual value is the number of Entity Links currently configured on the security module. If these values do not match, perform the Synchronize action.
Certificate Used	Displays the details of the certificate type used.

Related Links

SIP Firewall status on page 443

Confirm Security Module Reset page field descriptions

Button	Description
Confirm	Resets the security module for the selected Session Manager instance. , Session Manager cannot process the calls while the security module is being reset.
Cancel	Cancels the resetting of the security module for the selected Session Manager

About Connection Status

Connection Status allows administrator to view current status of inbound and outbound links between Session Manager security module and external hosts. Use Connection Status to perform general-purpose monitoring and debugging activities, such as:

- Identification of whether Session Manager is required to be taken out of service
- Determination of whether links are secured or not
- Viewing of link details and statistics

Monitoring Connection Links

Procedure

1. On the System Manager console, under **Elements**, click **Session Manager**.
2. Click **System Status** > **Security Module Status** to open the Security Module Status page.
3. Select a system and click **Connection Status** to open the Connection Status page.
4. Apply the required filters using the **Connection Filter** section. Select the **Non-Compliant NIST TLS Only** check box to display only the TLS connections that are not compliant with NIST standards.
5. Under **Connection List**, click **Apply Filter** to display the list of connection links.
6. Select a row and click **Show** to view the detailed information about the selected connection.
7. Click **Return** to return to the Security Module Status page.

Connections Status field descriptions

Summary section

The Summary section displays the total number of Active Connections and the number of connections that are incoming, outgoing, TCP, and TLS.

Connection Filter section

Use the Connect Filter section to define a filter and to display the connection list based on the defined filters. A filter can be an FQDN or an IP Address and mask.

If you select the **Non-compliant NIST TLS Only** check box, the screen displays only the TLS connections having an algorithm that is not compliant with the NIST SP800-131A recommendation.

Connection List section

The Connection List table displays basic information of all the active connections. The following definitions apply to several of the fields:

- **A**: Acceptable. The algorithm and key length are safe to use. No security risk is currently known.
- **D**: Deprecated. The use of the algorithm and key length is allowed, but the user must accept some risk.
- **X**: Disallowed.
- **N**: Not approved.
- **R**: Restricted. The use of the algorithm or key length is deprecated, and there are additional restrictions required to use the algorithm or key length for applying cryptographic protection to data.
- **U**: Unknown. The system cannot determine the status.

Name	Description
Details	Show or hide the detailed information of the selected connection link.
Dir	Link direction (inbound or outbound).
Local Port	Local Security Module port.
Remote IP	Remote IP address.
Remote Port	Remote port.
Remote FQDN/IP	Remote FQDN or IP address.
Transport	Transport protocol (UDP, TCP, TLS).
Policy	Security Policy (Trusted, Default, Instance)
Cert Sign	Certificate Signature. Digital signature algorithms (for example, RSA or DSA) and the cryptographic hash function (for example, SHA) of the certificate in use by the TLS connection.
Key Exch	Key exchange algorithm (for example, RSA, DSA, Diffie-Hellman,) and key bit length (for example, 1024, 2048) to establish symmetric keys between the endpoints on the TLS connection.
Encryption	Cryptographic operation that provides confidentiality of the data being carried on the TLS connection.
MAC	Message Authentication Code algorithm (for example, SHA) that authenticates the TLS data and provides integrity and authenticity assurance on the message.

Connection Details section

The Connection Details section displays detailed information for the selected connection.

Name	Description
Direction	Link direction.
Creation time	Link creation time.
Last message received	Last message received time.
Last message sent	Last message sent time.
Messages/Bytes Received	Received message count and byte count.
Messages/Bytes Transmitted	Transmitted message count and byte count.
Messages/Bytes Dropped	Dropped message count and byte count.
Subject	The subject field identifies the entity associated with the public key stored in the subject public key field of the X.509 certificate.
Alt Subject	Alt subject is an extension to X.509 that allows various values to be associated with a security certificate.
CA	The issuer who signed the certificate.
Cipher	The negotiated TLS cipher suite. The cipher suite includes the Key Exchange, Encryption and MAC algorithms.
Public Key Algorithm	The encryption algorithm of the public key (e.g. RSA, DSA or Diffie-Hellman).
Key Size (bits)	The Public Key length.
q bits size	For DSA public keys, this represents the q parameter size.
Signature Algorithm	The identifier for the cryptographic algorithm used by the CA to sign this certificate.
MAC Algorithm	The Message Authentication Code (MAC) algorithm to verify data integrity.

SIP Firewall Status

Viewing SIP Firewall status

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **SIP Firewall Status** to open the SIP Firewall Status page.

Result

The SIP Firewall Status page shows the SIP Firewall processing status for each Session Manager and Branch Session Manager instances.

Auditing Firewall configuration

About this task

You can perform periodic audit of Firewall configuration to ensure the functioning state of the SIP Firewall. The audit operation checks for Rule Set upgrades and imports the latest default Rule Sets. The system also performs the audit operation automatically at every 5 minutes.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **SIP Firewall Status** to open the SIP Firewall Status page.
3. Click **Audit** to open the Rule Set Audit and Repair Results page.
4. Click **Done**.

Result

Rule Set Audit and Repair Results page shows the details of the SIP Firewall configuration state for all Session Manager and Branch Session Manager instances.

SIP Firewall Status page field descriptions

Button	Description
Reset	Resets all the processing counters of selected Session Managers and Branch Session Managers to zero, except for *Loop Detection* counters. Also, resets all the Rule matching counts to zero. **Note:** After a reset operation, the system updates the counts from the last reset time.
Audit	Performs sanity audit of the Session Manager Rule Set assignments. The Audit process also checks for Rule Set upgrades and imports pending default Rule Sets.
Configure	Navigates to the *SIP Firewall Configuration* page.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Details</td><td>Displays the detailed SIP Firewall processing status, for each Rule, of the selected Session Manager.

Rule Matching table
<table><tr><td>Name</td><td>Description</td></tr><tr><td>Rule</td><td>The name of the Rule.</td></tr><tr><td>Match</td><td>For the selected Session Manager, shows the matched count of the Rule.</td></tr><tr><td>Drop</td><td>For the selected Session Manager, shows the dropped count of the Rule.</td></tr></table></td></tr>
<tr><td>SM</td><td>The name of the Session Manager.</td></tr>
<tr><td>Type</td><td>Specifies the Session Manager type.</td></tr>
<tr><td>Rule Sets</td><td>The name of the Rule Set assigned to Session Manager.</td></tr>
<tr><td>Reset Time</td><td>The last reset time of the SIP Firewall processing counts.

Note:

Only Session Manager and Branch Session Manager of release 6.3.4 and later shows the reset time.</td></tr>
<tr><td>Processing Counts</td><td>Shows the summary of counts for Rules, Whitelist, Blacklist, and Loop Detection. Loop Detection counts do not reset.

To view the exact counts, hover your mouse over the Processing Counts column.

Note:

Only Session Manager and Branch Session Manager of release 6.3.4 and later show the processing counts.</td></tr>
</table>

Related Links

Viewing SIP Firewall status on page 449

Registration Summary

Registration Summary

Use Registration Summary module to view the registration status for all Avaya SIP Telephony (AST) devices registered for the selected Session Manager Instance. These AST devices are reloaded or rebooted based on the following actions:

- Reset of endpoints
- Full reload of endpoints
- Partial reload of endpoints
- Failback of endpoints to the primary controller

Viewing Registration Summary

About this task

This module provides the ability to view the basic registration information for a particular device.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Registration Summary** to open the Registration Summary page.

   The Registration Summary page displays the list of registered devices per Session Manager.
3. Click **Refresh** to retrieve the latest Device Summary results.

Rebooting of selected AST devices

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Registration Summary** to open the Registration Summary page.

   The Registration Summary page displays the list of registered devices.
3. Select the AST Device and click **Reboot**.

   The system displays the Confirm Reboot Notification page.
4. On the Confirm Reboot Notification page, click **Confirm**.

   After user confirmation, a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

Reloading of selected AST devices

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Registration Summary** to open Registration Summary page.
3. Click the rows to select SIP AST devices and perform one of the following tasks:
   a. Click **Reload** > **Reload Complete** to force complete reload of selected SIP AST devices that includes maintenance data, configuration data, and a complete data reload.

      On the Confirm Reload Complete Notification page, click **Confirm**.

      After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.
   b. Click **Reload** > **Reload Config** to reload only configuration details of selected SIP AST subscribed devices.

      On the Confirm Reload Config Notification page, click **Confirm**.

      After user confirmation, the system displays a status page showing the detailed information regarding the current state of scheduled and running endpoint actions.
   c. Click **Reload** > **Reload Contacts** to reload only contact details of selected SIP AST subscribed devices.

      On the Confirm Reload Contacts Notification page, click **Confirm**.

      After user confirmation, the system displays the status page showing the detailed information regarding the current state of scheduled and running endpoint actions.

Failback of selected AST devices

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Registration Summary** to open the Registration Summary page.

   The Registration Summary page displays the list of registered devices.
3. Click to select the AST Devices and click **Failback**.

   The system displays the Confirm Failback Notification page.
4. On the Confirm Failback Notification page, click **Confirm**.

Result

This enables failback to the primary Session Manager.

Advanced Searching

Procedure

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
Advanced Search Criteria	In the Advanced Search Criteria section, perform the following steps: a. Define the search criterion by performing the following steps: a. Select the search criterion from the first drop-down list box. b. Select the operator from the second drop-down list box. c. Enter the search value in the third field. b. If you want to add another search condition, click the plus sign (+). c. If you want to delete a search condition, click the minus sign (-) . d. Click **Clear** to clear the fields. e. Click **Search** to search as per the set search criteria. f. Click **Close** to contract the **Advanced Search Criteria** section.

Registration Summary field descriptions

Button	Description
Reboot	Reboots the selected Avaya SIP Telephony (AST) devices.
Reload Complete	Forces complete reload of the selected AST devices.
Reload Config	Reloads only configurations of the selected AST devices.
Reload Contacts	Reloads only contacts of the selected AST devices.
Failback	Ensures that devices failback to Primary Session Manager.

Name	Description
Session Manager	Name of the Session Manager instance.
Type	Either as Session Manager or Branch Session Manager (BSM).

Table continues…

Name	Description
Primary Registered	Number of users registered to this Session Manager as the primary Session Manager.
Primary AST	Number of PPM subscriptions to this Session Manager for users as the primary Session Manager.
Primary Admin	Number of users administered to use this Session Manager as the primary Session Manager. **Note:** Session Manager of type **BSM** does not have any registration status entries in the Primary column group and the system displays the status as "---".
Secondary Registered	Number of users registered to this Session Manager as the secondary Session Manager.
Secondary AST Failover	Number of PPM subscriptions to this Session Manager for users as the secondary Session Manager. This also indicates the failover users since failover users subscribe to the secondary Session Manager.
Secondary Admin	Number of users administered to use this Session Manager as the secondary Session Manager.
Total Registered	Sum of fields **Primary Registered** and **Secondary Registered**.
Total AST	Sum of fields **Primary AST** and **Secondary AST Failover**.
Total Admin	Sum of fields **Primary Admin** and **Secondary Admin**.

User Registrations

User Registrations

The User Registrations module sends notification to the selected SIP AST devices and displays the summary of the user registration status for the SIP AST Device based on the following actions:

- Forced termination of registrations for selected devices
- Reset of selected devices
- Full reload of selected devices
- Only reload configuration for selected devices

- Only reload contacts for selected devices
- Failback of devices to the primary controller

Viewing User Registrations

About this task

Use the User Registrations module to view the basic registration information for a particular user or groups of users.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open User Registrations page.

   The User Registrations page displays the list of registered users.
3. To view the User Registration status based on the following view options, click **View** and select the one of the viewing options.

User	For viewing current default view.
Time Detail	For viewing diagnosis of endpoint registration oriented problems.
Device	For viewing all available device specific information.
Active Controller	For viewing more detailed registration time view.
SM	For viewing that Session Managers are associated with the user registration.
Customized	For viewing custom views.
Create Customized	For customizing the display columns for viewing the user registration details.

4. To view individual row details, click the **Show** or **Hide** link under **Details** column to display or hide the details that have the following tabbed panes:

User	For viewing user specific details.
Registration	For viewing the registration specific details.
Device	For viewing device specific details.
Simultaneous	For viewing details of simultaneous registered devices.
History	For viewing the details of current and past AST devices associated with this user.

5. Click **Refresh** to retrieve the latest user registration summary results.

Customizing column display

About this task

You can customize the column display on the User Registrations page. Use any of the following methods to customize a column display:

- Select the columns you need to get displayed in the table
- Order the appearance of the columns
- Reset the column appearance to the default columns

Note:

The customization settings are valid for the current user session, that is, after the user logs out, the customization settings revert to the default appearance.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open User Registrations page.
3. Click **Customize** link to view this section.
4. Select columns in **Available Columns** and click the **Move** link to move the selected columns to **Display Columns** list. Click **Move All** link to move all columns to be displayed.
5. Click **Remove** and **Remove All** links to remove selected or all columns from displayed columns.
6. To rearrange the selected columns under **Display Columns**, perform the following steps:
   a. Click the **Top** link to move the selected column to the top of the list.
   b. Click the **Up** link to move the selected column one position up on the list.
   c. Click the **Down** link to move the selected column one position down on the list.
   d. Click the **Up** link to move the selected column to the bottom of the list.
7. Click **Default** to restore the default settings.
8. Click **Apply** to save the changed settings.
9. Click **Close** to close the customization section.

Forcing unregistration of device registration

About this task

This feature enables forced unregistration of any registered device and is not limited to only AST devices. These devices respond based on device settings.

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open the User Registrations page.

   The User Registrations page displays the list of registered devices.
3. Select the device and click **Force Unregister**.

   The system displays the Confirm Force Unregister Notification page.
4. On the Confirm Force Unregister Notification page, click **Confirm**.

   After user confirmation, a status page appears showing the detailed information of the unregistration action.

Rebooting of selected AST devices

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open User Registrations page.

   The User Registrations page displays the list of registered users.
3. Click to select the AST Devices and click **Reboot**. The Confirm Reboot Notification page appears.
4. On the Confirm Reboot Notification page, click **Confirm**.

   After user confirmation, a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

Reloading of selected AST devices

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open User Registrations page.
3. Click the rows to select the SIP AST Devices and do one of the following:
   a. Click **Reload** > **Reload Complete** to force complete reload of selected SIP AST Devices that includes maintenance data, configuration data, and a complete data reload.

      On the Confirm Reload Complete Notification page, click **Confirm**.

After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

b. Click **Reload** > **Reload Config** to reload only configuration details of selected SIP AST subscribed devices.

   On the Confirm Reload Config Notification page, click **Confirm**.

   After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

c. Click **Reload** > **Reload Contacts** to reload only contact details of selected SIP AST subscribed devices.

   On the Confirm Reload Contacts Notification page, click **Confirm**.

   After user confirmation a status page appears showing the detailed information regarding the current state of scheduled and running endpoint actions.

Failback of selected AST devices

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **User Registrations** to open User Registrations screen. The User Registrations screen displays the list of registered users.
3. Click to select the AST Devices and click **Failback**. The Confirm Failback Notification page appears.
4. On the Confirm Failback Notification page, click **Confirm**.

Result

This enables failback to the primary Session Manager.

Advanced Searching

Procedure

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
Advanced Search Criteria	In the Advanced Search Criteria section, perform the following steps: a. Define the search criterion by performing the following steps: a. Select the search criterion from the first drop-down list box. b. Select the operator from the second drop-down list box.

Table continues…

	c. Enter the search value in the third field. b. If you want to add another search condition, click the plus sign (+). c. If you want to delete a search condition, click the minus sign (-) . d. Click **Clear** to clear the fields. e. Click **Search** to search as per the set search criteria. f. Click **Close** to contract the **Advanced Search Criteria** section.

User Registrations field descriptions

Customize Column Display section

List	Description
Available Columns	Shows the list of available columns.
Display Columns	Shows the list of selected columns.

Link	Description
Customize	Expands **Customize Column Display** section.
Move	Moves selected items from **Available Columns** list to the **Display Columns** list.
Move All	Moves all items from **Available Columns** list to the **Display Columns** list.
Remove	Removes selected items from the **Display Columns** list.
Remove All	Moves all items from the **Display Columns** list.
Top	Moves the selected items of **Display Columns** list to the top of the list.
Up	Moves the selected items of **Display Columns** list to one position up in the list.
Down	Moves the selected items of **Display Columns** list to one position down in the list.
Bottom	Moves the selected items of **Display Columns** list to the bottom of the list.

Button	Description
Default	Reverts back to the default column settings of **Available Columns** and **Display Columns** lists.
Apply	Applies the changes made in the column customizing lists to the **AST Device Notifications** section.
Close	Collapses **Customize Column Display** section.

AST Device Notifications: section

The **As of (time)** label indicates the time of the last update of information for the **AST Device Notifications** section.

Button	Description
View > **Default**	For viewing current default view.
View > **User**	For viewing the user specific information.
View > **Time Detail**	For viewing diagnosis of endpoint registration oriented problems.
View > **Device**	For viewing all available device specific information.
View > **Active Controller**	For viewing registration information of the actively controller Session Manager for AST devices.
View > **SM**	For viewing which Session Managers are associated with the user registration.
View > **Customized**	For viewing custom views.
View > **Create Customized**	For customizing the display columns for viewing the user registration details.
Force Unregister	Forces termination of registrations for selected devices.
Reboot	Reboots selected AST devices.
Reload Complete	Forces complete reload of selected AST devices.
Reload Config	Reloads configurations of selected AST devices.
Reload Contacts	Reloads contacts of selected AST devices.
Failback	Enable devices to failback to Primary Session Manager.

Default View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
First Name	Shows the administered first login name.
Last Name	Shows the administered last login name.
Actual Location	Name of the registration location.
IP Address	Indicates numeric IP address of the end point.
Remote Office	Shows whether the incoming IP Address has been correlated with an administered "Remote Office - SIP Proxy Mapping".
Shared Control	Indicates that this registration, like Avaya OneX Communicator, controls another endpoint.

Table continues…

Name	Description
Simultaneous Devices	Number of devices registered and the maximum administered devices.
AST Device	Indicates an AST device.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

User View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
First Name	Shows the administered first login name.
Last Name	Shows the administered last login name.
Home Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
IP Address	Indicates numeric IP address of the end point.
Simultaneous Devices	Number of devices registered and the maximum administered devices.
AST Device	Indicates an AST device.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

Time Detail View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
IP Address	Indicates numeric IP address of the end point.
PPM Subscription Time (AC)	Indicates the subscription time for PPM services of AST endpoint.
Registration Time Prim	Indicates the registration time for the Primary Session Manager.
Registration Interrupted Prim	Indicates the last time when the registration was interrupted for the Primary Session Manager.

Table continues…

Name	Description
Registration Time Sec	Indicates the registration time for the Secondary Session Manager.
Registration Interrupted Sec	Indicates the last time when the registration was interrupted for the Secondary Session Manager.
Registration Time Surv	Indicates the registration time for the Survivable Session Manager.
Registration Interrupted Surv	Indicates the last time when the registration was interrupted for the Survivable Session Manager.

Device View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
IP Address	Indicates numeric IP address of the end point.
Remote Office	Indicates whether the incoming IP address correlates with an administered Remote Office — SIP Proxy Mapping.
MAC Address	MAC address of the endpoint.
Device Vendor	Device information from PPM.
Device Type	Device information from PPM.
Device Model	Device information from PPM.
Device Version	Device information from PPM.
Simult. Devices	Number of devices registered to the maximum number administered.

Active Controller View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
Actual Location	Name of the registration location.
Active Controller	Name of the Active Controller
Registration Time (AC)	Indicates the registration time for the Active Controller.
Registration Interrupt Time (AC)	Indicates the time duration since the last interruption occurred for the Active Controller.

Table continues…

Name	Description
Registration Interrupted (AC)	Indicates the last time when the registration was interrupted for the Active Controller.
AST Device	Indicates an AST device.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

SM View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
Home Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
Actual Location	Name of the registration location.
Active Controller	Name of the Active Controller
Primary SM	Primary Session Manager of the user profile.
Secondary SM	Secondary Session Manager of the user profile.
Survivable SM	Survivable Session Manager of the user profile.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

Customized View:

Name	Description
Details	Shows the options for viewing the Registration Detailed section.
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
First Name	Shows the administered first login name.
Last Name	Shows the administered last login name.
Home Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
IP Address	Indicates numeric IP address of the end point.
Simultaneous Devices	Number of devices registered and the maximum administered devices.

Table continues…

Name	Description
AST Device	Indicates an AST device.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

Create Customized view is same as Customize Column Display section as shown above.

Details section

User Tab:

Name	Description
First Name	Shows the administered first login name.
Last Name	Shows the administered last login name.
Login Name	Shows the administered user login name.
Registration Address	The Communication Address/handle user logged in with.
All Addresses	All of the SIP Communication Addresses the user has administered.
Home Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
Actual Location	Name of the registration location.
Primary SM	Primary Session Manager of the user profile.
Secondary SM	Secondary Session Manager of the user profile.
Survivable SM	Survivable Session Manager of the user profile.
Simultaneous Devices	Number of devices registered to the maximum number administered.
ELIN Number	The ELIN sent from ELIN server associated with the primary controller for a user.
ELIN Last Updated	The date and time that the ELIN was last updated by ELIN server based on the location of Session Manager. Format is: www mmm dd hh:mm:ss TMZ yyyy", where: • www implies day of the week • mmm implies month • dd implies date • hh:mm:ss implies hour (military time):minutes:seconds • TMZ implies time zone

Table continues…

Name	Description
	• yyyy implies year For example, Fri Feb 11 15:56:36 MST 2011.

Registration Tab:

Name	Description
Registration Address	The Communication Address/handle user logged in with.
IP Address	Indicates numeric IP address of the end point.
Active Controller	Session Manager currently serving the endpoint SIP signaling and event subscriptions.
PPM Subscription Time (AC)	Indicates the subscription time for PPM services of AST endpoint.
Event Subscriptions	Event subscription details.
Instance Id	SIP User Agent Instance Id as URN (Uniform Resource Name):UUID (Universally Unique IDentifier).
Primary Registration Time	Indicates the registration time for the Primary Session Manager.
Primary Registration Interrupted Time	Indicates the time duration since the last interruption occurred for the Primary Session Manager.
Primary Registration Interrupted	Indicates the last time when the registration was interrupted for the Primary Session Manager.
Secondary Registration Time	Indicates the registration time for the Secondary Session Manager.
Secondary Registration Interrupted Time	Indicates the time duration since the last interruption occurred for the Secondary Session Manager.
Secondary Registration Interrupted	Indicates the last time when the registration was interrupted for the Secondary Session Manager.
Survivable Registration Time	Indicates the registration time for the Survivable Session Manager.
Survivable Registration Interrupted Time	Indicates the time duration since the last interruption occurred for the Survivable Session Manager.
Survivable Registration Interrupted	Indicates the last time when the registration was interrupted for the Survivable Session Manager.

Device Tab:

Name	Description
MAC Address	MAC address of the endpoint.
IP Address	Indicates numeric IP address of the end point.

Table continues…

Name	Description
Remote Office	Indicates whether the incoming IP address correlates with an administered Remote Office — SIP Proxy Mapping.
Remote Office SIP Proxy Name	Name of the SIP Proxy.
Active Controller	Name of the Active Controller
Event Subscriptions	Event subscription details.
AST Device	Indicates an AST device.
Device Vendor	Device information from PPM.
Device Type	Device information from PPM.
Device Model	Device information from PPM.
Device Version	Device information from PPM.

Simultaneous Tab:

Shows all other registrations associated with this user.

Name	Description
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
IP Address	Indicates numeric IP address of the end point.
MAC Address	MAC address of the endpoint.

History Tab:

Shows up to 10 of the last device registrations performed by this user.

Name	Description
MAC Address	MAC address of the endpoint.
Vendor	Device information.
Type	Device information.
Model	Device information.
Version	Device information.

Session Counts

SIP sessions count

Session Manager Element Manager collects, monitors, and logs the number of concurrent SIP sessions in the system. As the total number of session licenses used is equal to the number of

concurrent SIP sessions, you can use the SIP sessions count feature to monitor and report the number of session licenses used by the system.

The system raises an alarm in the following conditions:

- In the case of a single occurrence of an event where the number of concurrent SIP INVITE sessions exceeds the authorized number of session licenses.
- If the number of concurrent SIP INVITE sessions in use continues to exceed the number of authorized licenses. In this condition, the system raises a new alarm once every 24 hours until either the number of concurrent SIP INVITE sessions is reduced below the number of authorized licenses or the number of authorized licenses is increased to be equal to or greater than the number of concurrent SIP INVITE sessions.

Note:

The system raises an alarm if a valid license file is not installed on the system.

SIP sessions count functionality enables historical analysis of SIP sessions count data for the system or the selected Session Manager instance and allows:

- The generation of graphs of the analyzed data.
- The export of the analyzed data as a report in the comma separated value (CSV) or XML format.

Using the generated reports, you can conduct a time based analysis of the license usage of the system.

Viewing Session Count data

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Session Counts** to open the Session Counts page.
3. In the **Session Manager** field, select the Session Manager instance.
4. Specify the date and time for the required period of the session counts data.
5. Click **Generate Graphs** for viewing the data in graphical format.

Exporting analyzed Session Count data

Procedure

1. On System Manager Web Console, click **Elements** > **Session Manager**.
2. In the left navigation pane, click **System Status** > **Session Counts** to open the Session Counts page.
3. Select the required Session Manager instance.

4. Specify the date and time for the required period of the session counts data.
5. Specify **Export Data Range** and **Export Data Format**.
6. Click **Download Data** to save a copy of the generated report.

Session Counts field descriptions

Name	Description
Global Session Status as of	Indicates when the session count data was last updated.
Sessions Used	The number of SIP sessions currently used by the system.
Sessions Available	The number of SIP sessions authorized for usage by the system.
Session Manager	The Session Manager instance or all Session Manager instances for which session count data is desired.
Data Available	The period for which session count data is available.
Date and Time	The period of the session count data. Predefined values: 1. all dates and times • last month • last week • today • yesterday 2. Last: 1-99 Days or Hours 3. Between: Specified Date Range
Generate Graphs	Generates session count graphs based on specified parameters.
Export Data Range	The period for which session count data must be exported: • All – Retrieve all data for specified Session Manager. • Selected Range – Retrieve data based on the Date and Time field selection.
Export Data Format	The format of downloaded session count data: CSV or XML.
Download Data	Exports session count data based on the specified parameters.

User Data Storage status and Call History management

Use the User Data Storage status screen to manage, monitor, backup, and restore User Data Storage on Session Managers.

User Data Storage only stores the call logs of a user.

Note:

The User Data Storage backup is *not* related in any way to the System Manager backup.

Viewing the User Data Storage Status screen

Procedure

On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.

Data Server Status field descriptions

The Data Server Status screen displays the status of the User Data Storage data server.

The User Data Storage **Status** on the Session Manager can be one of the following states:

- Normal Operation
- Auditing: Call History information is being audited and obsolete data is being removed.
- Restoring: User Data Storage is being restored from a backup server file.
- Backing Up: An on-demand or automated backup is in progress.
- Needs Repair: A Restore action has failed.

Name	Description
Details	Show or hide the details of the last action that was performed on the Session Manager.
SM	Name of the core Session Manager.
Status	Current state of the User Data Storage on the Session Manager.
Connect Test	Status of the maintenance connection test to the User Data Storage server.
Last Action	The last action performed on the User Data Storage server. An action can be: • Audit • Backup • Restore

Table continues…

Comments on this document? infodev@avaya.com

Name	Description
	• Recreate
Last Action Status	Result of the last action performed (Complete or Failed).
Last Action Time	The requested or completion time of the **Last Action** .
Disk Usage	Cumulative disk usage for data storage.

User Data Storage backup

Backups and audits run on a daily basis at 1:15 AM local time on the Session Manager. The backup server audit removes extra backup files at 2:15 AM local time on the System Manager.

The User Data Storage backup feature:

- is *not* related in any way to the System Manager backup.
- does not pre-allocate space. The administrator must administer a location for backup files. 4 GB of space is adequate for this release, but more space will need to be allocated over time.
- makes a backup directly from the Session Manager to the backup location.
- backs up call history data only.

If the user does not configure a backup server:

- a warning message displays until the user configures a backup server location.
- no backups are made.
- the status page displays that no backup server is configured.

Backup and Restore field descriptions

Use this screen to configure and monitor User Data Storage backups and recoveries. The backup server must be in place before configuring the backup information.

The fields display **- -**:

- If the system cannot retrieve the status of a Session Manager.
- If the Session Manager is running a release earlier than 6.3.8.

Backup Host	Name of the backup server.
File Transport	Type of file transport in use.
Directory	Location on the backup server to store the backup files.
Directory Disk Used	Amount of disk space used for the backup file
Retained Copies	Number of backup copies saved on the backup server per Session Manager.

Button	Description
Backup	Start the backup process on the selected Session Managers.
Restore	Start the restore process on the selected Session Managers.
Configure Backup	Configure backup server location and directory for backup file storage.
Audit Backup	Audit the backup configuration, status, and directory. Provides an option to remove unnecessary files to reclaim disk space.

Name	Description
Details	Show or hide the backup file details for a selected Session Manager (File Name, Backup Date, File Size, Session Manager Release).
SM	The name of the core Session Manager.
Backup Status	Indicates the status of the last backup (Complete or Failed).
Backup Files	The number of backup files that are stored on the backup server for the selected Session Manager.
Last Backup Time	The time a backup was last run on the selected Session Manager.
Last Restore Status	The status of the last Restore request on the selected Session Manager (Complete or Failed).
Last Restore Time	The time a restore request was last run on the selected Session Manager.

Administering Backup Storage Configuration

Use the Backup Storage Configuration screen to create or change the backup server configuration information.

Backups and audits run on a daily basis at 1:15 AM local time on the Session Manager. The backup server audit removes extra backup files at 2:15 AM local time on the System Manager.

Important:

The backup server must support the SSH2 protocol.

Warning:

If you change the server or backup file location directory using this screen, existing backup files are not automatically moved to the new location and are not available for restoring. The user must move the backup files to the new location and remove files from the unused location.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Backup and Restore**.
3. Click **Configure Backup**.
4. Enter the required information. See Backup Storage Configuration field descriptions on page 536.
5. Do one of the following:
   - Click **Commit** to save the configuration changes.
   - Click **Test Connection** to verify the configuration information is correct.
   - Click **Cancel** to cancel the configuration request.

Backup Storage Configuration field descriptions

Button	Description
Commit	Accept and store the configuration changes to the database.
Test Connection	Test the SSH connection, directory access for the login, and write/delete permissions.
Cancel	Do not make any changes to the existing configuration information.

Name	Description
Hostname or IP Address	Hostname or IP address of the SSH-accessible server.
Login	The login that has SSH privileges and can gain access to the server.
Password **Confirm Password**	The password associated with the login.
Backup File Transfer	The default is **SFTP**. **SCP** is a slightly faster transport but can be affected by interrupts.
SSH Port	The default is 22.
Directory	The directory location where backup files are stored on the backup server.
Retained backup copies per SM	The maximum number of backup file copies retained for each Session Manager on the backup location.

Backing up User Data Storage

Run the backup immediately. Running the backup on demand does not alter the nightly backup schedule.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.

2. Click **Backup and Restore**.
3. Select the Session Manager or multiple Session Managers on which to run the backup.
4. Click **Backup**.
5. Click **Confirm** to start the backup process, or **Cancel** to cancel the backup request.

Restoring User Data Storage

The restore operation:

- Only restores call history information that exists in a backup file.
- Deletes call history information that exists only in the database.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Backup and Restore**.
3. Select the Session Manager on which to run the restore operation.
4. Click **Restore**.
5. In the **Restore File** column, select the appropriate file you want to restore from the drop-down menu.
6. Do one of the following:
   - Click **Commit** to accept the selection.
   - Click **Reset** to reload the **Restore File** selection list.
   - Click **Cancel** to cancel the restore request and return to the User Data Storage screen.
7. Click **Confirm** to send a request to each Session Manager to begin the restore operation using the selected file, or click **Cancel** to cancel the restore request.

Auditing a Backup Storage Location

The audit runs on the backup server and provides a summary status of the backup server and files.

The Audit Backup Storage Location screen also displays the files which will be removed in the next nightly audit. If not enough disk space is currently available, the administrator can click **Remove Pending** to immediately remove the pending files on the backup server.

Backups and audits run on a daily basis at 1:15 AM local time on the Session Manager. The backup server audit removes extra backup files at 2:15 AM local time on the System Manager.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Backup and Restore**.
3. Select a Session Manager from the **SM** list.

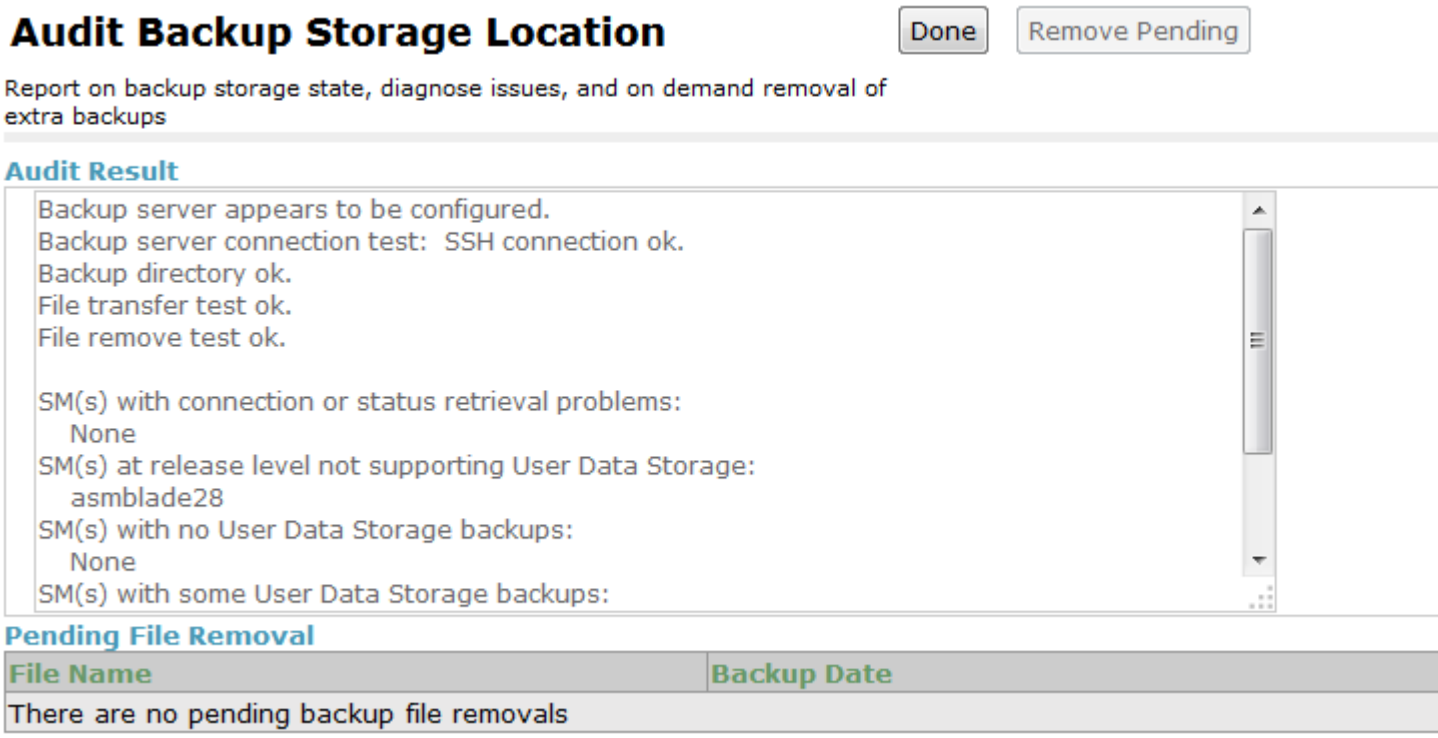
4. Click **Audit Backup**.

   The system displays the results of the audit.

5. To immediately remove any files listed under **Pending File Removal**, click **Remove Pending**.
6. Click **Done**.

Example

The audit displays results similar to the following:



Call History

Starting with Session Manager Release 6.3.8, logged out missed call information is saved for both H.323 and SIP endpoints.

- For H.323 endpoints, Communication Manager stores logged out missed calls and downloads the Call History logs when the endpoint logs in.
- For SIP endpoints, the primary Session Manager stores all call logs and downloads the logs to the endpoint during login. The endpoint maintains the logs locally while logged in. Call logs are only stored on the primary Session Manager of the user. No call logs are stored on the secondary Session Manager for the user. Call log storage is not redundant..

You control Call History logging for the SIP user by selecting or deselecting the **Enable Centralized Call History** check box on the Session Manager Communication Profile screen. The check box is

deselected by default (disabled). The maximum number of call logs for each Communication Profile is 100. You cannot configure the maximum number of call logs.

Administering Call History

Enable or disable call history collection for a user.

Warning:

When a user logs in for the first time after the **Centralized Call History** check box is selected for that user, all calls that were made or received by that user before enabling **Centralized Call History** are lost.

Procedure

1. On the home page of the System Manager Web Console, under **Users**, click **User Management** > **Manage Users**.
2. Do one of the following:
   - If you are adding a new user, click **New** and add the information for the new user.
   - If you are enabling/disabling call history collection for a current user, select the user and click **Edit**.
3. On the User profile Edit: screen, click the **Communication Profile** tab.
4. Select the **Session Manager Profile** checkbox.
5. Under the **Call History Settings** section, select (enable) or clear (disable) the **Enable Centralized Call History?** check box.
6. Click **Commit**.

Administering Call History for SIP users with the Communication Profile Editor

You can bulk enable or disable the call history collection for all SIP users or selected SIP users.

Warning:

When a user logs in for the first time after the **Centralized Call History** check box is selected for that user, all calls that were made or received by that user before enabling **Centralized Call History** are lost.

Procedure

1. On the System Manager web console home page, under **Elements**, click **Session Manager** > **Communication Profile Editor**.
2. Select a user, select multiple users, or select **All**.
3. In the **New Communication Profile Values** section, under **Call History Settings**, select a value from the **Enable Centralized Call History** drop-down menu.
4. Click **Commit**.

Viewing the Call History Status screen

Use this screen to manage and monitor call history tables in the User Data Storage database.

An audit runs every night at 1:15 a.m. local time to the Session Manager. The audit deletes the call history logs of a user who is permanently deleted or is assigned to another Session Manager.

The audit compacts the table storage after it completes.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Call History Status**.

Call History Status field descriptions

Button	Description
Audit	Audit the call history and remove entries for deleted users, users with deleted Session Manager Communication Profiles, and users who have been reassigned to another Session Manager. Compact the data storage table after removing the affected files.

Name	Description
Details	Show or hide the Call Log Table details for a selected Session Manager.
SM	The name of the core Session Manager.
Last Audit	The time when an audit process last ran. Audits run nightly or on-demand.
Call Log Records	The total number of records in the Call Log table.
Call Id Records	The total number of records in the Call Log Id table.
Primary SIP Users	Number of SIP users assigned to the Primary Session Manager.
Call History Users	The number of users who have Call History enabled in their Session Manager Communication Profile.

Chapter 11: Managing system events

Managing alarms

Alarming

The Alarming service provides an interface for monitoring alarms generated by System Manager and other components. You can:

- View an alarm.
- Change the status of an alarm.
- Export alarms to a Comma Separated Values (.csv) file through the Alarming service.

System Manager generates alarms to notify users of system events. Alarms are classified by their effect on system operation. Alarms can also identify the system component that generated the alarm.

Note:

- System Manager cannot forward traps to NMS for:
  - Release 6.1 elements with the 6.1 SAL agent.
  - Release 6.2 elements with the 6.2 serviceability agent.

  You can configure 6.1 elements with the 6.1 SAL agent and 6.2 elements with the 6.2 serviceability agent to send SNMP traps directly to a customer Network Management System (NMS).
- For Release 6.2.x elements, you can configure the serviceability agent from System Manager instead of configuring in each element.
- For Release 5.2 elements and Release 6.0 elements, you can configure System Manager to forward alarms to the Avaya Data Center (ADC).

For more information about configuring alarms, see SNMP support for Session Manager on page 716.

Viewing alarms

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, select an alarm from the Alarm List. You can select multiple alarms.
4. Click **View**.

   The system displays the alarm details on the Alarm - View Alarm Detail page.

Changing the alarm status

The status of an alarm can be:

- **Acknowledged**: Maintenance support must manually set the alarm to this state. Indicates the alarm is under investigation.
- **Cleared**: Maintenance support must manually set the alarm to this state. Indicates the error condition has been resolved.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, select an alarm and click **Change Status**.

   You can select multiple alarms.
4. Click the status that you want to apply to the selected alarms.

Exporting alarms

You can export alarms to a Comma Separated Values (.csv) file. You can open the CSV file using a text editor such as Wordpad or a spreadsheet application such as Microsoft Excel.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, perform one of the following actions:
   - To export an alarm to a CSV file, select an alarm and click **More Actions** > **Export Selected**.
   - To export the filtered alarms to a CSV file, click **More Actions** > **Export All**.

When you use **Advanced Search** or **Filter** option to filter alarms based on some criteria, **Export All** exports all the filtered data.

4. Click **Save** to save the exported file to the local disk.

Filtering alarms

The criteria for filtering the alarms are Severity, Status, Host Name, Message, Identifier, and M/E Ref Number. You can use more than one filter criterion on the selected alarms.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, select the alarms you want to filter.
4. Click **Filter: Enable** at the top right corner of the Alarm List table.
5. Select the filter criteria you want to apply to the selected alarms.

   The **Status** and **Severity** fields have drop-down menus.

   You can enter the alarm code in the Message field to find all alarms that contain a particular alarm code.
6. Click **Filter: Apply**.

   Note:

   The system displays a message if no records are found that match the specified filter criteria.

Result

The system displays the alarms that match the filter criteria.

Searching for alarms

Use the Advanced Search function to find alarms based on certain specified conditions. The system displays only those alarms that satisfy the search conditions. You can specify multiple search conditions.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, click **Advanced Search**.
4. In the **Criteria** section, from the first and second drop-down fields, select the search criterion and the operator.

The default value in the first drop-down field is **Time Stamp**.

5. Select or enter the search value in the third field.
6. To add another search condition, click **+** and perform the following:
   a. Select the AND or OR operator from the drop-down field.
   b. Repeat Step 4 and Step 5.

   To delete a search condition, click **-**. You can delete a search condition only if you added more than one search condition.
7. To find alarms for the given search conditions, click **Search**.

Managing Geographic Redundancy related alarms

Forwarding the secondary System Manager alarms to the primary System Manager server

Before you begin

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

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents.**

   The system displays the entries for the primary and the secondary System Manager.
3. Create a target profile of the primary System Manager server, and copy the profile to the secondary System Manager server.

   The system forwards the secondary System Manager alarm to the primary System Manager server.

Viewing the secondary System Manager alarms

About this task

You can view the alarms for the secondary System Manager that is in the standby mode.

Procedure

1. Log in to System Manager through CLI as root.
2. Type `sh $MGMT_HOME/alarmingui/scripts/DisplayAlternateDBAlarms.sh`.
3. At the prompt, type the number that matches the option that you must select from the following options:
   - (0) Exit
   - (1) Display All Alarm count
   - (2) Display alarm by notification oid (0)

- (3) Display alarm by Status (0)
- (4) Clear Alarm with notification oid (0)
- (5) Display all alarms
- (6) Display Alarms by severity (0)

The system displays the alarms according to the option that you selected.

Alarming field descriptions

The Alarming page displays a list of alarms. Use this page to view the alarms in the **Auto-Refresh** mode. In this mode, the page updates the alarm information automatically.

Field	Description
Time Stamp	The date and time when the alarm is generated.
Severity	The severity of the alarm.
Status	The current status of the alarms.
Host Name/SysName	The name of the host computer that generated the alarm.
Source IP address	The IP address of the system from that generated the alarm.
Description	The detailed description of the problem that generated the alarm.
Identifier	The unique identifier for an alarm.
Event ID	The log event ID if the alarm is generated from logs or the Event OID if the alarm is generated from the trap listener service.
NotificationOID	The SNMP OID of the alarm.
M/E Ref Number/SysOID	The unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm. For alarms that are generated from trap listener, the system displays the System OID.

Button	Description
Alarm landing Page	Changes the mode from **Auto-Refresh** to Manual refresh and displays the Alarming home page. This is a toggle button.

Alarming field descriptions

The Alarming home page contains two sections: upper and lower. The upper section contains buttons that you can use to view the details of the selected alarms, change the status of alarms, search for alarms , and set filters to view specific alarms. The lower section displays alarms in a table. The table provides information about the status of the alarms along with their severity. You can click a column title to sort the information in the table in ascending or descending order.

Field	Description
Time Stamp	The date and time when the alarm is generated.
Severity	The severity of the alarm.
Status	The current status of the alarms.
Host Name / SysName	The name of the host server that generated the alarm. In case of the trap listener service, this column displays the system name.
Source IP Address	The IP address of the system that generated the alarm.
Description	The detailed description of the problem that generated the alarm.
M/E Ref Number / SysOID	The unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm. For alarms that are generated from trap listener, the system displays the System OID.
Identifier	The unique identifier for an alarm.
Event ID	The log event ID if the alarm is generated from logs or the Event OID if the alarm is generated from the trap listener service.
NotificationOID	The SNMP OID of the alarm.

Button	Description
View	The details of the selected alarms.
Change Status	Changes the status of the selected alarm. The options are: • **Acknowledged** • **Cleared**

Table continues…

Button	Description
Auto-Refresh Mode	Changes over to the **Auto-Refresh** mode. When the Alarming page is set in this mode, it automatically updates the alarms in the table. A toggle button.
More Actions > **Export Selected**	Exports the selected alarms to a CSV file. You can view the logs using the Wordpad or Excel application.
More Actions > **Export All**	Exports all the alarms to a CSV file. You can view the logs using the Wordpad or Excel application. **Note:** When you use **Advanced Search** or **Filter** option to filter alarms based on some criteria, **Export All** exports all the filtered data.
More Actions > **Delete Selected**	Deletes the alarms that you select from the list.
More Actions > **Delete ALL**	Deletes all alarms that the system displays on the page.
Advanced Search	Displays fields that you can use to specify the search criteria for searching an alarm.
Refresh	Refreshes the log information in the table.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. A toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. A toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters alarms based on the filter criteria.
All	Selects all the alarms in the table.
None	Clears the check box selections.
Previous	The logs in the previous page. This button is not available if you are on the first page.
Next	The logs in the next page. This button is not available if you are on the last page.

Criteria section

This system displays the section when you click **Advanced Search** on the upper-right corner of page.

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.

Table continues…

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>Select following search criteria from the first drop-down list:
Time Stamp: Searches all of the alarms that match the specified date and time. The valid format for entering the date is MM/DD/YYYY. The valid format for entering the time is HH:MM.
Severity: Searches all the alarms that match the specified severity level.
Status: Searches all the alarms that match the specified status.
Host Name: Searches all of the alarms that are generated from the specified host.
M/E Ref Number: Searches all the alarms that match the specified M/E Ref Number.
Event ID: Searches all the alarms that match the specified Event ID.
Source IP address: Searches all of the alarms that are generated from the specified source IP address.
NotificationID: Searches all the alarms that match the specified NotificationID.
Identifier: Searches all the alarms that match the specified identifier.
Description: Searches all the 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 table lists the operators that are available for a search criterion:<table><tr><th>Criterion</th><th>Operators</th></tr><tr><td>Time Stamp</td><td>=, >, <, >=, <=, >=, !=</td></tr><tr><td>Severity</td><td>Equals, Not Equals</td></tr><tr><td>Status</td><td>Equals, Not Equals</td></tr><tr><td>Host Name</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr><tr><td>Identifier</td><td>=, >, <, >=, <=, >=, !=</td></tr><tr><td>Source IP address</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr></table>*Table continues…*</td></tr>
</table>

Name	Description
	<table><tr><th>Criterion</th><th>Operators</th></tr><tr><td>Event ID</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr><tr><td>Description</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr><tr><td>M/E Ref Number</td><td>Equals, Not Equals, Starts With, Ends With, and Contains</td></tr></table> When you select **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 log viewer

Log Viewer

Log Viewer displays all the logs generated by System Manager and the applications. The Log List displays a list of all the logs. You can view the details of each log, perform a search for logs, and filter specific logs. Log details include information about the event which generated the log, the severity level of the log, and other relevant information. You can search logs based on search conditions and set filters to view logs that match the filter criteria. Log viewer displays only logs that are of type Audit.

Viewing log details

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.

3. On the Logging page, select a log.
4. Click **View**.

Exporting logs

You can export logs to a Comma Separated Values (.csv) file. You can open the CSV file using a text editor such as Wordpad or a spreadsheet application such as Microsoft Excel.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
3. On the Logging page, perform one of the following actions:
   - To export a log to a CSV file, select a log from the list and click **More Actions** > **Export Selected**.
   - To export the filtered logs to a CSV file, click **More Actions** > **Export All**.

     When you use **Advanced Search** or **Filter** option to filter logs based on a specific criteria, **Export All** exports all the filtered data
4. Click **Save** to save the exported log file to the local disk.

Filtering logs

You can filter and view logs that meet the specified filter criteria. To apply the filters, you need to specify the filter criteria in the fields provided under select columns in the table displaying the logs. The column titles are the filter criteria. You can filter logs on multiple filter criteria.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
3. On the Logging page, click **Filter: Enable** at the top right corner of the log table.
4. Enter or select the filter criteria.
5. Click **Filter: Apply**.

   The page displays the logs that match the specified filter criteria.

   Note:

   If no records matching the filter criteria are found, the Management Console application displays a message that no records matching the search criteria are found.

Searching for logs

You can specify conditions for finding logs. The system displays logs that satisfy the search conditions. You can specify multiple search conditions.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Viewer**.
3. On the Logging page, click **Advanced Search**.
4. In the **Criteria** section, from the first and second drop-down fields, select the search criterion and the operator.
5. Select or enter the search value in the third field.
6. If you want to add another search condition, click **+** and repeat the steps 4 through 6.

   Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.
7. To add another search condition, click **+** and repeat the steps 4 through 6.

   Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.
8. Select the **AND** or **OR** operator from the drop-down field.

   This page displays this drop-down field when you specify more than one search condition.
9. Click **Search** to find the logs for the given search conditions.

Logging field descriptions

The Logging page has two sections: the upper section contains buttons that allow you to view the details of the selected logs, search for logs, and set filters. The lower section displays logs in a table. The table provides information about the logs. You can click the title of the column to sort the data of the column in ascending or descending order.

Name	Description
Select check box	Provides the option to select a log.
Log ID	Displays the unique identification number that identifies the log.
Time Stamp	The date and time of the log generation.
Host Name	Displays the name of the system from which the log is generated.

Table continues…

Name	Description
Product Type	Displays 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	Displays the severity level of the log. The following are the type of severities: • **Emergency**: System is unusable. • **Alert**: Action must be taken immediately. • **Critical**: Critical conditions. • **Error**: Error conditions. • **Warning**: Warning conditions. • **Notice**: Normal but significant condition. • **Informational**: Informational messages. • **Debug**: Debug-level messages. **Note:** The colors of severities do not indicate logging severities
Event ID	Displays the unique identification number assigned to the event that generated the log.
Message	A brief description about the log. The message is generated based on the severity level of the log. For a log with severity level debug, the message contains information about debugging an error.
Process Name	The process on the device that has generated the message, usually the process name and process ID.
Facility	The operating system, processes, and applications quantify messages into one of the several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The following are the types of supported facilities: • User-Level Messages • Security/authorization • Log Audit

Button	Description
View	Opens the Log - View Log Detail page. Use this page to view the details of the selected log.

Table continues…

Button	Description
Auto-Refresh Mode	Switches to the Auto-Refresh mode. When the Logging page is set in this mode, it automatically updates the logs in the table. A toggle button.
More Actions > **Export Selected**	Exports the selected logs to a CSV file. You can view the logs using the Wordpad or Excel application.
More Actions > **Export All**	Exports all the logs to a CSV file. You can view the logs using the Wordpad or Excel application. **Note:** When you use **Advanced Search** or **Filter** option to filter logs based on some criteria, **Export All** exports all the filtered data.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a log.
Refresh	Refreshes the log information in the table.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. A toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. A toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters logs based on the filter criteria.
Select: All	Selects all the logs in the table.
Select: None	Clears the selections.
Previous	Displays logs in the previous page. This button is not available if you are on the first page.
Next	Displays logs in the next page. This button is not available if you are on the last page.

Criteria section

This section appears when you click **Advanced Search** on the top right corner.

Name	Description
Criteria	Use this section to specify search conditions. Select the search criteria from the first drop-down field. Select the operator from the second drop-down list. Enter the search value in the text field. Select following search criteria from the first drop-down list: • Log ID: The unique identification number assigned to the log. • Host Name: Name of the system for which log is generated.

Name	Description
	• Product type: A code which uniquely identifies the component which generated the log. For example, product, device, application, service, and so on. • Severity: Severity level of the log. • Message: Brief description about the log. • Event ID: Unique identification number assigned to the event. • Process Name: Process on the device that has generated the message • Time Stamp: Date and time of the log generation. • Facility: The operating systems, processes, and applications quantify messages into one of several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The second drop-down list displays operators. Based on the search criterion that you select in the first drop-down field, only those operators that are applicable for the selected criterion are displayed in the second drop-down list. The following are the list of operators: • Equals • Not Equals • Starts With • Ends With • Contains The operators for Time Stamp are: =, >, <, >=, <=, and !=. When you select Time Stamp from the first drop-down list, the page provides date and time fields for entering the date and time in the respective fields. Enter the date in MM/DD/YYYY format . You can select the date from the calender. You need to enter the time in one of the following formats: • 24Hr • AM • PM

Button	Description
Clear	Clears the search criterion and sets the criterion to the default search criteria.
Search	Searches the logs based on the search conditions.
Close/Advanced Search	Hides the search fields.
+	Adds a search condition.
-	Deletes a search condition

Logging field descriptions

Use this page to view logs in the Auto-Refresh mode. In this mode, the page updates the log information automatically.

Name	Description
Log ID	Specifies the unique identification number that identifies the log.
Time Stamp	Specifies the date and time of the log generation.
Host Name	Specifies the name of the system from which the log is generated.
Product Type	Specifies the code which uniquely identifies the component which generated the log. For example, product, device, application, service and so on. GW600, which is a product type code identifier is an example of the log product type.
Severity	Specifies the severity level of the log. The following are the type of severities: • **Emergency**: System is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant condition • **Informational**: Informational messages • **Debug**: Debug-level messages **Note:** The colors of severities do not indicate logging severities.

Table continues…

Name	Description
Event ID	Specifies the unique identification number assigned to the event that has generated the log.
Message	Brief description about the log. The message is generated based on the severity level of the log. For a log with severity level debug, the message contains information about debugging an error.
Process Name	Specifies the process on the device that has generated the message. This is usually the process name and process ID.
Facility	The operating system, processes, and applications quantify messages into one of the several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The following are the types of supported facilities: • User-Level Messages • Security/authorization • Log Audit

Button	Description
Logging Landing Page	Switches the mode from Auto-Refresh to manual refresh and displays the Logging Home page. This is a toggle button.

Managing log settings

Log Settings

Log Settings displays the loggers and appenders for any log configuration file that you select. You can also modify the logger and appender settings through this menu. The Logger List displays the name and level of the log along with the appender details.

Accessing the Log Settings service

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.

Result

The system displays the **Log Settings** page.

Viewing loggers for a log file

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.

Related Links

Logging Settings field descriptions on page 641

Logging Settings field descriptions

Use this page to view and edit loggers defined in a log file.

Log Settings

Name	Description
Select Log File	The field lists the log files that you can configure.

Logger List

Name	Description
Logger	Specifies the loggers in the selected log files.
Log level	Specifies the log level indicating the level of logging set for the corresponding logger.
Attached Appenders > Name	Specifies the name of the appender.
Attached Appenders > File Path	Specifies the path of the file to which the appender logs the information.
Attached Appenders >Facility	Specifies the process running on the machine that created the log message.
Attached Appenders > host	Specifies the name of the syslog host where the log output is stored.
Show All	Provides you an option to select the maximum number of logger records that you can view at a time.

Button	Description
Edit	Opens the Edit Logger page that you can use to edit loggers.

Related Links

Viewing loggers for a log file on page 641

Editing a logger in a log file

About this task

You can set log levels for loggers which define as to what level of logging the logger logs.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.
4. In the **Logger List** section, select a logger and click **Edit**.
5. On the Edit logger page, in the **Log Level** field select a log level.

   Note:

   As a user of System Manager Communication Manager capabilities, if you want to view the logs for successful events, then change the **Log Level** settings for any specified log to **Info**. The **Info** setting enables the system to log the successful events. When 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 that if you carry out 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.

6. Click **Commit**.

   The log level is set for the selected logger.

Related Links

Edit Logger field descriptions on page 643

Assigning an appender to a logger

About this task

The appender where a logger logs the log messages.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.

4. In the **Logger List** section, select a logger and click **Edit**.
5. On the Edit logger page, click **Attach** in the Attached Appenders section.
6. On the Attach Appender page, select an appender in the **Select Appender** field.
7. Click **Commit**.

   The appender is added to the selected logger and you can view the appender on the **Log Settings** page.

Related Links

Attach Appender field descriptions on page 645

Modifying an appender

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.
4. In the **Logger List** section, select a logger and click **Edit**.
5. On the Edit logger page, select an appender in the **Attached Appenders** section.
6. Click **Edit**.
7. On the Edit Appender page, modify the appender information.

   You can modify information in the **Threshold Log Level**, **Max File Size**, **File Path**, and **Number Of Backup Files** fields
8. Click **Commit**.

Related Links

Edit Appender field descriptions on page 645

Removing an appender from a logger

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.
4. In the **Logger List** section, select a logger and click **Edit**.
5. On the Edit logger page, select an appender in the **Attached Appenders** section.
6. Click **Detach**.

Edit Logger field descriptions

Use this page to edit logger and appender information. You can also add and remove appenders from the loggers.

Logger

Name	Description
Logger	Specifies the name of the logger.
Log level	Specifies the level of logging for which the logger logs the information.

Attached Appender

Name	Description
Appender	Specifies the name of the appender.
Threshold Log Level	Specifies the threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level.
File Path	Specifies the path of the file where the appender logs the information.
Max File Size	Specifies the maximum size in KB, MB, and GB reserved for the appender file.
# Backup Files	Specifies the number of log files that an appender can use to store log information if one log file becomes full. If all the backup files are full, the appender overwrites the previous backup files in the order the files are created.
Facility	Specifies the process running on the machine for which log messages are created.
Host	Specifies the name of the syslog host that stores the log output.
Header	Specifies the header part of the syslog packet. The header part contains timestamp and host name information.
Facility Printing	Specifies the printed message includes the facility name of the application.

Button	Description
Edit	Opens the Edit Appender page. Use this page to modify the appender information.
Attach	Opens the Attach Appender page. Use this page to add an appender to the logger.
Detach	Removes the selected appender from the logger.
Commit	Saves the changes in the logger information to the database.
Cancel	Closes the Edit Logger page and takes you back to the Logging Configuration page.

Edit Appender field descriptions

Use this page to edit the information of an appender.

Name	Description
Logger	Specifies the name of the logger. **Note:** You can only view this information.
Appender	Specifies the name of the appender. **Note:** You can only view this information.
Threshold Log Level	Specifies the threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level .
File Path	Specifies the path of the file where the appender logs the information.
Max File Size	Specifies the maximum KB, MB, and GB reserved for the appender file.
# Backup Files	Specifies the number of log files that an appender can use to store log information if one log file becomes full. If all the backup files are full, the appender overwrites the previous backup files in the order the files are created.

Button	Description
Commit	Saves the changes to the database.
Cancel	Closes Edit Appender page and takes you back to the Edit Logger page.

Attach Appender field descriptions

Use this page to assign an appender to the logger.

Name	Description
Logger	Specifies the name of the logger.
Log Level	Specifies the level of logging for which the logger logs the information.
Select Appender	Specifies the list of appenders that you can assign to the logger.

Button	Description
Commit	Assigns the appender to the logger.

Table continues…

Button	Description
Cancel	Closes the **Attach Appender** page and takes you back to the Edit Logger page.

Managing log harvester

Log Harvester

The Log harvesting service manages the retrieval, archival, and analysis of harvested log files stored in Serviceability Agent enabled hosts or elements. The Serviceability Agent harvests the logs and sends the harvested logs to the Logging Service through HTTPS. The logging service recognizes a successful harvest request related to a harvest profile, accepts the file segments, creates a well-defined file structure, and saves the request in the System Manager node.

You can harvest log files for one or more products of the same or different types running on the same computer or on different computers. The system displays the list of file archives and respective profiles on the log harvesting user interface and the status of each archive is available in the user interface table.

You can perform the following operations using the log harvesting service:

- Create a log harvesting profile to specify the products for which you want to harvest the logs.
- Submit the log harvesting request defined in a profile to the product.
- View the status of the log harvesting request.
- Store the harvested log files of a product in an archive file.
- View the harvested log files stored in the archive file.
- Download the harvested log files to a local computer.
- Search for a matching text in the harvested log files.

Accessing the Log Harvester service

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.

Result

The system displays the **Log Harvester** page.

Creating a new log harvesting profile

About this task

To create a new log harvesting profile, you must specify:

- The host name of the server on which the product is running

  Note:

  If you do not see the host name of CS 1000 when you create the profile, at the command prompt of CS 1000, run the following command:

  ```
  cd /opt/nortel/oam-logging
  ./configureSpiritAgentClient.sh <enrollment password>
  ```

  The system now enrolls CS 1000 to the log harvester of System Manager.

- The product name
- The directories or the log files
- The filter text if you select one or more directories

To harvest log files for products running on different servers, you must specify multiple filter criteria.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, click **New**.
4. On the Create New Profile page, enter the appropriate information in the **Profile Name** and **Profile Description** fields.
5. Select the host name of the server, product, and directories or files from the respective fields.
   - To select multiple directories or files from the respective list boxes, press `CTRL` and click the directories or files.
   - To clear a selection, press `CTRL` and click the item.
   - To add another log harvesting request for a different product or for another instance of the same product running on the same server or on a different server, click plus (**+**).
6. If you select one or more directories, in the **File Name Filter** field, enter a text pattern as the filter criteria.

   During the harvesting operation, the system harvests only those files that match the filter criteria.
7. To save the profile and the log harvesting requests in the profile, click **Save Profile**.

Related Links

Create New Profile field descriptions on page 655

Editing a log harvesting profile

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **Edit**.
4. On the Harvest Criteria Edit page, modify the information in the **Profile Name** and **Profile Description** fields.
5. Modify the hostname of the server, product, and directories or files from the respective fields.
   - To select multiple directories or files from the respective list boxes, press `CTRL` and click the directories or files.
   - To clear a selection, press the `CTRL` and click the item you select.
   - To add another log harvesting request for another product or for another instance of the same product running on the same server or on a different server, click **+**.
6. If you select one or more directories, you can enter a new filter criteria in the text box below the **Directories / Filter Text** field and click **Commit**.

   During the harvesting operation, the system harvests only those files that match the filter text.
7. Click **Save Profile** to save the changes you made to the log harvesting profile.

Related Links

Harvest Criteria Edit field descriptions on page 656

Viewing the harvested log files in an archive

You can view the harvested log files of a product stored in an archive file.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. Click **Show files**.

   On the Search Archives page, navigate through the folders in the archive to view the harvested log files.

Deleting a profile

About this task

You cannot delete a profile that is in use by the Log Harvester service. If you attempt to delete a profile that is in use, the system displays an error message.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **Delete**.
4. On the Profile Delete Confirmation page, click **Delete**.

Note:

When you delete a profile, the system deletes all requests and all archives related to the profile from the file system.

Submitting a request for harvesting log files

About this task

Use this feature to submit a log harvesting request to one or more products running on the same or different servers. After the request is successfully processed, the system on which the products are installed returns the harvested log files that are specified in the request. When you select a profile and click **Request**, the system generates a single request for all the requests contained in the profile.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, enter the relevant information in the **Archive Name** and **Archive Description** fields.

   The system saves the harvested log files in the specified archive file.
5. Click **Run Profile** to send a request.

   The table in the Harvest Criteria View section provides you the status of the log harvesting request. If the execution status of the request is successful, then the system creates a zip file containing the harvested log files and saves the file in the specified location.

Related Links

Harvest Archives field descriptions on page 657

Viewing details of a log harvesting request

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. If the system does not display any requests, submit a new request.
6. Click **View**.

   The Harvest - View Harvest detail page displays the details of the selected request.

Related Links

Harvest - View Harvest detail field descriptions on page 659

Searching for text in a log file

Use this feature to search for matching text in the log file of a product.

About this task

The search is based on Lucene Search. The search results are highlighted as per the Lucene highlighter. The highlight package contains classes to provide *keyword in context* features, typically used for highlighting search terms on the results page.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. Click **Show Files**.
6. On the Search Archives page, in the **Enter search text** field, enter the text for which you want to search.
7. In the Tree view, navigate to the log file by expanding the folders and select the log file.
8. Click **Search**.

   The system displays the search results in the Search Result Panel. The **Search Results Panel** field displays the line numbers as hyperlinks on which the searched text is found.

9. Click the hyperlink in the **Search Results Panel** field.

   The system displays the page that contains the highlighted searched text in the **Log Browser Panel** field.

Related Links

Search Archives field descriptions on page 659

Viewing the contents of harvested log files

About this task

Use this feature to view the log messages stored in the harvested log files for a product. You can view the contents of one log file at a time.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. If the system does not display any requests, submit a new request.
6. Click **Show Files**.

   The system lists the log files that are harvested.

7. Select the log file and click **View**.

   The system displays the file content in the Log Browser Panel pane.

Related Links

Search Archives field descriptions on page 659

Downloading the harvested log files

About this task

You can download the harvested log files of one or more products that you stored in a zip file on your local server.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.

4. On the Harvest Archives page, click a request in the table in the Harvest Request Details section.
5. If the system does not display any requests, submit a new request.
6. Click **Show Files**.
7. On the Search Archives page, select a product name, host name of the server on which one or more products are running, or a directory.
   - If you select a product name, the system creates a zip file that contains the harvested log files for the selected product instances running on the same server or on different servers.
   - If you select a host name of a server under a product, the system creates a zip file that contains the harvested log files for the products running on the server that you selected.
   - If you select a directory, the system creates a zip file containing the harvested log files under the selected directory.
8. Click **Download**.

   The system prompts you to save the file on your local server.
9. Click **Save**.

Related Links

Search Archives field descriptions on page 659

Filtering log harvesting profiles

Use this feature to set filter criteria to view only those log harvesting profiles that meet the set filter criteria. The titles of the columns of the table that displays the log harvesting profiles are the filter criteria.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, click **Filter: Enable**.

   You can find this button at the top right of the table containing log harvesting profiles.
4. Enter or select the filter criteria.

   You can filter the log harvesting profiles by the name, description and creator of the profiles.
5. Click **Filter: Apply**.

   Note:

   If no records matching the filter criteria are found, the Log Harvester page displays a message that no records matching the search criteria are found.

   The log harvesting profile table displays the profiles that matches the specified filter criteria.

Filtering log harvesting requests

Use this feature to set filter criteria to view only those log harvesting requests that meet the set filter criteria. The titles of the columns of the table that displays the log harvesting requests are the filter criteria.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile and click **Requests**.
4. On the Harvest Archives page, click **Filter: Enable**.
5. Enter or select the filter criteria.

   You can filter the log harvesting requests by:

   - The request ID of the log harvesting request. For example, to view the requests starting with Request ID 5, enter `5`.
   - The zip file name that stores the harvested files.
   - The description of the log harvesting request.
   - The location of the archived file that stores the harvested files.
   - The status of the log harvesting request.
   - The description of the log harvesting request status.
6. Click **Filter: Apply**.

   Note:

   If no records matching the filter criteria are found, the Log Harvesting page displays a message that no records matching the search criteria are found.

   The table containing log harvesting requests displays only those log harvesting requests that match the specified filter criteria.

Viewing details of a log harvesting profile

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **View**.

   The Profile Criteria View page contains the details of the log harvesting profile you selected.

Related Links

Profile Criteria View field descriptions on page 656

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	Specifies the name of the log harvesting profile.
Description	A brief description of the profile.
Created By	Specifies the name of the creator of the profile.
Created Time Stamp	Specifies the date and time when the profile was created.

Button	Description
View	Opens the Harvest Archives page. You can use this page to view the details of a selected log harvest profile.
New	Opens the Create New Profile page. You can use this page to create a new log harvesting profile.
Edit	Opens the Edit Profile page. You can use this page to edit a log harvesting profile.
Delete	Deletes the selected profile. You can not delete a profile if the profile is in use by the Log Harvester service.
Requests	Opens the Harvest Archives page. You can use this page to run the log harvesting requests in a selected profile.
Filter: Disable	Hides the fields displayed under the columns on which you can apply the filters without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays fields under the columns in the table where you can enter the filter criteria. Only columns on which you can apply filter display the fields in which you can enter the filter criteria. This is a toggle button.

Table continues…

Button	Description
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 host name of CS 1000 when you create the profile, at the command prompt of CS 1000, run the following command:
	`cd /opt/nortel/oam-logging`
	`./configureSpiritAgentClient.sh <enrollment password>`

Product	The products for which you can harvest logs.
Directories / Filter Text	A list of directories that contains the log files for the selected product.
Files	The log files that you can harvest for the selected product.
Filter Text	The text based on which the log files present under a selected directory are filtered for harvesting. If you select the directory `/a/b/c` and enter `com` in this field, the harvest operation for this profile harvests the log files that are in the directory `/a/b/c`. The log files contain com in the file name. The field does not support wild cards.

Button	Description
+	Specifies another log harvesting request for a product.
-	Deletes the log harvesting request for the product.
Commit	Commits the filter criteria for the selected directories.
Save Profile	Saves the new profile and settings for log harvesting requests in the database.

Harvest Criteria Edit field descriptions

Use this page to edit an existing log harvesting profile.

Name	Description
Profile Name	Displays the name of the log harvesting profile
Profile Description	Displays a brief description of the profile.
Host Name	Displays the hostname of the servers on which you installed the products.
Product	Displays the products for which you can harvest logs.
Directories / Filter Text	Lists the directories that contains the log files for the selected product.
Files	Displays the log files that you can harvest for the selected product
Filter Text	Displays the text based on which the log files present under a selected directory gets filtered for harvesting. If you select the directory `/a/b/c` and enter `com` in the **Filter Text** field, the harvest operation for this profile harvests the log files that contain *com* in the file name. The field does not support wildcards.

Button	Description
+	Allows you to specify another log harvesting request for a product.
-	Deletes the log harvesting request for the product.
Commit	Commits the filter criteria for the selected directories.
Save Profile	Saves the new profile and settings for log harvesting requests in the database.
Cancel	Ignores the changes you make to the Harvest Criteria Edit page and takes you back to the Log Harvester page.

Profile Criteria View field descriptions

Use this page to view the details of a selected log harvest profile.

Name	Description
Profile Name	Displays the name of the log harvesting profile.

Table continues…

Name	Description
Profile Description	A brief description of the profile.
Product	Displays the name of the product for which logs are harvested.
Hosts	Displays the hostname of the server on which the product resides.
Files	Displays the names of the log files for which you can harvest log messages.
Directory	Displays the directory that contains the log files.
Filter Text	The text based on which the log files present under a selected directory are filtered for harvesting. For example, if you select the directory `/a/b/c` and enter the text `com` in this field, the harvest operation for this profile harvests the log files that contain *com* in the file name. This field does not support wild characters.

Button	Description
Done	Closes this page and takes you back to the Harvest Profile List page.
Refresh	Refreshes the records in the table.

Harvest Archives field descriptions

Use this page to create an archive for the log harvesting request. The archive created for a successful harvesting request contains the requested log files in a zip file.

Name	Description
Archive Name	The name of the archive file that you want to create for storing the harvested log files.
Archive Description	A brief description of the archive. This field is optional.

Name	Description
Request Id	The unique identification number assigned to a log harvesting request.
Archive Name	The name of the archive file that you create for storing the harvested log files.
Request Time Stamp	The date and time when the log harvesting request is submitted.
Request Description	A brief description of the log harvesting request.

Table continues…

Name	Description
Status	The status of the log harvesting request. The options are: • SUCCESS: The status is SUCCESS if System Manager successfully harvests the log messages. • FAILURE: The status is FAILURE if System Manager failed to harvest the log messages for the product. • PARTIAL SUCCESS: The status is PARTIAL SUCCESS if System Manager partially harvests the log messages.
Status Time Stamp	The date and time when the execution status of the log harvesting request is generated.
Status Description	A brief description of the log harvesting request status. The description provides you the information about the success or failure of the log harvesting request.
Location	The location where the harvested log messages are archived.

Button	Description
Run Profile	Runs the log harvesting requests for the selected profile.
View	Opens the View Harvest detail page. You can use this page to view the details of a selected log harvesting request.
Show Files	Opens the Search Archives page. You can use this page to search for text contained in the harvested log files, download log files of one or more products running on a same or different servers, view the contents of a log file.
Filter: Disable	Hides the fields displayed under the column filter fields without resetting the filter criteria. A toggle button.
Filter: Enable	Displays fields under the column headers of the table displaying the log harvesting requests. You can enter the filter criteria in these fields. Only columns that can be filtered display the fields in which you can enter the filter criteria. This is a toggle button.
Filter: Apply	Filters the log harvest profiles present in the system based on the filter criteria.

Search Archives field descriptions

Use this page to perform the following activities on the log files contained in an archive:

- View the contents of the harvested log files.
- Search a text in the harvested log files.
- Download the harvested log files on your local server.

Name	Description
Enter search text	The text that you want search for in the harvested log files.
List box	Displays the hierarchy of the harvested log files in an archive. The files are organized in a tree view.
Log Browser Panel	Displays the contents of the selected log files.
Search Results Panel	Displays the search results. This field displays the line numbers as hyperlinks in which the searched text is found. When you click the line number, the system displays the line containing the searched text at the top in the **Log Browser Panel** field.

Button	Description
Previous	Displays the log file contents on the previous page. This button is available only if the contents of a log files span across multiple pages.
Next	Displays the log file contents on the next page. This button is available only if the contents of a log files span across multiple pages.
Search	Searches for the occurrences of the text specified in the **Enter search text** field in the selected log files.
View	Displays the contents of the selected log files in the **Log Browser Panel** field.
Download	Downloads the selected log files present in the archive to your local server.

Harvest - View Harvest detail field descriptions

Use this page to view the details of a selected log harvest request.

View Parent

Name	Description
Request Id	Displays the unique identification number assigned to a log harvesting request.
Archive Name	Displays the name of the archive file that stores the harvested log files containing the log messages.
Status	Displays the status of log harvesting requests. The options are: • SUCCESS: The status is SUCCESS if System Manager successfully harvests the log messages. • FAILURE: The status is FAILURE if System Manager fails to harvest the log messages for the product.
Request Description	A brief description of the log harvesting request.

Child Request Details

Name	Description
Product	Displays the unique identification number assigned to a log harvesting request.
Status	Displays the status of the log harvesting request. The options are: • **SUCCESS**: The status is SUCCESS if System Manager successfully harvests the log messages. • **FAILURE**: The status is FAILURE if System Manager fails to harvest the log messages for the product.
Host Name	Displays the hostname of the server on which the product resides.
Status Description	A brief description about the execution status of the request.
Status Time Stamp	Displays the date and time when the system generates the status of the log harvesting request.

Button	Description
Done	Closes this page and takes you back to the Harvest Archives page.
Refresh	Refreshes the records in the table.
Filter: Enable	Displays fields under the column headers of the table displaying the log harvesting requests. You can enter the filter criteria in these fields. Only columns that

Table continues…

Button	Description
	can be filtered display the fields in which you can enter the filter criteria. A toggle button.
Filter: Apply	Filters the log harvesting requests based on the filter criteria.
Filter: Disable	Hides the fields displayed under the columns on which you can apply the filters without resetting the filter criteria. A toggle button.

Chapter 12: Managing system data

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. You do not need to create data backups of individual elements that System Manager manages. The data and configuration files for the entire system are kept centrally on System Manager.

System Manager supports local backup and remote backup. Remote servers support only Linux-based operating systems. The Linux operating system must support the SSH protocol version 2. You can transfer backup files by using the sftp or scp protocol.

You can perform either a backup or a restore operation at a specified time. The restore operation fails if a backup operation is in progress. When a restore operation is in progress, the system skips all backup jobs that you scheduled.

You can restore the data on System Manager that has the same software version and IP address or FQDN as that of System Manager on which you created the backup.

The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

To perform the backup and restore operations, you must map the user to the role with the following permissions:

Resource type	Permissions
OnDemand	add
All elements of type:SMGR Core Services	backup and restore
All elements of type:alarmoperation	view and modify
All elements of type:elements	add, change, delete, and view

For instructions to create a custom role, see Adding a custom role.

Disk space management for System Manager backup

Ensure that sufficient disk space is available before you create a local backup. You can configure the disk space on the View Profile:SMGR Element Manager page from **Settings** > **SMGR** > **SMGR Element Manager** on System Manager Web Console.

The system generates an alarm when the disk space reaches the threshold value. You can configure the 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.

Related Links

Disk space required for backup on page 663

Disk space required for backup

Table 7: System Manager backup file size

Number of users	Database size	Approximate backup file size			
		System Manager		System Platform	
		Local	Remote	Local	Remote
1k	524MB	27M	27M	36M	36M
5k	2253MB	29M	29M	37M	37M
25k	2774MB	34M	34M	42M	42M
50k	4066MB	42M	42M	49M	49M
75k	5601MB	49M	49M	56M	56M
100k	6482MB	56M	56M	62M	62M
150k	7855MB	69M	69M	75M	75M
200k	8219MB	81M	81M	86M	86M
250k	8537MB	94M	94M	98M	98M

Time duration for backup and restore

Backup and Restore Time Duration				
Number of users	System Manager		System Platfor	
	Backup	Restore	Backup	
1k	57 sec	22 min 41 sec	1 min 30 sec	4
5k	1 min 15 sec	36 min 23 sec	1 min 42 sec	5
25k	1 min 46 sec	48 min 23 sec	1 min 47 sec	1 h
50k	2 min 03 sec	50 min 27 sec	2 min 21 sec	1 hr
75k	2 min 32 sec	56 min 11 sec	2 min 39 sec	1 hr
100k	2 min 54 sec	1 hr 4 min 03 sec	2 min 58 sec	1 hr
150k	4 min 02 sec	1 hr 6 min 52 sec	4 min 07 sec	1 hr
200k	4 min 55 sec	1 hr 14 min 40 sec	4 min 59 sec	1 hr
250k	5 min 54 sec	1 hr 20 min 40 sec	6 min 03 sec	1 hr

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.

System Manager data backup options

To back up System Manager data, use one of the following methods:

1. Back up the System Manager configuration files and the System Manager database on System Manager Web Console.
2. Back up System Platform and System Manager data on System Platform Web Console.

However, use System Platform to create the System Manager backup in the following scenarios:

- Restoring the System Manager and System Platform data
- Upgrading System Manager and System Platform
- Changing over to the cold standby System Manager server

Note:

System Manager does not support the backup and restore operations from System Platform Web Console if System Manager is running on VMware.

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 662

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 672

Creating a data backup on a local server

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local**.
4. In the **File name** field, enter the backup file that you want to create.
5. Click **Now**.

   If the backup is successful, the Backup and Restore page displays 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 664
Backup field descriptions on page 673

Creating a data backup on a remote server

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - 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. 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 664
Backup field descriptions on page 673

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 673
Schedule Backup field descriptions on page 675

Scheduling a data backup on a remote server

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.

4. Perform one of the following:
   - Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
   - Select the **Use Default** check box.

     Important:

     To use the **Use Default** option, provide the remote server IP, 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 673
Schedule Backup field descriptions on page 675

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 667
Scheduling a data backup on a local server on page 667
Deleting the scheduled backup job on page 669

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 693.
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 668

Restoring data backup from a local server

About this task

Note:

- Do not restore the backup data from VMware on System Platform.
- 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 complete path of the file that you must restore.

   Note:

   The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

5. Click **Restore**. On the Restore Confirmation page, the system displays the following message:

   ```
   The Restore operation will terminate all sessions and no services
   will be available until the operation completes. So, the System
   Manager console will not be available for approximately 45 minutes
   but this time may vary based on Database size. Click on Continue to
   go ahead with the Restore operation or click on Cancel to abort the
   operation.
   ```

6. Click **Continue**.

   The system logs you out of the System Manager web console and then shuts down.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Related Links

Backup and restore on System Manager that is configured for Geographic Redundancy on page 664
Restore field descriptions on page 676

Restoring a backup from a remote server

About this task

Note:

- Do not restore the backup data from VMware on System Platform.
- 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 **Remote**.
4. In the **Parameterized Restore** tab, perform one of the following:
   - Provide the name of the file that you must restore, the file transfer protocol, the remote server IP, remote server port, user name, and the password to access the remote computer in the respective fields.

     Note:

     The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.
   - 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. In the Backup List, view the list of the remote backups that are created by using the SFTP and SCP protocols.

   If the location of a backup file is modified, in the **Parameterized Restore** tab, specify the correct location of the backup file in the **File Name** field. You can select only one file at a time.
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 664
Restore field descriptions on page 676

Restoring the backup through the command line interface

Before you begin

Start an SSH session and provide the correct IP address and the port number.

About this task

You can restore the data through the command line when the machine is in an unstable state and the system does not display the Web console.

Procedure

1. Log in to System Manager using the command line interface as root.
2. At the prompt, type `$MGMT_HOME/pem/fileRestoreCLIUtility`.
3. In the `restorecli.properties` file, enter the build number of the machine in the **version** field.
4. In the properties file, ensure that `fq_backup_file_name` displays the complete path of the backup zip file.
5. In the `fileRestoreCLIUtility.properties` file, ensure that `backup_name` points to the backup zip file.
6. Type `sh $MGMT_HOME/pem/fileRestoreCLIUtility/file_restore.sh<full path of fileRestoreClIUtility><0/1>`

   Where, *0* denotes only the file restore and *1* denotes a full restore.

   Note:

   The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.
7. Complete the steps on the screen to perform the restore operation successfully.

Backup and Restore field descriptions

Use this page to view the details of backup files or the files you require to restore.

Name	Description
Operation	Specifies the type of operation. The values are: • Backup • Restore
File Name	• For the backup operation, specifies the name of the backup file. • For the restore operation, specifies the name of the file you want to restore.
Path	• For the backup operation, specifies the path of the backup file. • For the restore operation, specifies the path of the file you want to restore.
Status	Indicates the status of the backup or restore operation. The values are: • SUCCESS • FAILED • PLANNED • RUNNING
Status Description	Displays the error details of the backup or restore operation that has failed.
Operation Time	Specifies the time of the backup or restore operation.
Operation Type	Defines whether the backup or restore operation is local or remote.
User	Displays the user who performed the operation.

Button	Description
Backup	Opens the Backup page. Use this page to back up data on a specified local or remote location.
Restore	Opens the Restore page. Use this page to restore data to a specified local or remote location.

Backup field descriptions

Use this page to backup the System Manager data on a local or a remote location. You can also use this page to schedule a backup job.

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 on a local computer.

Name	Description
File Name	The file name that identifies the backup. System Manager creates a backup file in the home directory of the specified user.

The page displays the following fields when you choose to create a backup of System Manager data on a remote server.

Name	Description
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.
File Name	The path and name of the file that identifies the backup. If you provide only the file name, System Manager creates a backup file in the default directory of the user. 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 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
Now	Creates a backs up of the data in the specified location immediately.
Schedule	Displays the Schedule Backup page where you can enter the details to schedule a back up.
Cancel	Closes the Backup page and takes you back to the Backup and Restore page.

Schedule Backup field descriptions

Use this page to schedule a job for backing up data by specifying the date and time.

Job Details

Name	Description
Job Name	The name of the job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	The settings define whether the execution of the jobs is a recurring activity or a one-time activity. In case of a recurring job, the field also displays the time interval of recurrence. The options are: • Execute task one time only. • Tasks are repeated.
Range	The settings define the number of recurrences or date after which the job stops to recur. The options are: • No End Date • End After occurrences • End By Date

Button	Description
Commit	Schedules the backup job.
Cancel	Closes the Schedule Backup page and takes you back to the Backup Restore page.

Restore field descriptions

Use this page to restore the application data from a local or a remote location.

Field	Description
Type	The type of computer from where you restore the application data. The options are: • **Local**. The data is restored from a local machine. • **Remote**. The data is restored from a remote machine.

The page displays the following fields, when you select **Local** as **Type**.

Field	Description
Select File Name	The list of files from where you select the backup file that you must restore.
File Name	The name of the backup file that you must restore. If the system does not display the file that you must restore, specify the complete path of the backup file. **Note:** The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

Backup List

The page displays the following fields when you select **Remote** as **Type**.

The **Backup List** tab displays the list of remote backup files that are created using the SFTP or SCP protocol. Select a backup and click the **Parameterized Restore** tab to change the restore details. For example, if the location of a backup file is modified, specify the correct location of the file in the **File Name** field.

Parameterized Restore

The page displays the following fields when you select **Remote** as **Type**.

Field	Description
File Name	The name and complete path of the backup file that you want to restore.
File transfer protocol	The protocol that you can use to restore the backup. The values are SCP and SFTP.
Remote Server IP	The IP address of the SFTP or SCP server.
Remote Server Port	The SSH port of the SFTP or SCP server.

Table continues…

Field	Description
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 opens the Backup and Restore page.

Managing data retention rules

Accessing the Data Retention Rules service

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Data Retention**.

   The system displays the Data Retention page with the Rule list.

Result

The system displays the Data Retention page.

Data retention rules

You can configure data retention rules to specify the number of days you want the system to retain the following records:

- Logs
- Backup files

- Cleared alarms
- Aged alarms

Viewing data retention rules

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Data Retention**.

   The system displays the Data Retention page with the Rule list.

Related Links

Data Retention field descriptions on page 678

Modifying data retention rules

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Data Retention**.

   The system displays the Data Retention page with the Rule list.
3. Select a rule from the Rule list.
4. Click **Edit**.
5. Modify the value in the **Retention Interval (Days)** field.
6. Click **Update** to save the value.

Related Links

Data Retention field descriptions on page 678

Data Retention field descriptions

Use this page to view and edit data retention rules.

Name	Description
Option button	Provides the option to select a data retention rule.
Rule Name	Specifies the name of the rule.
Rule Description	A brief description about the data retention rule.
Retention Interval (Days)	Specifies the number of days the data is retained.

Button	Description
Edit	Modifies the selected rule.
Update	Updates the rule with changes made to the rule.
Cancel	Cancels the editing operation.
Apply	Applies the selected rule.

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 do the following:

- View replica nodes in a replica group.
- Perform a repair on the replica nodes that are not synchronized. This 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 683

Viewing replica nodes in a replica group

You can view the replica nodes in a group.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, select a replica group and click **View Replica Nodes**.

   Alternatively, you can click a replica group name displayed under the **Replica Group** column to view the replica nodes for that replica group.

   The Replica Nodes page displays the replica nodes for the select group.

Related Links

Replica Nodes field descriptions on page 684

Repairing a replica node

You can replicate data for a replica node whose database is not synchronized with the System Manager database. Repair is necessary if there is a post-install failure of Data Replication Service.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, perform one of the following:
   - Select a replica group for which you want repair the replica nodes from the table displaying replica groups and click **View Replica Nodes**.
   - Click the name of the replica node under the **Replica Group** column.
3. On the Replica Nodes page, select a replica node and click **Repair**.

   The **Synchronization Status** column displays the data replication status for the repairing replica node.

Related Links

Replica Nodes field descriptions on page 684

Repairing all replica nodes in a replica group

You can replicate data for all the replica nodes that are in a group. You can perform this operation if replica nodes in a group are not synchronized with the System Manager database.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, select a replica group for which you want repair the replica nodes from the table displaying replica groups.
3. Click **Repair**.

   The **Synchronization Status** column displays the data replication status for the replica group.

Viewing replication details for a replica node

You can view the batch-related information such as total number of batches received, processed, and skipped for a replica node. The master database sends the requested data in batches to the replica node.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, select a replica group and click **View Replica Nodes**.

   The Replica Nodes page displays the replica nodes for the selected replica group in a table.
3. Select a replica node and click **View Details**.

   The Data Replication page displays the replication details for the selected replica node.

Related Links

Replication Node Details field descriptions on page 686

Removing a replica node

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, select the replica group from which you must remove a node and click **View Replica Nodes**.
3. On the Replica Node page, click **Remove**.

Removing a replica node from the queue

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, select the replica group for which you must remove the node and click **View Replica Nodes**.
3. On the Replica Node page, click **Remove from Queue**.

Replica Groups field descriptions

The replica groups are logical groupings of the replica nodes. You can use the replica groups field descriptions page to:

- View all the replica groups in the enterprise.
- View the replication status of the replica groups.

The page displays the following fields when you select `All` from the **Replica Group** field.

Name	Description
Select check box	An option to select a replica group.
Replica Group	The name of the replica group. Each replica group in the list is a hyperlink. When you click a group, the system displays the replica nodes for that group on the Replica Nodes page.
Synchronization Status	For each replica group, displays the combined synchronization status of all replica nodes under the group
Group Description	A brief description of the replica group.

Button	Description
View Replica Nodes	Displays the Replica Nodes page. Use this page to view replica nodes for a group that you select.
Repair	Initiates full-sync for the selected groups and effectively for all the replica nodes that belong to the selected groups.
Filter: Enable	Displays fields under **Replica Group** and **Synchronization Status** columns where you can set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Apply	Filters replica nodes based on the filter criteria.

Replica Nodes field descriptions

You can use this page to:

- View the replica nodes in a selected replica group when you request data replication from the master database of System Manager.
- View the replication status of the replica nodes in a group.

Name	Description
Select check box	Provides the option to select a replica node.
Replica Node Host Name	Displays the full hostname of the replica node. If you need to administer Session Manager, the Replica Nodes Web page displays the fully qualified domain name. For example, ab-ct10-defg-bsm.mydata.com.
Product	Displays the name of the product.
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.

Table continues…

Name	Description
	A replica node can be in any one of the following states during the lifecycle: • **Ready for Repair**. The database of the replica node is not synchronized with the master database. • **Queued for Repair**. The replication request of the replica server is in queue with other data replication requests. The color code of the status is yellow. • **Repairing**. The data replication process is in progress. The color code of the status is yellow. • **Synchronized**. The system has successfully replicated the data that the replica node requested from the master database to the database of the replica node. The color code of the status is green. **Note:** If you encounter the following, contact the administrator who can manually intervene to resolve the problem: • `Not Reachable`. System Manager is unable to connect to the replica node. This indicates that the replica node is switched off for maintenance, a network connectivity failure, or any other issue that affects general connectivity between System Manager and the replica node. • `Synchronization Failure`. Data replication is broken between System Manager and the replica node. This status generally indicates a catastrophic failure. 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

Table continues…

Name	Description
	for the node. On completion of audit activity, the node displays any of the other states as applicable. The color code of the status is yellow.
Last Synchronization Time	Displays the last time when the system performed the data synchronization or replication for the replica node.
GR Enabled	Displays whether the replica node is GR-enabled or not.
Last Pull Time	Displays the last time when the client polled DRS for changed data.

Button	Description
View Details	Opens the Data Replication page. Use this page to view the synchronization details for a replica node.
Repair	Replicates or resynchronizes data from the master node to a selected replica node.
Remove	Removes the nodes you select from the replica group.
Remove From Queue	Removes the replica node you select from the queue.
Show All Replica Groups	Takes you back to the Replica Groups page.

Replication Node Details field descriptions

You can use this page to view the following details:

- The batch-related information such as total number of batches received, processed, and skipped for a replica node.
- The last time when the replication server performed the synchronization or replication.
- Synchronization or replication error details.

General

Name	Description
Replica Node Group	Displays the name of the group that the replica node belongs to. A node-group is a logical grouping of similar nodes.
Replica Node Host Name	Displays the full hostname of the replica node. If you need to administer Session Manager, the Replica Nodes Web page displays the fully qualified

Table continues…

Name	Description
	domain name. For example, ab-ct10-defg-bsm.mydata.com.
Last Down Time	Displays the last time and date when the replica node could not be reached. System Manager periodically checks whether a replica node is reachable.
Last Repair Start Time	Displays the last time and date when a full-sync was started for the node.
Last Repair End Time	Displays the last time and date when a full-sync was completed for the node.
Last Pull Time	Displays the last time when the client polled DRS for changed data.
Build Version	Displays the version of the element configuration.
GR Enabled	Displays whether the replica node is GR-enabled or not.

Synchronization Statistics

Name	Description
Pending Batches	Lists the batches that are yet to be replicated to the replica node. During the data replication process, System Manager records the changes for a particular replica node in the form of events. When a replica node 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.

Table continues…

Name	Description
Last Batch Acknowledged	Displays the last batch that an element acknowledged as successfully processed on the element side. During an audit, Data Replication Service (DRS) compares the last successfully committed batch on the node with the data in the last batch acknowledged batch. If the node has a more recent batch, then DRS schedules a full-sync for the node.
Marked For Audit	Marks for audit all replica nodes that are GR-enabled: • 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.

Managing scheduled jobs

Scheduler

The Scheduler service provides a generic job scheduling service for System Manager and Avaya Aura® applications. The Scheduler service provides an interface to run a job on demand or on a periodic basis. You can schedule a job to generate an output immediately or set the frequency of the

task execution to run on a periodic basis. You can modify the frequency for a periodic job schedule any time. After you define a task or a job, System Manager creates instances of the task, monitors the execution of the task, and updates the status of the task.

Scheduled jobs can be of three types:

- System scheduled: The job that the system executes on a periodic basis for the system to operate normally. The system adds these jobs at start-up and supports all frequencies other than one time. Scheduled jobs run asynchronously in the background. As an administrator, you cannot add or delete system-scheduled jobs. You can only disable or enable the jobs to stop temporarily.
- Admin scheduled: The job that the administrator schedules for administering the application. The administrator can use various navigation paths to schedule jobs such as bulk import and directory synchronization. The system lists the jobs in the scheduler as admin scheduled jobs.
- On-demand: The administrator can schedule on-demand jobs from the list of existing jobs.

You can perform the following operations using the Scheduler page on System Manager Web Console:

- View the pending and completed scheduled jobs.
- Modify a job scheduled by an administrator or an on-demand job.
- Delete a scheduled job.
- Schedule an on-demand job.
- Stop a running job.
- Enable or disable a job.
- Search a scheduled job.

Accessing scheduler

Procedure

On the System Manager web console, click **Services** > **Scheduler**.

Viewing pending jobs

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. In the left navigation pane, click **Pending Jobs**.
3. To view the details of the job, on the Pending Jobs page, select a pending job and click **View**.

   The Job Scheduling-View Job page displays the details of the selected job.

Related Links

Pending Jobs field descriptions on page 694

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 696

Viewing logs for a job

About this task

Use this functionality to view logs for a pending and completed job.

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Perform the following:
   - To view logs for a pending job, perform the following steps:
     a. Click **Pending Jobs** in the left navigation pane.
     b. On the Pending Jobs page, select a pending job and click **More Actions** > **View Log**.
   - To view logs for a competed job, perform the following steps:
     a. Click **Completed Jobs** in the left navigation pane.
     b. On the Completed Jobs page, select a completed job and click **More Actions** > **View Log**.

   The log viewer displays the details for the selected job.

Filtering jobs

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Perform one of the following:
   - To filter pending jobs:
     a. In the left navigation pane, click **Scheduler** > **Pending Jobs**.
     b. On the Pending Jobs page, click **Filter: Enable**.
   - To filter completed jobs:
     a. In the left navigation pane, click **Scheduler** > **Completed Jobs**.
     b. On the Completed Jobs page, click **Filter: Enable**.

   The system displays the **Filter: Enable** option at the upper-right corner of the page.
3. Complete the fields to filter a job using the following criteria:
   - **Job Type**. The type of the job.
   - **Job Name**. Name of the job.
   - **Job Status**. Status of the job.
   - **State**. State of the job.
   - **Frequency**. Frequency at which the job must be executed.
   - **Scheduled By**. The user who scheduled the job
4. Click **Apply**.

   The system displays jobs that match the filter criteria.

Editing a job

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Perform one of the following steps:
   - To edit a pending job, perform the following steps:
     a. Click **Pending Jobs** in the left navigation pane.
     b. On the Pending Jobs page, select a pending job and click **Edit** or click **View** > **Edit**.
   - To edit a competed job, perform the following steps:
     a. Click **Completed Jobs** in the left navigation pane.

b. On the Completed Jobs page, select a completed job and click **Edit** or click **View** > **Edit**.

3. On the Job Scheduling-Edit Job page, modify the appropriate information and click **Commit** to save the changes.

   You can modify information in the following fields: **Job Name**, **Job State** in the Job Details sections, and **Task Time**, **Recurrence**, **Range** in the Job Frequency section.

Deleting a job

Before you begin

You have logged in as an administrator to delete an administrator scheduled job.

About this task

Use this functionality to delete an obsolete job. You can delete an on-demand and an administrator scheduled job.

Note:

You can remove only **Schedule On Demand** type of jobs.

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Perform one of the following steps:
   - To remove a pending job, perform the following steps:
     a. Click **Pending Jobs** in the left navigation pane.
     b. On the Pending Jobs page, select a pending job.

        If the job that you want to delete is currently running then you must stop the job. To stop the job, click **More Actions** > **Stop**.

        Note:

        If the job that you want to delete is in the enabled state, disable the job. See Disabling a job on page 693 on how to disable a job.

     c. Click **Delete**.
   - To remove a competed job, perform the following steps:
     a. Click **Completed Jobs** in the left navigation pane.
     b. On the Completed Jobs page, select a completed job.

        Note:

        If the job that you want to delete is in the enabled state, disable the job.

     c. Click **Delete**.
3. On the Delete Confirmation page, click **OK**.

System Manager deletes the job you select from the database.

Disabling a job

About this task

Use this functionality to make a job inactive.

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Perform one of the following steps:
   - To disable a pending job, perform the following steps:
     a. Click **Pending Jobs** in the left navigation pane.
     b. On the Pending Jobs page, select a pending job and click **More Actions** > **Disable**.
   - To disable a competed job, perform the following steps:
     a. Click **Completed Jobs** in the left navigation pane.
     b. On the Completed Jobs page, select a completed job and click **More Actions** > **Disable**.
3. On the Disable Confirmation page, click **Continue**.

   The **State** of the job you selected changes to **Disabled**.

Enabling a job

About this task

Use this functionality to make a job active.

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. Perform one of the following steps:
   - To enable a pending job, perform the following steps:
     a. Click **Pending Jobs** in the left navigation pane.
     b. On the Pending Jobs page, select a pending job and click **More Actions** > **Enable**.
   - To enable a competed job, perform the following steps:
     a. Click **Completed Jobs** in the left navigation pane.
     b. On the Completed Jobs page, select a completed job and click **More Actions** > **Enable**.

Note:

When you enable a job, the system does not restart the job that completed all executions. To restart a job that completed all executions, reconfigure the job parameters from Job Scheduling-Edit Job page.

The system displays `Enabled` in the **State** column of the selected job.

Stopping a job

Procedure

1. On the System Manager web console, click **Services** > **Scheduler**.
2. In the left navigation pane, click **Pending Jobs**.
3. On the Pending Jobs page, select a pending job in the running state and click **More Actions** > **Stop**.
4. Click **Continue** on the Stop Confirmation page.

   Scheduler stops the selected job.

Pending Jobs field descriptions

Name	Description
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. System scheduled job. 2. Admin scheduled job. 3. On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The types of status are: 1. Pending Execution 2. Running
State	The state of a job whether the job is active or inactive. The types of state are: • Enabled: An active job. • Disabled: An inactive job.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The person who scheduled the job.

Button	Description
View	Displays the Job Scheduling-View Job page that displays the details of the selected pending job.
Edit	Displays the Job Scheduling-Edit Job page that you can use to modify the information of a selected pending job.
Delete	Displays the Delete Confirmation page that prompts you to confirm the deletion of the selected jobs.
More Actions > **View Log**	Displays the Logging page that displays the logs for the selected pending jobs.
More Actions > **Stop**	Stops the selected job that is currently running.
More Actions > **Enable**	Changes the state of the selected pending job from inactive to active.
More Actions > **Disable**	Displays the Disable Confirmation page that prompts you to confirm the disabling of the selected pending job.
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.

Name	Description
	• 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 689
Scheduler on page 688

Completed Jobs field descriptions

Name	Description
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. System scheduled job. 2. Admin scheduled job. 3. On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The types of status are: 1. Status Unknown 2. Interrupted 3. Failed 4. Successful 5. Not Authorized
Last Run	The date and time when the job was last run.

Table continues…

Name	Description
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 690
Scheduler on page 688

Job Scheduling-View Job field descriptions

Use this page to view the details and frequency of a job.

Job Details

Name	Description
Job Name	The name of the job.
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. System scheduled job. 2. Admin scheduled job. 3. On-demand job.
Job Status	The current status of the job. The types of status are: 1. Running 2. Pending

Table continues…

Name	Description
	3. Status Unknown 4. Interrupted 5. Failed 6. Successful 7. Not Authorized
Job State	The state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	The settings that define whether the execution of the jobs is a recurring activity or a one time activity. In case of a recurring job, the field also displays the frequency of recurrence.
Range	The number of recurrences or a date after which the job stops to recur.

Button	Description
View Log	Opens the Logging page that you can use to view the logs for the selected job.
Edit	Opens the Job Scheduling-Edit Job page that you can use to edit the pending job information.
Cancel	Closes the Job Scheduling-View Job page and returns to the Pending Jobs or Completed Jobs page.

Related Links

Scheduler on page 688

Job Scheduling-Edit Job field descriptions

Job Details

Name	Description
Job Name	The name of the job.

Table continues…

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. **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.
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 688

Job Scheduling-On Demand Job field descriptions

Use this page to schedule an on-demand job.

Job Details

Name	Description
Job Name	The name of the job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	The settings that define whether the execution of the jobs is a recurring activity or a one time activity. In case of a recurring job, the field also display the time interval of recurrence. The options are: • Execute task one time only. • Task are repeated: - Minutes - Hourly - Daily - Weekly - Yearly
Range	The settings that define the number of recurrences or date after which the job stops recurring. The options are: • No End Date • End After occurrences • End By Date

Button	Description
Commit	Schedules an On-Demand job.
Cancel	Cancels the scheduling of an On Demand job operation and takes you back to the Pending Jobs or Completed Jobs page.

Disable Confirmation field descriptions

Use this page to disable selected jobs.

Name	Description
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. System scheduled job. 2. Admin scheduled job. 3. On-demand job.
Job Name	Specifies the name of the scheduled job.
Job Status	Specifies 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	Specifies the state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job.
Last Run	Specifies the date and time when the job was last run successfully. **Note:** The last run is applicable only for completed jobs.
Frequency	Specifies the time interval between two consecutive executions of the job.
Scheduled By	Specifies the scheduler of the job.

Button	Description
Continue	Disables the job and cancels the next executions that are scheduled for the job.
Cancel	Cancels the operation of disabling a job and takes you back to the Pending or completed Jobs page.

Related Links

Scheduler on page 688

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	Specifies the name of the scheduled job.
Job Status	Specifies the current status of the pending job. The jobs on this page have status Running.
State	Specifies the state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job. All the jobs on this page are in the **Enabled** state.
Last Run	Specifies the date and time when the job was last run successfully. **Note:** The last run is applicable only for completed jobs.
Frequency	Specifies the time interval between two consecutive executions of the job.
Scheduled By	Specifies the scheduler of the job.

Button	Description
Continue	Stops the job.
Cancel	Cancels the operation of stopping a job and takes you back to the Pending Jobs page.

Related Links

Scheduler on page 688

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	Specifies the name of the scheduled job.
Job Status	Specifies the current status of the job.
State	Specifies 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	Specifies the date and time when the job was last run. **Note:** The last run is applicable only for completed jobs.
Frequency	Specifies the time interval between two consecutive executions of the job.
Scheduled By	Specifies the scheduler of the job.

Button	Description
Continue	Deletes the selected job.
Cancel	Cancels the operation of deleting a job and takes you back to the Pending or completed Jobs page.

Related Links

Scheduler on page 688

Chapter 13: SIP phone pre-configuration template

Starting with Session Manager 6.3.8, Avaya provides support for pre-configuring endpoint-specific settings such as button assignments, Language and Region settings, and whether button clicks are enabled. Customers can use administration screens on System Manager to centrally administer SIP phone settings that were previously only accessible from the SIP phone device itself.

All **Home** > **Users** > **User Management** > **Manage Users** > **user xyz** > **CM Endpoint Profile** > **Endpoint Editor** settings data are stored in the System Manager database. The system replicates these settings changes to the Session Manager and Branch Session Manager databases. The Personal Profile Manager (PPM) makes these settings available to the user's endpoints for reading and updating.

When the user first logs in, the endpoint downloads the endpoint settings from the PPM and applies the values.

Note:

When the user logs in to the user's Endpoint for the first time, the administered template may not match the specific endpoint type of that Endpoint. For example, the administrator assigns a 9641 template to the user and the user logs in with a 9611 Endpoint. If the 9611 Endpoint does not support a specific 9641 setting, such as full screen mode, the 9611 Endpoint removes that setting since the setting does not apply to the 9611. The net effect is that the 9641 parameter is never administered. If that same user later logs in with a 9641 Endpoint, the removed 9641 setting is no longer present and the 9641 Endpoint does not reflect that setting.

Users can override template settings by changing the settings on the endpoint. The changes take effect immediately, assuming the changes are valid.

The system supports the SIP phone pre-configuration template for the following set types:

- 96x1SIP
- 96x1SIPCC

The software requirements for the SIP phone pre-configuration template are:

- Communication Manager 6.2 or 6.3.x
- System Manager 6.3.8
- Session Manager 6.3.8

The following use cases are not supported:

- Applying a template to a group of existing users. Due to existing limitations, you can only apply a template to individual users, one at a time.
- Updating a template and propagating endpoint setting changes to all users and devices assigned to that template.

Creating a new customized SIP phone template

Create a new customized SIP phone template. The administrator can change any of the parameter values in the new custom template.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Templates** > **CM Endpoint**.
2. In the **Supported Feature Server Versions** table, select the appropriate software version for the **CM** System Type.
3. Click **Show List**.
4. Click the **Custom templates** tab.
5. Click **New** to create a new template.
6. On the **New Endpoint Template** screen, select the appropriate **Set Type** from the drop-down menu. The screen refreshes after you make a selection.
7. Enter a **Template Name**.
8. Under the **General Options** tab, enter the required information.
9. Click on the tabs and specify the endpoint settings for the new template.
10. Click **Commit**.

Creating a SIP phone template from a default template

Administrators can create a new customized template using a copy of a default template. The administrator can change any of the parameter values in the new template.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Templates** > **CM Endpoint**.
2. In the **Supported Feature Server Versions** table, select the appropriate software version for the **CM**.

3. Click **Show List**.
4. Click the **Default templates** tab.
5. Select the appropriate template from the **Default Templates List**.
6. Click **Duplicate**.
7. On the **Duplicate Endpoint Template** screen, select the **Set Type** from the drop-down menu. The screen refreshes after you make a selection.
8. Enter the **New Template Name**.
9. On the **General Options** screen, enter the required information.
10. Click on the tabs and specify the endpoint settings as needed.
11. Click **Commit**.

Applying a SIP phone template to an existing user

Important:

When you apply a template to an existing user, the values in the template override all existing settings that are configurable using the System Manager Endpoint Editor. If a value is currently set on the endpoint and not set in the template, applying the template causes the setting on the endpoint to become unassigned.

If you need to apply new phone settings to an endpoint, use the existing endpoint editing capability to modify endpoint settings for an existing user. You can select and modify the settings directly. Editing an endpoint only overwrites the selected settings. To edit the settings for an existing user, navigate to **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints** on the System Manager Web Console.

Note:

You can also make changes by navigating to **Home** > **Users** > **User Management** > **Manage Users** and selecting and editing the user information.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Communication Manager** > **Endpoints** > **Manage Endpoints**.
2. Select the endpoint to which you want to apply the template.
3. Click **Edit**.
4. In the **Template** field, select the template you want to apply from the drop-down menu.
5. To further customize the endpoint settings, make changes to any of the parameters on any of the tabs.
6. Click **Commit**.

Modifying endpoint settings for an existing user

This procedure describes how to modify the endpoint settings for an existing user.

Important:

When the administrator commits the changes, the system sends the changes to the endpoint. Certain changes can be disruptive. Use caution when making changes and be aware of the impact of a change on a user.

Using the **Job Scheduler** screen, you can schedule endpoint setting changes to occur at a later time that might be less disruptive to the user, for example, midnight local time.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**.
2. Click **Show List**.
3. Select the **Name** of the endpoint you want to modify.
4. Click **Edit**.
5. Make the necessary changes.
6. When you finish modifying the settings do one of the following:
   - Click **Commit** to commit the changes, or
   - Click **Schedule**, specify the date and time to change the endpoint settings, and click **Schedule**.

Modifying endpoint settings for a group of existing users

This procedure describes how to modify the endpoint settings for a group of existing users using the Global Endpoint Change capability, also known as Global Search & Replace.

Important:

When the administrator submits the changes, the system sends the changes to the endpoint. Certain changes can be disruptive. Use caution when making changes and be aware of the impact of a change on a user.

Using the **Job Scheduler** screen, you can schedule endpoint setting changes to occur at a later time that might be less disruptive to the user, for example, midnight local time.

Before you begin

Perform a bulk import of a group of users to apply an initial set of endpoint settings. For example, LDAP import.

When using bulk import to define a group of users, import the users in such a way to easily identify those users with the Global Search & Replace criteria, for example, a sequential set of extensions.

If the Global Search & Replace criteria match multiple endpoint types, for example 9641 and 9611, you can change parameters that are applicable to one endpoint type but not the other.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**.
2. In the upper right corner of the **Endpoint List** table, click **Advanced Search**.
3. Enter the search criteria to obtain the list of endpoints you want to change.
4. Select the endpoints from the resulting list.
5. Click **More Actions** > **Global Endpoint Change**.
6. Change the settings under the appropriate tabs.
7. When you finish modifying the settings, do one of the following:
   - Click **Commit** to commit the changes, or
   - Click **Schedule**, specify the date and time to change the endpoint settings, and click **Schedule**.

Removing a SIP phone template

Delete a previously defined SIP phone template. Deleting a template makes it unavailable for future use. Removing a template does not directly affect endpoint settings.

Note:

You can only remove custom templates. You cannot remove default templates.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Templates** > **CM Endpoint**.
2. Select the template you want to delete.
3. Click **Delete**.

Chapter 14: SIP Team Button

SIP Team button

A Team button is a button that has two generic functions: a display function and an execution function.

With the display function, a member of the team (monitoring station) can observe the station state of another team member (monitored station). The station state of the monitored station is a combination of active calls and ringing calls on the station.

With the execution function, a member of the team can use a Team button as a Speed Dial button or Pick-Up button. Depending on the state of the monitored station, a user can:

- establish a call directly to the monitored station.
- pick up a ringing call from the monitored station.
- **Direct Transfer**: Transfer an active call by pressing the Team button. The call automatically is put on hold and the transfer-destination (monitored station) is called. The user does not need to press the transfer button.
- **Transfer Upon Hangup**: Complete a transfer operation by hanging up the phone without the need to press the **Transfer Complete** button.
- **Override the Monitored Station's Forwarding**: The Monitoring Station can override the redirection of the monitored station. If the monitored station does not answer within a certain amount of time, the system redirects the call according to the redirection policy of the monitoring station.

Feature operation and control are the same for H.323 and SIP.

The SIP Team button is supported on 1XC 6.2 and 96X1 SIP 6.2.4.

Administering the SIP Team button

Administer the SIP Team button. To administer the SIP Team button, you need to:

1. Configure a team button for the Monitoring Station. The **SAC/CF Override** value pertains to all Monitored stations. The values are:
   - **n**: Do not override the call redirection of the Monitored station.
   - **y**: Override the call redirection of the Monitored station and terminate the call to the Monitored station.

- **ask**: Ask the user of the Monitoring station if the call redirection of the Monitored station should be overridden or not.

2. Administer the **Transfer Upon Hang-up** value, configured per Communication Manager.
3. Administer the COR values, configured per Communication Manager and per station.

The system takes about 3 minutes for the changes to download to the SIP phones after you make the changes.

Procedure

1. Configure the Monitoring Station:
   a. On the home page of the System Manager Web Console, under **Users**, select **User Management** > **Manage Users**.
   b. Select the user to configure. This user is the **Monitoring Station**.
   c. Click **Edit**.
   d. On the **Communication Profile** page, select **CM Endpoint Profile**.
   e. Click **Endpoint Editor**, next to the **Extension** field.
   f. On the **Edit Endpoint** page, select the **Button Assignment** tab.
   g. Select a button to be the Team button, and select **Team** from the drop-down menu.
   h. Enter the extension of the Monitored station/team member.
   i. Enter **y** or **n** to enable/disable ringing for the monitoring station.
   j. Select the **Enhanced Call Fwd** tab.
   k. In the **SAC/CF Override** field, select the appropriate value from the drop-down menu.
   l. Select the **General Options** tab and note the **Class of Restriction** for the Monitoring station.
   m. Click **Done**.
   n. Click **Commit**.
2. Determine the COR for the Monitored Station:
   a. Select the user to configure. This is the **Monitored Station**.
   b. Click **View**.
   c. On the **Communication Profile** page, select **CM Endpoint Profile**.
   d. Click **Endpoint Editor**, next to the **Extension** field.
   e. Select the **General Options** tab and note the **Class of Restriction** for the Monitored station.
   f. Click **Cancel**, then click **Cancel** again.
3. Configure the **Transfer Upon Hang-up** value:
   a. On the home page of the System Manager Web Console, under **Elements**, select **Communication Manager** > **Parameters** > **System Parameters** > **Features**.

b. Select the Communication Manager you want to change.
c. Click **Edit**.
d. Click **Next Page** until you get to Page 7.
e. Under **Conference/Transfer**, set the **Transfer Upon Hang-Up?** value to **y** or **n**.
f. Click **Enter** to save the change.

4. Configure the COR of the Monitoring station for the correct Communication Manager:
   a. On the home page of the System Manager Web Console, under **Elements**, select **Communication Manager** > **System** > **Class Of Restriction**.
   b. Select the COR of the Monitoring station for the correct Communication Manager.
   c. Click **Edit**.
   d. Go to Page 3.
   e. Set the value for **SAC/CF Override by Team Btn** to **y**.
   f. Click **Enter** to save the change.
5. Configure the COR of the Monitored station for the correct Communication Manager:
   a. Select the COR of the Monitored station for the correct Communication Manager.
   b. Click **Edit**.
   c. Go to Page 3.
   d. Set the value for **SAC/CF Override Protection for Team Btn** to **n**.
   e. Click **Enter** to save the change.

Appendix A: Restricted commands for the ASSET interface

Caution:

Only use System Manager to manipulate the ASSET interface. *Do not use any of the Linux administration tools that involve the ASSET interface, other than status commands, on the Session Manager platform.* The following commands can cause the Session Manager to enter an irrecoverable state.

Do not use the following Linux commands. These commands do not work correctly or persistently:

- service network stop/start/restart
- ifup
- ifdown
- route
- ip
- ethtool
- iptables

Appendix B: Regular Expression constructs

Construct	*Matches*
Characters	
x	The character x
\\	The backslash character
Character classes	
[abc]	a, b, or c (simple class)
[^abc]	Any character except a, b, or c (negation)
[a-zA-Z]	a through z or A through Z, inclusive (rang
[a-d[m-p]]	a through d, or m through p: [a-dm-p] (uni
[a-z&&[def]]	d, e, or f (intersection)
[a-z&&[^bc]]	a through z, except for b and c: [ad-z] (su
[a-z&&[^m-p]]	a through z, and not m through p: [a-lq-z](
Predefined character classes	
.	Any character (may or may not match line
\d	A digit: [0-9]
\D	A non-digit: [^0-9]
\s	A whitespace character: [\t\n\x0B\f\r]
\S	A non-whitespace character: [^\s]
\w	A word character: [a-zA-Z_0-9]
\W	A non-word character: [^\w]
java.lang.Character classes (simple java character type)	
\p{javaLowerCase}	Equivalent to java.lang.Character.isLower
\p{javaUpperCase}	Equivalent to java.lang.Character.isUpper
\p{javaWhitespace}	Equivalent to java.lang.Character.isWhite
\p{javaMirrored}	Equivalent to java.lang.Character.isMirror
Classes for Unicode blocks and categories	

\p{InGreek}	A character in the Greek block (simple blo
\p{Lu}	An uppercase letter (simple category)
\p{Sc}	A currency symbol
\P{InGreek}	Any character except one in the Greek blo
[\p{L}&&[^\p{Lu}]]	Any letter except an uppercase letter (sub
Boundary matchers	
^	The beginning of a line
$	The end of a line
Greedy quantifiers	
X?	X, once or not at all
X*	X, zero or more times
X+	X, one or more times
X{n}	X, exactly n times
X{n,}	X, at least n times
X{n,m}	X, at least n but not more than m times
Logical operators	
XY	X followed by Y
X|Y	Either X or Y

Note:

Refer to the full documentation at http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html for details.

Appendix C: SNMP support for Session Manager

This chapter provides details on creating of SNMP User and Target profiles, and attaching the Target profiles to Serviceability Agents.

Session Manager SNMP master agent is installed as part of factory install. This agent provides basic IP discovery, inventory, and status capabilities through the MIB II and Host Resources MIBs for the server and Linux operating system. The Session Manager agent requires configuration by System Manager for assignment of SNMP V3 user to support queries. This agent:

- Provides read-only access to the SNMP agent on the Session Manager server
- Does not allow any SNMP Set capability to the Session Manager
- Does not restrict the IP addresses that are allowed to query the MIBs
- Allows access control only via SNMP V3

The System Manager server also provides a basic SNMP V3 agent.

The Serviceability Agent is an enhanced version of the SAL agent for forwarding logs, harvesting logs, and for alarming. The Serviceability Agent sends SNMP V2, SNMP V3 traps and informs the configured NMS destinations where two of the mandatory destinations are System Manager and the SAL gateway.

Using the Serviceability Agent user interface on System Manager, you can:

- Remotely manage and configure SNMP V3 users.
- Remotely manage and configure SNMP trap destinations.
- Create, edit, view, and delete user and target profiles. You can also attach these profiles to agents or detach these profiles from agents.

Manage Serviceability Agents has three sub-pages:

- **SNMP User Profiles** is used to establish and modify SNMP V3 user accounts. These accounts are used for both SNMP V3 traps/informs and also SNMP V3 queries of the SNMP master agent.
- **SNMP Target Profiles** is used to establish SNMP trap/inform destinations for System Manager, SAL GW, and customer NMS along with attaching user profiles setup under SNMP User Profiles. The profile setup supports both SNMP V2 and SNMP V3 with either trap or inform type for notifications.

- **SNMP Serviceability Agents** is used to manage serviceability agents registered with System Manager agent manager. The System Manager hostname is automatically included in the list of agents.

Configuring Session Manager Serviceability Agent

About this task

Perform the following procedure to configure the Session Manager serviceability agent to send alarm traps:

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, select **Manage Serviceability Agents** to open the Manage Serviceability Agents page.
3. In SNMPv3 User Profiles, set up a user profile to match the System Manager TrapListener settings. The default System Manager trap listener settings for a fresh System Manager template install or upgrade, if no modifications are done using TrapListener service page, are user name as **initial** and MD5/AES password as **avaya123**. See the section System Manager TrapListener service on page 728 for details. The SNMP user profile for this System Manager is needed for the SNMP target profile for the System Manager TrapReceiver. Optional other user profiles can be created for other NMS or SAL GW destinations and Session Manager serviceability agents. See the section *Managing SNMPv3 user profiles* for details.
4. In SNMP Target Profiles, set up a target profile for the System Manager TrapReceiver. This profile includes the System Manager IP address, port **10162**, Domain type **UDP**, Notification type **trap** or **inform**, and Protocol **V3**. Also assign the System Manager user profile created under **SNMP User Profiles** before committing the profile. The System Manager serviceability agent is already configured with a default target profile and user for the local TrapReceiver. Other target profiles may be set up for SAL GW and NMS to also receive alarm traps/informs. See the section *Managing SNMP target profiles* for details.
5. After Session Manager install or upgrade is complete and the **`statapp`** command shows sal-agent is UP, verify that the Session Manager serviceability agent hostname and IP address has registered with System Manager in Serviceability Agents page.
6. If status is not active, select the Session Manager serviceability agent and enable the **Activate** button and verify status changes to active.
7. After the Session Manager serviceability agent becomes active, re-select the agent to make the **Manage Profiles** button active. Click **Manage Profiles** to assign the System Manager target profile and other desired optional target profiles. Attach a user profile for the serviceability agent to support V3 queries from a customer or NMS, then click **Commit**.

8. Verify that the Session Manager serviceability agent is properly configured for forwarding alarms to the System Manager. Enter **`generateTestAlarmSM.sh`** on the Session Manager CLI.

   Note:

   After a System Manager serviceability agent has been configured with SNMP target profiles and a user profile on the System Manager, subsequent System Manager and Session Manager upgrades preserve the setting and only require necessary modifications because of changes to user passwords, trap or inform type, NMS IP addresses, and others.

Managing SNMPv3 user profiles

Creating an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Click **New**.
4. On the New User Profile page, complete the User Details section.
5. Click **Commit**.

Related Links

SNMP User profile list on page 720
SNMPv3 user profiles field descriptions on page 721

Editing an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Select the user profile you want to edit from the profile list.
4. Click **Edit**.
5. Edit the required fields in the Edit User Profile page.

Note:

You cannot edit an SNMPv3 user profile that is assigned to the serviceability agent of an element or that is attached to a target profile.

6. Click **Commit**.

Related Links

SNMP User profile list on page 720
SNMPv3 user profiles field descriptions on page 721

Viewing an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Click the user profile you want to view from the profile list.
4. Click **View**.

   You can view the details, except the password, of the SNMPv3 user profile in the View User Profile page.

Related Links

SNMP User profile list on page 720
SNMPv3 user profiles field descriptions on page 721

Deleting an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Select the user profile or profiles you want to delete from the profile list.
4. Click **Delete**.
5. On the User Profile Delete Confirmation page, click **Delete**.

Note:

You cannot delete a user profile that is attached to an element or a target profile.

Filtering SNMPv3 user profiles

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
3. Click **Filter: Enable** above the Profile List.
4. Apply the filter to one or multiple columns of the User Profile List.
5. Click **Apply**.

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

SNMP User profile list

Name	Description
User Name	The SNMPv3 user name.
Authentication Protocol	The authentication protocol used to authenticate the source of traffic from SNMP V3 users.
Privacy Protocol	The encryption policy for an SNMP V3 user.
Privileges	The read-write privilege that determines the operations you can perform on MIBs.

Button	Description
New	To go to the New User Details page where you can add a new SNMP user profile.
View	To go to the View User Details page where you can view an existing SNMP user profile.
Edit	To go to the Edit User Details page where you can edit an existing SNMP user profile.
Delete	To delete the existing SNMP user profiles that you select.
Filter: Enable	To filter the SNMP user profiles list based on one or multiple criteria.

Related Links

Creating an SNMPv3 user profile on page 718
Editing an SNMPv3 user profile on page 718
Viewing an SNMPv3 user profile on page 719

SNMPv3 user profiles field descriptions

Name	Description
User Name	The SNMPv3 user name. **Note:** The user name can contain the following characters: alphanumeric, period, underscore, white space, single quote, and hyphen. The user name cannot be blank.
Authentication Protocol	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The possible values are: • MD5 • SHA The default is MD5.
Authentication Password	The password used to authenticate the user. **Note:** The password can contain any printable and non-whitespace characters. The password must be at least 8 characters in length and can contain up to 255 characters. The password cannot be an empty string.
Confirm Authentication Password	The authentication password that you re-enter for confirmation.
Privacy Protocol	The encryption policy for an SNMP V3 user. The possible values are: • DES: Use DES encryption for SNMP-based communication. • AES: Use AES encryption for SNMP-based communication. • None The default value is AES.
Privacy Password	The pass phrase used to encrypt the SNMP data.
Confirm Privacy Password	Retype the privacy password in this field for confirmation.

Table continues…

Name	Description
Privileges	The privileges that determines the operations that you can perform on MIBs. • Read/Write: Use to perform GET and SET operations. • Read: Use to perform only GET operation. • None The default is None.

Button	Description
Commit	Use to create a new SNMPv3 user profile. Saves the changes after an edit operation.
Back	Cancels the action and takes you to the previous page.
Delete	Use to delete the user profiles you select.
Edit	Use to edit the user profile you select.

Related Links

Creating an SNMPv3 user profile on page 718
Editing an SNMPv3 user profile on page 718
Viewing an SNMPv3 user profile on page 719

Managing SNMP target profiles

Creating an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. On the SNMP Target Profiles page, click **New**.
4. On the New Target Profiles page, complete the Target Details section.
5. **(Optional)** Click the **Attach/Detach User Profile** tab to attach a user profile.

   Perform the step only if you select the SNMPv3 protocol.
6. Click **Commit**.

Related Links

SNMP Target profile list on page 724
SNMP target profiles field descriptions on page 725

Editing an SNMP target profile

About this task

Note:

Modify the target profiles that point to System Manager to reflect the changed IP address in the event of an IP address change on System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. In the Target Profile list, click the profile that you must edit.
4. Click **Edit**.
5. On the Edit Target Profiles page, modify the required fields.

   Note:

   You cannot edit a target profile that is assigned to the serviceability agent of an element. You must unassign the target profile before you edit the profile.
6. Click **Commit**.

Related Links

SNMP Target profile list on page 724
SNMP target profiles field descriptions on page 725

Viewing an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. From the Target Profile list, click the profile you must view.
4. Click **View**.

   The system displays the details of the target profile in the View Target Details page.

Related Links

SNMP Target profile list on page 724
SNMP target profiles field descriptions on page 725

Deleting an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. From the Target Profile list, click the profile or profiles you want to delete.
4. Click **Delete**.
5. On the Delete Confirmation page, click **Delete**.

Note:

You cannot delete a target profile that is attached to an element or an agent.

Filtering target profiles

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **SNMP Target Profiles**.
3. Click **Filter: Enable** above the Profile List.
4. Apply the filter to one or multiple columns of the Target Profile List.
5. Click **Apply**.

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

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.

Related Links

Creating an SNMP target profile on page 722
Editing an SNMP target profile on page 723
Viewing an SNMP target profile on page 723

SNMP target profiles field descriptions

Name	Description
Name	The name of the SNMP target profile.
Description	The description of the SNMP target profile.
IP Address	The IP address of the target.
Port	The port number of the target.
Domain Type	The type of the message flow. The default is UDP.
Notification Type	The type of notification. The options are: • Trap • Inform
Protocol	The type of the SNMP protocol.

Button	Description
Commit	Creates the target profile in the New Target Profile page or saves the changes in the Edit Target Profile page.
Back	Cancels your action and takes you to the previous page.

Related Links

Creating an SNMP target profile on page 722
Editing an SNMP target profile on page 723
Viewing an SNMP target profile on page 723

Managing Serviceability Agents

Activating a serviceability agent

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In the **Agent List** section, select one or more agents that you must activate.
4. Click **Activate**.

   The system activates the SNMPv3 functionality in the remote serviceability agent that you selected. If the system does not activate the SNMPv3 functionality, refresh the Web page and repeat Step 3 and Step 4.

Managing SNMPv3 user profiles for the selected serviceability agents

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In the **Agent List** section, select an active agent that you must manage.
4. Click **Manage Profiles**.
5. Click the **SNMPv3 User Profile** tab.
6. In the **Assignable Profiles** section, select the user profiles that you want to assign.
7. Click **Assign**.

   To remove user profiles, in the **Removable Profiles** section, select the user profiles and click **Remove**.
8. To assign the user profiles to the selected agent, click **Commit**.

   Note:

   You can also select more than one serviceability agents and assign the same user profiles to all agents.

Managing target profiles for the selected serviceability agents

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents** > **Serviceability Agents**.
3. In Agent List, select the active agents that you must manage.
4. Click **Manage Profiles**.
5. Click the **SNMP Target Profiles** tab.
6. Select the target profiles you must assign from the Assignable Profiles section.
7. Click **Assign**.

   You can unassign or remove target profiles from the Removable Profiles section by clicking **Remove**.
8. Click **Commit** to assign the profiles to the selected agent.

   Note:

   You can also select more than one serviceability agents and assign the same target profiles to all the agents.

Serviceability Agents list

Name	Description
Hostname	The host name of the server on which the serviceability agent runs.
IP Address	The IP address of the server on which the serviceability agent runs.
System Name	The system name of the server on which the serviceability agent runs.
System OID	The system OID of the server on which the serviceability agent runs.
Status	The enabled or disabled status of the serviceability agent. The system disables SNMPv3 and displays **Inactive** as the default status.

System Manager TrapListener service

The TrapListener service receives traps and informs from different applications and displays the traps and alarms on the System Manager Alarming UI.

- TrapListener receives V2c and V3 traps and informs that are defined in the common alarm definition file.
- TrapListener also processes the Common Alarm Definition file for applications, where all the trap definitions are present.

You can configure the TrapListener service through Service Profile Management on System Manager. For information on configuring the TrapListener service, see *Configuring the TrapListener service* in this chapter.

If you change the Trap Listener settings, as an administrator, you should create a new SNMP Target Profile for the System Manager IP address, and a new SNMPv3 User Profile for the System Manager. Optionally, you can also edit the System Manager Target Profile and User Profile to match setting changes on System Manager trap listener. The values in these profiles should match the values in the Trap Listener settings. You should also attach this System Manager SNMPv3 User Profile to the System Manager Target Profile and then attach this Target Profile to all the Serviceability Agents.

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**.

TrapListener service field descriptions

Name	Description
Authentication Password	The password used to authenticate the user. The default is avaya123.

Table continues…

Name	Description
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.
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.

Session Manager SNMP MIB

This section lists the SNMP MIB tables and objects that can be queried on the Session Manager server by a network management system on the same network as the Session Manager

management interface. The Security Module is not included in this MIB. The Security Module is a different network interface and does not support SNMP queries.

- HOST-RESOURCES-MIB::hrDeviceDescr
- HOST-RESOURCES-MIB::hrDeviceErrors
- HOST-RESOURCES-MIB::hrDeviceID
- HOST-RESOURCES-MIB::hrDeviceIndex
- HOST-RESOURCES-MIB::hrDeviceStatus
- HOST-RESOURCES-MIB::hrDeviceType
- HOST-RESOURCES-MIB::hrDiskStorageAccess
- HOST-RESOURCES-MIB::hrDiskStorageCapacity
- HOST-RESOURCES-MIB::hrDiskStorageMedia
- HOST-RESOURCES-MIB::hrDiskStorageRemoveble
- HOST-RESOURCES-MIB::hrFSAccess
- HOST-RESOURCES-MIB::hrFSBootable
- HOST-RESOURCES-MIB::hrFSIndex
- HOST-RESOURCES-MIB::hrFSLastFullBackupDate
- HOST-RESOURCES-MIB::hrFSLastPartialBackupDate
- HOST-RESOURCES-MIB::hrFSMountPoint
- HOST-RESOURCES-MIB::hrFSRemoteMountPoint
- HOST-RESOURCES-MIB::hrFSStorageIndex
- HOST-RESOURCES-MIB::hrFSType
- HOST-RESOURCES-MIB::hrMemorySize
- HOST-RESOURCES-MIB::hrNetworkIfIndex
- HOST-RESOURCES-MIB::hrPartitionFSIndex
- HOST-RESOURCES-MIB::hrPartitionID
- HOST-RESOURCES-MIB::hrPartitionIndex
- HOST-RESOURCES-MIB::hrPartitionLabel
- HOST-RESOURCES-MIB::hrPartitionSize
- HOST-RESOURCES-MIB::hrProcessorFrwID
- HOST-RESOURCES-MIB::hrProcessorLoad
- HOST-RESOURCES-MIB::hrSWRunPerfCPU
- HOST-RESOURCES-MIB::hrSWRunPerfMem
- HOST-RESOURCES-MIB::hrStorageAllocationUnits

- HOST-RESOURCES-MIB::hrStorageDescr
- HOST-RESOURCES-MIB::hrStorageIndex
- HOST-RESOURCES-MIB::hrStorageSize
- HOST-RESOURCES-MIB::hrStorageType
- HOST-RESOURCES-MIB::hrStorageUsed
- HOST-RESOURCES-MIB::hrSystemDate
- HOST-RESOURCES-MIB::hrSystemInitialLoadDevice
- HOST-RESOURCES-MIB::hrSystemInitialLoadParameters
- HOST-RESOURCES-MIB::hrSystemMaxProcesses
- HOST-RESOURCES-MIB::hrSystemNumUsers
- HOST-RESOURCES-MIB::hrSystemProcesses
- HOST-RESOURCES-MIB::hrSystemUptime
- IF-MIB::ifAdminStatus
- IF-MIB::ifDescr
- IF-MIB::ifInDiscards
- IF-MIB::ifInErrors
- IF-MIB::ifInNUcastPkts
- IF-MIB::ifInOctets
- IF-MIB::ifInUcastPkts
- IF-MIB::ifInUnknownProtos
- IF-MIB::ifIndex
- IF-MIB::ifLastChange
- IF-MIB::ifMtu
- IF-MIB::ifNumber
- IF-MIB::ifOperStatus
- IF-MIB::ifOutDiscards
- IF-MIB::ifOutErrors
- IF-MIB::ifOutNUcastPkts
- IF-MIB::ifOutOctets
- IF-MIB::ifOutQLen
- IF-MIB::ifOutUcastPkts
- IF-MIB::ifPhysAddress
- IF-MIB::ifSpecific

- IF-MIB::ifSpeed
- IF-MIB::ifType
- SNMPv2-MIB::snmpEnableAuthenTraps
- SNMPv2-MIB::snmpInASNParseErrs
- SNMPv2-MIB::snmpInBadCommunityNames
- SNMPv2-MIB::snmpInBadCommunityUses
- SNMPv2-MIB::snmpInBadValues
- SNMPv2-MIB::snmpInBadVersions
- SNMPv2-MIB::snmpInGenErrs
- SNMPv2-MIB::snmpInGetNexts
- SNMPv2-MIB::snmpInGetRequests
- SNMPv2-MIB::snmpInGetResponses
- SNMPv2-MIB::snmpInNoSuchNames
- SNMPv2-MIB::snmpInPkts
- SNMPv2-MIB::snmpInReadOnlys
- SNMPv2-MIB::snmpInSetRequests
- SNMPv2-MIB::snmpInTooBigs
- SNMPv2-MIB::snmpInTotalReqVars
- SNMPv2-MIB::snmpInTotalSetVars
- SNMPv2-MIB::snmpInTraps
- SNMPv2-MIB::snmpOutBadValues
- SNMPv2-MIB::snmpOutGenErrs
- SNMPv2-MIB::snmpOutGetNexts
- SNMPv2-MIB::snmpOutGetRequests
- SNMPv2-MIB::snmpOutGetResponses
- SNMPv2-MIB::snmpOutNoSuchNames
- SNMPv2-MIB::snmpOutPkts
- SNMPv2-MIB::snmpOutSetRequests
- SNMPv2-MIB::snmpOutTooBigs
- SNMPv2-MIB::snmpOutTraps
- SNMPv2-MIB::snmpProxyDrops
- SNMPv2-MIB::snmpSilentDrops
- SNMPv2-MIB::sysContact

- SNMPv2-MIB::sysDescr
- SNMPv2-MIB::sysLocation
- SNMPv2-MIB::sysName
- SNMPv2-MIB::sysORDescr
- SNMPv2-MIB::sysORID
- SNMPv2-MIB::sysORLastChange
- SNMPv2-MIB::sysORUpTime
- SNMPv2-MIB::sysObjectID
- TCP-MIB::tcpActiveOpens
- TCP-MIB::tcpAttemptFails
- TCP-MIB::tcpCurrEstab
- TCP-MIB::tcpEstabResets
- TCP-MIB::tcpInErrs
- TCP-MIB::tcpInSegs
- TCP-MIB::tcpMaxConn
- TCP-MIB::tcpOutRsts
- TCP-MIB::tcpOutSegs
- TCP-MIB::tcpPassiveOpens
- TCP-MIB::tcpRetransSegs
- TCP-MIB::tcpRtoAlgorithm
- TCP-MIB::tcpRtoMax
- TCP-MIB::tcpRtoMin
- UDP-MIB::udpInDatagrams
- UDP-MIB::udpInErrors
- UDP-MIB::udpNoPorts
- UDP-MIB::udpOutDatagrams

Appendix D: Product notifications

Avaya issues a product change notice (PCN) for a software update. A PCN accompanies a service pack or patch that must be applied universally.

Avaya issues a product support notice (PSN) when there is a change in a product. A PSN provides information such as a workaround for a known problem and steps to recover software.

Both of these types of notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. Enter your login credentials, if applicable.
3. On the top of the page, click **DOCUMENTS**.
4. In the **Enter your Product Here** field, enter the name of the product, then select the product from the drop-down menu.
5. In the **Choose Release** field, select the specific release from the drop-down menu.
6. In the list of filters, select the **Product Correction Notices** and/or **Product Support Notices** check box.

   Note:

   You can select multiple filters to search for different types of documents at one time.
7. Click **Enter**.

Registering for product notifications

Note:

This procedure applies only to registered Avaya customers and business partners with an SSO login.

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. Log in using your SSO credentials.
3. Click on the **MY PROFILE** link.
4. Click the highlighted **HI, <username>** tab.
5. Select **E Notifications** from the menu.
6. In the **Product Notifications** section:
   a. Click **Add More Products**.
   b. Select the appropriate product.
7. In the Product box that appears on your screen:
   a. Select the appropriate release or releases for which you want to receive notifications.
   b. Select which types of notifications you want to receive. For example, **Product Support Notices** and **Product Correction Notices (PCN)**.
   c. Click **Submit**.
8. If you want notifications for other products, select another product from the list and repeat the above step.
9. Log out.

Appendix E: List of XML Schema Definitions and sample XMLs for bulk import

The following is the list of XML Schema Definition and sample XML snippets for bulk import of users, global setting records, elements, endpoint profiles, Messagingprofiles, CS 1000 profiles, CallPilot profiles, IP Office profiles, agent profiles, Session Manager profiles, Presence profiles, Collaboration Environment, and Conferencing profiles:

XML Schema Definition for bulk import of users on page 737

Sample XML for bulk import of users with minimal attributes on page 744

Sample XML for bulk import of users with all attributes on page 744

XML Schema Definition for partial import of user attributes on page 752

Sample XML for partial import of user attributes on page 754

XML Schema Definition for bulk deletion of users on page 756

Sample XML for bulk deletion of users on page 757

XML Schema Definition for bulk import of elements on page 757

Sample XML for bulk import of elements on page 762

XML Schema Definition for bulk import of Session Manager profiles on page 764

Sample XML for bulk import of Session Manager profiles on page 765

XML Schema Definition for bulk import of endpoint profiles on page 767

Sample XML for bulk import of endpoint profiles on page 794

XML Schema Definition for bulk import of messaging profiles on page 796

Sample XML for bulk import of Messaging profiles on page 803

XML Schema Definitions for bulk import of agent profiles on page 804

XML Schema for CS1000 and CallPilot communication Profiles on page 809

Sample XML for the CS1000 and CallPilot Communication Profiles on page 810

XML Schema for IP Office Communication Profiles on page 811

Sample XML for the IP Office Communication Profiles on page 818

XML Schema for bulk import and export of Presence Profile on page 819
Sample XML for Presence Communication Profile on page 819
XML Schema for bulk import of Conferencing Profile on page 822
Sample XML for the Conferencing Communication Profile on page 822
XML Schema for bulk import of Collaboration Environment Profile on page 793
Sample XML for bulk import of Collaboration Environment Profile on page 792
XML Schema Definition for bulk import of global setting records on page 823
Sample XML for bulk import of global setting records on page 829
XML Schema Definition for bulk deletion of global setting records on page 833
Sample XML for bulk deletion of global setting records on page 834
XML Schema Definition for bulk import of roles on page 835
Sample XML for bulk import of roles on page 838

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 '

When you copy the XML schema from the document you must take care of the line breaks.

XML Schema Definition for bulk import of users

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ext="http://xml.avaya.com/
schema/import" xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="http://
xml.avaya.com/schema/import" version="2.0">
    <xs:element name="secureStore" type="tns:xmlSecureStore"/>
    <xs:element name="user" type="tns:xmlUser"/>
    <xs:element name="users">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="secureStore" type="tns:xmlSecureStore" minOccurs="0"
maxOccurs="1"/>
                <xs:element name="user" type="tns:xmlUser" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:complexType name="xmlUser">
        <xs:sequence>
            <xs:element name="UserOrganizationDetails"
type="tns:UserOrganizationDetailsType"
                maxOccurs="1" minOccurs="0" />
            <xs:element name="UserProvisionRules" minOccurs="0">
                <xs:complexType>
```

```
                    <xs:sequence>
                        <xs:element name="UserProvisionRuleName" type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="authenticationType" type="xs:string"
                minOccurs="1" maxOccurs="1" />
            <xs:element name="description" type="xs:string"
                minOccurs="0" />
            <xs:element name="displayName" type="xs:string"
                minOccurs="0" />
            <xs:element name="displayNameAscii" type="xs:string"
                minOccurs="0" />
            <xs:element name="dn" type="xs:string" minOccurs="0" />
            <xs:element name="isDuplicatedLoginAllowed"
                type="xs:boolean" minOccurs="0" />
            <xs:element name="isEnabled" type="xs:boolean" minOccurs="0"
                maxOccurs="1" />
            <xs:element name="isVirtualUser" type="xs:boolean"
                minOccurs="0" />
            <xs:element name="givenName" type="xs:string" minOccurs="1"
                maxOccurs="1" />
            <xs:element name="givenNameAscii" type="xs:string" minOccurs="0"
                maxOccurs="1" />
            <xs:element name="honorific" type="xs:string" minOccurs="0" />
            <xs:element name="loginName" minOccurs="1" maxOccurs="1">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:maxLength value="128" />
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="newLoginName" minOccurs="0" maxOccurs="1">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:maxLength value="128" />
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="employeeNo" type="xs:string"
                minOccurs="0" maxOccurs="1">
            </xs:element>
            <xs:element name="department" type="xs:string" minOccurs="0"
                maxOccurs="1">
            </xs:element>
            <xs:element name="organization" type="xs:string"
                minOccurs="0" maxOccurs="1">
            </xs:element>
            <xs:element name="middleName" type="xs:string"
                minOccurs="0" />
            <xs:element name="managerName" type="xs:string"
                minOccurs="0" />
            <xs:element name="preferredGivenName" type="xs:string"
                minOccurs="0" />
            <xs:element name="preferredLanguage" type="xs:string"
                minOccurs="0" />
            <xs:element name="source" type="xs:string" minOccurs="0"
                maxOccurs="1" />
            <xs:element name="sourceUserKey" type="xs:string"
                minOccurs="0" maxOccurs="1" />
            <xs:element name="status" type="xs:string" minOccurs="0" />
            <xs:element name="suffix" type="xs:string" minOccurs="0" />
            <xs:element name="surname" type="xs:string" minOccurs="1"
                maxOccurs="1" />
```

```
            <xs:element name="surnameAscii" type="xs:string" minOccurs="0"
                maxOccurs="1" />
            <xs:element name="timeZone" type="xs:string" minOccurs="0" />
            <xs:element name="title" type="xs:string" minOccurs="0" />
            <xs:element name="userName" type="xs:string" minOccurs="0"
                maxOccurs="1" />
            <xs:element name="userPassword" type="xs:string"
                minOccurs="0" />
            <xs:element name="commPassword" type="xs:string"
                minOccurs="0" />
            <xs:element name="userType" type="xs:string" minOccurs="0"
                maxOccurs="unbounded" />
            <xs:element name="roles" minOccurs="0">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="role" type="xs:string"
                            minOccurs="0" maxOccurs="unbounded" />
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        <xs:element name="localizedNames" type="tns:xmLocalizedNames" minOccurs="0"
maxOccurs="1"></xs:element>
            <xs:element name="address" type="tns:xmlAddress"
                minOccurs="0" maxOccurs="unbounded" />
            <xs:element name="securityIdentity"
                type="tns:xmlSecurityIdentity" minOccurs="0" maxOccurs="unbounded" />
            <!-- Contact list Entries -->
            <xs:element name="ownedContactLists" minOccurs="0"
                maxOccurs="1">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="contactList"
                            type="tns:xmlContactList" maxOccurs="1" />
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="ownedContacts" minOccurs="0">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="contact" type="tns:xmlContact"
                            maxOccurs="unbounded" />
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <!-- Presence ACL User Entries -->
            <xs:element name="presenceUserDefault"
                type="tns:xmlPresUserDefaultType" minOccurs="0" />
            <xs:element name="presenceUserACL"
                type="tns:xmlPresUserACLEntryType" minOccurs="0"
                maxOccurs="unbounded" />
            <xs:element name="presenceUserCLDefault"
                type="tns:xmlPresUserCLDefaultType" minOccurs="0" maxOccurs="1" />
            <xs:element name="commProfileSet"
                type="tns:xmlCommProfileSetType" minOccurs="0"
                maxOccurs="unbounded" />

        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlSecurityIdentity">
        <xs:sequence>
            <xs:element name="identity" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="realm" type="xs:string" minOccurs="0"/>
            <xs:element name="type" type="xs:string" minOccurs="1" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
```

```
    <xs:complexType name="xmlPresInfoTypeAccessType">
        <xs:sequence>
            <xs:element name="infoType" type="tns:xmlPresInfoTypeType" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="access" type="xs:string" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlPresACRuleType">
        <xs:sequence>
            <xs:element name="infoTypeAccess" type="tns:xmlPresInfoTypeAccessType"
minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlPresUserDefaultType">
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType"/>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresUserCLDefaultType">
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType"/>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresUserACLEntryType">
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType">
                <xs:sequence>
                    <xs:choice>
                        <xs:element name="watcherLoginName" type="xs:string"
minOccurs="0"/>
                        <xs:element name="watcherDisplayName" type="xs:string"
minOccurs="0"/>
                    </xs:choice>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresInfoTypeType">
        <xs:sequence>
            <xs:element name="label" type="xs:string" maxOccurs="1"/>
            <xs:element name="filter" type="xs:string" maxOccurs="1"/>
            <xs:element name="specFlags" type="xs:string" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <!-- Contact List entries -->
    <xs:complexType name="xmlContactList">
        <xs:sequence>
            <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="description" type="xs:string" minOccurs="0"/>
            <xs:element name="isPublic" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
            <xs:element name="members" type="tns:xmlContactListMember" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="contactListType" type="xs:string" minOccurs="1"
maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlContactListMember">
        <xs:sequence>
            <xs:choice>
                <xs:sequence>
                    <xs:element name="memberContact" type="xs:string" minOccurs="0"/>
                    <xs:element name="speedDialContactAddress"
type="tns:xmlContactAddress" minOccurs="0"/>
                </xs:sequence>
                <xs:sequence>
```

```
                    <xs:element name="memberUser" type="xs:string" minOccurs="0"/>
                    <xs:element name="speedDialHandle" type="tns:xmlHandle"
minOccurs="0"/>
                </xs:sequence>
            </xs:choice>
            <xs:element name="isFavorite" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
            <xs:element name="isSpeedDial" type="xs:boolean" minOccurs="1"/>
            <xs:element name="speedDialEntry" type="xs:int" minOccurs="0"/>
            <xs:element name="isPresenceBuddy" type="xs:boolean" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="label" type="xs:string" minOccurs="0"/>
            <xs:element name="altLabel" type="xs:string" minOccurs="0"/>
            <xs:element name="description" type="xs:string" minOccurs="0"/>
            <xs:element name="priorityLevel" type="xs:int" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlContactAddress">
        <xs:sequence>
            <xs:element name="address" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="altLabel" type="xs:string" minOccurs="0"/>
            <xs:element name="contactCategory" type="xs:string" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="contactType" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="label" type="xs:string" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlAddress">
        <xs:sequence>
            <xs:element name="addressType" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="building" type="xs:string" minOccurs="0"/>
            <xs:element name="localityName" type="xs:string" minOccurs="0"/>
            <xs:element name="postalCode" type="xs:string" minOccurs="0"/>
            <!-- Additional Attribute Support - The attribute room will be mapped to
cubical.-->
            <xs:element name="room" type="xs:string" minOccurs="0"/>
            <xs:element name="stateOrProvince" type="xs:string" minOccurs="0"/>
            <xs:element name="country" type="xs:string" minOccurs="0"/>
            <xs:element name="street" type="xs:string" minOccurs="0"/>
            <!-- Additional Attribute Support -->
            <xs:element name="businessphone" type="xs:string" minOccurs="0"/>
            <xs:element name="otherbusinessphone" type="xs:string" minOccurs="0"/>
            <xs:element name="fax" type="xs:string" minOccurs="0"/>
            <xs:element name="homephone" type="xs:string" minOccurs="0"/>
            <xs:element name="otherhomephone" type="xs:string" minOccurs="0"/>
            <xs:element name="mobilephone" type="xs:string" minOccurs="0"/>
            <xs:element name="othermobilephone" type="xs:string" minOccurs="0"/>
            <xs:element name="pager" type="xs:string" minOccurs="0"/>
            <xs:element name="pager2" type="xs:string" minOccurs="0"/>
            <!-- Additional Attribute Support - End -->
            <xs:element name="postalAddress" minOccurs="0">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:maxLength value="1024"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="isPrivate" type="xs:boolean" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlContact">
        <xs:sequence>
            <xs:element name="company" type="xs:string" minOccurs="0"/>
            <xs:element name="description" type="xs:string" minOccurs="0"/>
            <xs:element name="displayName" type="xs:string" minOccurs="1" maxOccurs="1"/>
```

```
            <xs:element name="displayNameAscii" type="xs:string" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="dn" type="xs:string" minOccurs="0"/>
            <xs:element name="givenName" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="givenNameAscii" type="xs:string" minOccurs="0"
maxOccurs="1"/>
            <xs:element name="initials" type="xs:string" minOccurs="0"/>
            <xs:element name="middleName" type="xs:string" minOccurs="0"/>
            <xs:element name="preferredGivenName" type="xs:string" minOccurs="0"
maxOccurs="1"/>
            <xs:element name="preferredLanguage" type="xs:string" minOccurs="0"/>
            <xs:element name="isPublic" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
            <xs:element name="source" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="sourceUserKey" type="xs:string" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="suffix" type="xs:string" minOccurs="0"/>
            <xs:element name="surname" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="surnameAscii" type="xs:string" minOccurs="0" maxOccurs="1"/>
            <xs:element name="title" type="xs:string" minOccurs="0"/>
            <xs:element name="ContactAddress" type="tns:xmlContactAddress" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="addresses" type="tns:xmlAddress" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlHandle">
        <xs:sequence>
            <xs:element name="handleName" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="handleType" type="xs:string" minOccurs="1" maxOccurs="1"/>
            <xs:element name="handleSubType" type="xs:string" minOccurs="0"
maxOccurs="1"/>
            <xs:element name="domainName" type="xs:string" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlCommProfileType">
        <xs:sequence>
            <xs:element name="commProfileType" type="xs:string" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="commProfileSubType" type="xs:string" minOccurs="0"
maxOccurs="1"/>
            <xs:element name="jobId" type="xs:string" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlCommProfileSetType">
        <xs:sequence>
            <xs:element name="commProfileSetName" type="xs:string" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="isPrimary" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
            <xs:element name="handleList" minOccurs="0">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="handle" type="tns:xmlHandle"
maxOccurs="unbounded"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="commProfileList" minOccurs="0">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="commProfile" type="tns:xmlCommProfileType"
maxOccurs="unbounded"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
```

```
    </xs:complexType>
    <xs:complexType name="ForgeinCommProfileType">
        <xs:complexContent>
            <xs:extension base="ext:xmlCommProfileType">
                <xs:sequence>
                    <xs:element name="csEncryptionKeyId" type="xs:long" minOccurs="0"
maxOccurs="1"/>
                    <xs:element name="servicePassword" type="xs:string" minOccurs="0"
maxOccurs="1"/>
                    <xs:element name="serviceData" type="xs:string" minOccurs="0"
maxOccurs="1"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlSecureStore">
        <xs:sequence>
            <xs:element name="secureStoreData" type="xs:base64Binary" minOccurs="1"
maxOccurs="1"/>
            <xs:element name="passwordEncrypted" type="xs:boolean"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlLocalizedName">
        <xs:sequence>
            <xs:element name="locale" type="xs:string" minOccurs="1"
                maxOccurs="1">
            </xs:element>
            <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"></
xs:element>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmLocalizedNames">
        <xs:sequence>
            <xs:element name="localizedName" type="tns:xmlLocalizedName" minOccurs="0"
maxOccurs="7"></xs:element>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="UserOrganizationDetailsType">
            <xs:sequence>
            <xs:element name="tenant" maxOccurs="1" minOccurs="1">
                    <xs:complexType>
                    <xs:attribute name="name" type="xs:string" use="required"/>
                       <xs:attribute name="createTenantIfNotAlreadyPresent"
                                        type="xs:boolean"
                                            use="required"/>
                    </xs:complexType>
                </xs:element>
                <xs:element name="organizationUnitLevelOne" type="xs:string"
                    maxOccurs="1" minOccurs="0">
                </xs:element>
                <xs:element name="organizationUnitLevelTwo" type="xs:string"
                    maxOccurs="1" minOccurs="0">
                </xs:element>
                <xs:element name="organizationUnitLevelThree" type="xs:string"
                    maxOccurs="1" minOccurs="0">
                </xs:element>
            </xs:sequence>
    </xs:complexType>

</xs:schema>
```

Sample XML for bulk import of users with minimal attributes

```
<?xml version="1.0" encoding="UTF-8"?>
    <!--  Root Element 'Users' represent collection of  user (containing 1 or
    more users)-->
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"  xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd" >

  <tns:user>
    <authenticationType>Basic</authenticationType>
    <givenName>John</givenName>
    <loginName>jmiller@avaya.com</loginName>
    <surname>Miller</surname>
    <userPassword>mypassword</userPassword>
  </tns:user>
</tns:users>
```

Sample XML for bulk import of users with all attributes

```
<?xml version="1.0" encoding="UTF-8"?>
<!--  Root Element 'Users' represent collection of  user (containing 1 or more
        users)-->
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"  xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd">
<!--    authenticationType: This defines the type of authentication that this user
        will undergo at runtime to obtain access to the system.
        Possible Values: BASIC,ENTERPRISE
     ---description:A text description of the user. Human readable description of
        this user instance.
     ---displayName:The localized name of a user to be used when displaying. It
        will typically be the localized full name. This value may be provisioned
        from the users enterprise directory entry. If it does not exist,
        synchronization rules can be used to populate it for other fields
        e.g. Surname, GivenName, or LoginName.
     ---displayNameAscii:This corresponds to the
         Console attribute-Endpoint Display Name.
        The full text name of the user represented in ASCII. It is used to support
        display (e.g. endpoints) that cannot handle localized text
     ---dn:The distinguished name of the user. The DN is a sequence of relative
        distinguished names (RDN) connected by commas. An RDN is an attribute with
        an associated value in the form of attribute=value, normally expressed in a
        UTF-8 string format.The dn can be used to identify the user and may be used
        for authentication subject mapping. Note the dn is changeable.
     ---isDuplicatedLoginAllowed:A boolean indicator showing whether this user is
        allowed a duplicate concurrent logins.A true stipulates that the user is
        allow to have duplicate logins. Default value is true.
     ---isEnabled:A boolean indicator showing whether or not the user is active.
        Users with AuthenticationType equals Basic will fail if this value is false.
        This attribute can be used to disable access between login attempts.
        A running sessions login will not be revocable. Alternatively the
        administrator can always modify the password to disable the user from
        logging in. A true stipulates this is an active user, a false used for a
        disabled  user. Default value is false.
     ---isVirtualUser:A boolean indicator showing whether or not the record is being
        used for a non-human entity such as an application, service, software agent,
        etc. This is to be used where the entity will behave as a user and needs to
        have subset of the user profile populated. If the entity does not behave as
        a user and has a different trust relationship e.g. a trust certificate it
        should not be treated as a virtual user. A virtual user can represent an
        Avaya or external non-human entity. This attribute is provided as a
        convenience to track such accounts.A true stipulates this is a virtual user,
        a false is used for human users. Default value is false.
     ---givenName:The first name of the user.
     ---honorific:The personal title used to address a user. This is typically a
```

```
      social title and not the work title which is contained in the title
      attribute. This attribute can map to PersonalTitle.
   ---loginName:This is the unique system login name given to the user. It can
      take the form of username@domain or just username.This may vary across
      customers.It  can be used to help provision default user handles in the
      CSHandle table. The username is an alphanumeric value that must comply
      with the userinfo related portion of a URI as described in rfc2396. However,
      it is further restricted as ASCII characters with only the _ and . special
      characters supported.  This is the rfc2798 uid attribute.
   ---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 only the _ and . special characters supported.
      This is the rfc2798 uid attribute.
   ---userPassword:The encrypted password for this users account.A null password
      is used when the user is authenticated by the enterprise such as with a
      separate source such as the enterprise LDAP.
   ---commPassword:The encrypted subscriber or communication password with which
      the user logs can use to authentication with on to any CommProfile SIP and
      non SIP.  This attribute is meant to be a shared across different
      communication profiles and thus different communication services.
   ---userType:This enumerates the possible primary user application types.
      A User can be associated with multiple user types. Possible values are
      ADMINISTRATOR; COMMUNICATION USER;AGENT;SUPERVISOR;RESIDENT EXPERT;SERVICE
      TECHNICIAN;LOBBY PHONE
   ---roles:Text name of a role.This value needs to pre-exist in SMGR DB
   ---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" 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>
```

XML Schema Definition for bulk import of elements

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://www.avaya.com/rts"
    xmlns="http://www.avaya.com/rts"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="qualified" attributeFormDefault="unqualified">

    <!-- <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"> -->
```

```
    <xs:element name="RTSElements">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="ApplicationSystems" minOccurs="0"
                    maxOccurs="unbounded">
                    <xs:annotation>
                        <xs:documentation>
                            Application System Types
                        </xs:documentation>
                    </xs:annotation>
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="ApplicationSystem"
                                type="ApplicationSystem" maxOccurs="unbounded">
                            </xs:element>

                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="ApplicationSystemAssigns"
                    minOccurs="0" maxOccurs="unbounded">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Source" type="Source"
                                minOccurs="1" maxOccurs="unbounded" />
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <xs:complexType name="ApplicationSystem">
        <xs:annotation>
            <xs:documentation></xs:documentation>
        </xs:annotation>

        <xs:sequence>
            <xs:element name="Host" type="Host" minOccurs="1"
                maxOccurs="1">
            </xs:element>
            <xs:element name="ApplicationSystemType"
                type="ApplicationSystemType" minOccurs="1" maxOccurs="1">
            </xs:element>

            <xs:element name="SecureStoreData" type="SecureStoreData" minOccurs="0"
maxOccurs="1"/>

            <xs:element name="AccessPoints" minOccurs="0"
                maxOccurs="unbounded">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="AccessPoint"
                            type="AccessPoint" minOccurs="1" maxOccurs="unbounded" />
                    </xs:sequence>
                </xs:complexType>
            </xs:element>

            <xs:element name="Ports" minOccurs="0"
                maxOccurs="unbounded">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="Port" type="Port"
                            minOccurs="1" maxOccurs="unbounded" />
                    </xs:sequence>
```

```
            </xs:complexType>
        </xs:element>

        <xs:element name="SNMPAttributes" type="SNMPAttributes" minOccurs="0"
            maxOccurs="1">
        </xs:element>

        <xs:element name="Attributes" minOccurs="0"
            maxOccurs="unbounded">
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="Attribute" type="Attribute"
                        minOccurs="1" maxOccurs="unbounded" />
                </xs:sequence>
            </xs:complexType>
        </xs:element>

    </xs:sequence>

    <xs:attribute name="name" type="xs:string" use="required">
    </xs:attribute>

    <xs:attribute name="description" type="xs:string">
    </xs:attribute>

    <xs:attribute name="displaykey" type="xs:string"></xs:attribute>

    <xs:attribute name="isTrusted" type="xs:boolean"></xs:attribute>

</xs:complexType>
<xs:complexType name="SNMPAttributes">
    <xs:annotation>
        <xs:documentation></xs:documentation>
    </xs:annotation>
    <xs:attribute name="snmpVersion" type="snmpVersionType" use="required">
    </xs:attribute>

    <xs:attribute name="readCommunity" type="xs:string">
    </xs:attribute>

    <xs:attribute name="writeCommunity" type="xs:string">
    </xs:attribute>

    <xs:attribute name="userName" type="xs:string">
    </xs:attribute>

    <xs:attribute name="authenticationProtocol" type="authenticationProtocolType">
    </xs:attribute>

    <xs:attribute name="authenticationPassword" type="xs:string">
    </xs:attribute>

    <xs:attribute name="privacyProtocol" type="privacyProtocolType">
    </xs:attribute>

    <xs:attribute name="privacyPassword" type="xs:string">
    </xs:attribute>

    <xs:attribute name="snmpRetries" type="xs:int" use="required">
    </xs:attribute>

    <xs:attribute name="snmpTimeout" type="xs:long" use="required">
    </xs:attribute>

    <xs:attribute name="deviceTypeName" type="xs:string"> </xs:attribute>
```

```
    <xs:attribute name="sysOid" type="xs:string">
    </xs:attribute>
</xs:complexType>

<xs:complexType name="Host">
    <xs:annotation>
        <xs:documentation></xs:documentation>
    </xs:annotation>

    <xs:attribute name="ipaddress" type="xs:string"
        use="required">
    </xs:attribute>

    <xs:attribute name="description" type="xs:string">
    </xs:attribute>

    <xs:attribute name="ostype" type="xs:string"></xs:attribute>
</xs:complexType>

<xs:complexType name="ApplicationSystemType">
    <xs:annotation>
        <xs:documentation></xs:documentation>
    </xs:annotation>

    <xs:attribute name="name" type="xs:string" use="required">
    </xs:attribute>

    <xs:attribute name="version" type="xs:string" use="required">
    </xs:attribute>

</xs:complexType>

<xs:complexType name="AccessPoint">
    <xs:annotation>
        <xs:documentation></xs:documentation>
    </xs:annotation>

    <xs:attribute name="name" type="xs:string" use="required">
    </xs:attribute>

    <xs:attribute name="description" type="xs:string">
    </xs:attribute>

    <xs:attribute name="displaykey" type="xs:string"></xs:attribute>

    <xs:attribute name="type" type="AccessPointType"
        use="required">
    </xs:attribute>

    <xs:attribute name="uri" type="xs:string"></xs:attribute>

    <xs:attribute name="host" type="xs:string" use="required">
    </xs:attribute>

    <xs:attribute name="port" type="xs:string"></xs:attribute>

    <xs:attribute name="protocol" type="xs:string"></xs:attribute>

    <xs:attribute name="loginid" type="xs:string"></xs:attribute>

    <xs:attribute name="password" type="xs:string"></xs:attribute>

    <xs:attribute name="containerType" type="ContainerType"></xs:attribute>
```

```
        <xs:attribute name="order" type="xs:int" use="required">
        </xs:attribute>

    </xs:complexType>

    <xs:complexType name="Port">
        <xs:annotation>
            <xs:documentation></xs:documentation>
        </xs:annotation>

        <xs:attribute name="name" type="xs:string" use="required">
        </xs:attribute>

        <xs:attribute name="description" type="xs:string">
        </xs:attribute>

        <xs:attribute name="protocol" type="xs:string" use="required"></xs:attribute>

        <xs:attribute name="port" type="xs:int" use="required"></xs:attribute>
    </xs:complexType>

    <xs:complexType name="Source">
        <xs:sequence>
            <xs:element name="Assignment" minOccurs="1"
                maxOccurs="unbounded">
                <xs:complexType>
                    <xs:attribute name="name" type="xs:string">
                    </xs:attribute>

                    <xs:attribute name="targetAppSystemName"
                        type="xs:string" use="required">
                    </xs:attribute>

                    <xs:attribute name="targetAppSystemTypeName"
                        type="xs:string" use="required">
                    </xs:attribute>

                    <xs:attribute name="targetAppSystemTypeVersion"
                        type="xs:string" use="required">
                    </xs:attribute>

                    <xs:attribute name="targetAppSystemHost"
                        type="xs:string" use="required">
                    </xs:attribute>

                    <xs:attribute name="priority" type="xs:int"></xs:attribute>
                </xs:complexType>
            </xs:element>
        </xs:sequence>

        <xs:attribute name="sourceApplicationSystemName"
            type="xs:string" use="required">
        </xs:attribute>

        <xs:attribute name="sourceAppSystemTypeName" type="xs:string"
            use="required">
        </xs:attribute>

        <xs:attribute name="sourceAppSystemTypeVersion" type="xs:string"
            use="required">
        </xs:attribute>

        <xs:attribute name="sourceAppSystemHost" type="xs:string"
            use="required">
        </xs:attribute>
```

```
    </xs:complexType>

    <xs:complexType name="Attribute">
        <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
        <xs:attribute name="value" type="xs:string" use="required"></xs:attribute>
        <!--  added for secure store integration. -->
        <xs:attribute name="isencrypted" type="xs:boolean" use="optional"
default="false"></xs:attribute>
    </xs:complexType>

    <xs:complexType name="SecureStoreData">
        <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
        <xs:attribute name="value" type="xs:string" use="required"></xs:attribute>
    </xs:complexType>

    <xs:simpleType name="AccessPointType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="TrustManagement" />
            <xs:enumeration value="EMURL" />
            <xs:enumeration value="WS" />
            <xs:enumeration value="GUI" />
            <xs:enumeration value="Other" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="ContainerType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="JBOSS" />
            <xs:enumeration value="SIPAS" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="authenticationProtocolType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="MD5" />
            <xs:enumeration value="SHA" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="privacyProtocolType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="DES"/>
            <xs:enumeration value="3DES"/>
            <xs:enumeration value="AES128"/>
            <xs:enumeration value="AES192"/>
            <xs:enumeration value="AES256"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="snmpVersionType">
        <xs:restriction base="xs:int">
            <xs:enumeration value="1"/>
            <xs:enumeration value="3"/>
        </xs:restriction>
    </xs:simpleType>

</xs:schema>
```

Sample XML for bulk import of elements

```
<?xml version="1.0" encoding="UTF-8"?>
<RTSElements xsi:schemaLocation="http://www.avaya.com/rts ApplicationSystems.xsd "
xmlns="http://www.avaya.com/rts" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <ApplicationSystems>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test1">
```

```
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test2">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test3">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test4">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test5">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test6">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test7">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test8">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test9">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test10">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Tes11t">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test12">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test13">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test14">
```

```
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
    </ApplicationSystems>
</RTSElements>
```

XML Schema Definition for bulk import of Session Manager profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:smgr="http://xml.avaya.com/schema/import"
            targetNamespace="http://xml.avaya.com/schema/import_sessionmanager"
            elementFormDefault="qualified">

<!--
    This is the XML schema for the "Session Manager Profile". It defines this
    profile inside of an XML document that defines a user record
    (see userimport.xsd)
-->

<xsd:import namespace="http://xml.avaya.com/schema/import"
            schemaLocation="userimport.xsd"/>

<xsd:complexType name="SessionManagerCommProfXML">

    <xsd:complexContent>
        <xsd:extension base="smgr:xmlCommProfileType" >

    <xsd:sequence>
      <!--
       The following attributes are the names of objects that must
       already be administered in System Manager before performing
         the user import.

         The relative order here cannot be changed because it would
         break backwards compatibility with existing XML documents
         that could be used for an import.
      -->

      <!-- Name of the primary Session Manager (required) -->
      <xsd:element name="primarySM" type="xsd:string" minOccurs="1" />

      <!--  Name of the secondary Session Manager (optional) -->
          <xsd:element name="secondarySM" type="xsd:string" minOccurs="0" />

      <!-- Name of the Termination Application Sequence (optional) - administered
           under Session Manager /Application Configuration /Application Sequences
       -->
          <xsd:element name="terminationAppSequence" type="xsd:string"  minOccurs="0" />

          <!-- Name of the Origination Application Sequence (optional)
               - administered under
                 Session Manager /Application Configuration /Application Sequences --
>
          <xsd:element name="originationAppSequence" type="xsd:string" minOccurs="0" />

          <!-- Name of the Conference Factory Set (optional)
              - administered under
                Session Manager / Application Configuration / Conference Factories  -->
          <xsd:element name="confFactorySet" type="xsd:string" minOccurs="0" />

          <!-- Name of the Survivability Server (optional)
             - usually the name of a Branch Session Manager, but can be any non-CM
               SIP Entity -->
          <xsd:element name="survivabilityServer" type="xsd:string" minOccurs="0" />
```

```
          <!-- Name of the Home Location (required)
                - administered under Routing / Locations -->
          <xsd:element name="homeLocation" type="xsd:string"  minOccurs="1" />

          <!-- The maximum number of endpoints that can be simultaneously
                registered using this Session Manager Profile. (optional)
               - The value is an integer between 1 and 10 and
                 defaults to 1 if not specified.  -->
          <xsd:element name="maxSimultaneousDevices" minOccurs="0">
            <xsd:simpleType>
                      <xsd:restriction base="xsd:integer">
                          <xsd:minInclusive value="1" />
                         <xsd:maxInclusive value="10" />
                      </xsd:restriction>
                  </xsd:simpleType>
          </xsd:element>

        <!--
        If true, new registrations will be blocked for this Session Manager
        Profile if the maximum number of simultaneously registered endpoints
        (see "maxSimultaneousDevices" above) is currently registered.  If
          false, an existing registration will be terminated to allow a new
          registration for this Session Manager Profile. (optional)
          - the value defaults to false if not specified
        -->
          <xsd:element name="blockNewRegistrationWhenMaxActive" minOccurs="0">
                <xsd:simpleType>
                      <xsd:restriction base="xsd:boolean" />
                  </xsd:simpleType>
          </xsd:element>

    </xsd:sequence>

        </xsd:extension>
    </xsd:complexContent>
 </xsd:complexType>


</xsd:schema>
```

Sample XML for bulk import of Session Manager profiles

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd ">

    <!-- User Record for: 5555555@domain.com -->
    <tns:user>

    (Other user elements are required here - consult the main user record
    XML schema reference)

    <!--
        This is the password for any SIP endpoints (phones) associated with the
        user's Session Manager Profile
    -->
        <commPassword>123456</commPassword>
    <!--
    (Other user elements may be required here - consult the main user record
    XML schema reference)
    -->
    <!-- Here, a Communication Profile is defined for the user -->
       <commProfileSet>
```

```
           <commProfileSetName>Primary</commProfileSetName>
                <isPrimary>true</isPrimary>

        <!-- The user must be given one or more handles of type "SIP" to associate SIP
            devices with the Session Manager Profile.  In this case, a SIP phone will
            be registered with a Session Manager as 5555555@domain.com -->
                <handleList>
                <handle>
                <handleName>5555555</handleName>
                <handleType>sip</handleType>
                <handleSubType>username</handleSubType>
                <domainName>domain.com</domainName>
                </handle>
                </handleList>

        <!-- Here, one or more product-specific profiles may be defined -->
        <!-- A Session Manager Profile is defined to associate a maximum of two
            SIP phones,having the SIP handle, 5555555@domain.com, with...
            "Primary Session Manager" ('Primary SM')
            "Secondary Session Mananger" instance ('Secondary SM')
            "Termination Sequence" ('Sequence to My CM'),
            "Origination Sequence" ('Sequence to My CM'),
            "Conference Factory Set" ('EngeeringDepartmentConferenceSet')
            "Survivability Server" ("BSM" value below),
            "Home Location" ('My Home').
            If both phones are registered and a third phone tries to register
            using the same SIP handle, one of the two phones will have its
            registration terminated to allow the third phone to register.
        -->
<commProfileList>
                <commProfile xsi:type="ns3:SessionManagerCommProfXML" xmlns:ns3="http://
xml.avaya.com/schema/import_sessionmanager">
                    <commProfileType>SessionManager</commProfileType>
                    <ns3:primarySM>Primary SM</ns3:primarySM>
                    <ns3:secondarySM>Secondary SM</ns3:secondarySM>
                    <ns3:terminationAppSequence>Sequence to My CM</
ns3:terminationAppSequence>
                    <ns3:originationAppSequence>Sequence to My CM</
ns3:originationAppSequence>
                                <ns3:confFactorySet>EngeeringDepartmentConferenceSet</
ns3:confFactorySet>
                    <ns3:survivabilityServer>BSM</ns3:survivabilityServer>
                    <ns3:homeLocation>My Home</ns3:homeLocation>
                    <ns3:maxSimultaneousDevices>3</ns3:maxSimultaneousDevices>
                    <ns3:blockNewRegistrationWhenMaxActive>false</
ns3:blockNewRegistrationWhenMaxActive>
                </commProfile>

        <!--
            A CM Station Profile is associated with this Communication Profile.
            The application sequence, "Sequence to My CM", invoked by Session
            Manager for calls to and from 5555555@domain.com, sequences calls to
            the CM, "My CM".
            SIP devices associated with this Communication Profile are associated
            with the CM Station that has number 555-5555. The CM Station, 555-5555,
            already exists on the CM, so the "useExistingExtension" element has
            value "true".
        -->

                <commProfile xsi:type="ipt:xmlStationProfile" xmlns:ipt="http://
xml.avaya.com/schema/import_csm_cm">
                    <commProfileType>CM</commProfileType>
                    <ipt:cmName>My CM</ipt:cmName>
                    <ipt:useExistingExtension>true</ipt:useExistingExtension>
                    <ipt:extension>5555555</ipt:extension>
```

```
                </commProfile>

            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema Definition for bulk import of endpoint profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:one="http://xml.avaya.com/
schema/import" elementFormDefault="qualified"
targetNamespace="http://xml.avaya.com/schema/import_csm_cm" xmlns:csm="http://
xml.avaya.com/schema/import_csm_cm">
<xs:import namespace="http://xml.avaya.com/schema/import"
schemaLocation="userimport.xsd"/>

<!--Changes in xsd file need to generate jaxb src using this xsd-->
<xs:complexType name="xmlStationProfile">
    <xs:complexContent>
           <xs:extension base="one:xmlCommProfileType" >
            <xs:sequence>

                <!-- CM Name as it appears under 'Applications/Application Management/
Entities -->
                <xs:element name="cmName" type="xs:string" maxOccurs="1" minOccurs="1"/>
                <xs:element name="prefHandleId" type="xs:string" maxOccurs="1"
minOccurs="0"/>
                <!-- 'true' if already created extension is to be used.  'false' if
available extension is to be used. -->
                <xs:element name="useExistingExtension" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

                <!-- Extension Range which will be used to create Station using available
extension within given range -->
                <xs:element name="extensionRange" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|([0-9]+([\.\-]
[0-9]+)*:[0-9]+([\.\-][0-9]+)*)"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Station extension number that need to be assigned to the user. -->
                <xs:element name="extension" maxOccurs="1" minOccurs="1">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|[nN][eE][xX][tT]"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Template name to be used to create station. Values defined in
Template will be used if not provided. -->
                <xs:element name="template" type="xs:string" maxOccurs="1" minOccurs="0"/>

                <!-- Specifies the set type of the station  -->
                <xs:element name="setType" type="xs:string" maxOccurs="1" minOccurs="0"/>

                <!-- Security code for station. Value can be digit only.  -->
                <xs:element name="securityCode" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]*"/>
```

```
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <!-- Valid values for port   -->
                <!--01 to 64  First and second numbers are the cabinet number  -->
                <!--A to E  Third character is the carrier  -->
                <!--01 to 20  Fourth and fifth characters are the slot number  -->
                <!--01 to 32  Sixth and seventh characters are the circuit number  -->
                <!--x or X  Indicates that there is no hardware associated with the port
assignment since the switch was set up, and the administrator expects that the extension
would have a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x
for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) stations, as well
as for SBS Extensions.  -->
                <!--IP  Indicates that there is no hardware associated with the port
assignment since the switch was set up, and the administrator expects that the extension
would have an IP set. This is automatically entered for certain IP station set types, but
you can enter for a DCP set with softphone permissions. This changes to the s00000 type
when the set registers.  -->
                <xs:element name="port" type="xs:string" maxOccurs="1" minOccurs="0" />

                <!-- Whether the station should be deleted if it unassigned from the
user. -->
                <xs:element name="deleteOnUnassign" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

                <!-- Whether the endpoint name on CM should be overridden with the value
in User. -->
                <xs:element name="overRideEndpointName" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

                <!-- true/false for Enhanced Callr-Info display for 1-line phones -->
                <xs:element name="enhCallrInfodisplay" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

                <!-- true/false to enable/disable lock messages feature. -->
                <xs:element name="lockMessages" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!-- A coverage path is a prioritized sequence of extensions to which
your voice system will route an unanswered call. -->
                <!-- Valid values: CM 5.2 - Path Number between 1-2000, time of day
table, t1-t999, or blank. -->
                <!-- Valid values: CM 6.0 - Path Number between 1-9999, time of day
table, t1-t999, or blank. -->
                <xs:element name="coveragePath1" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="([1-9]{0})|(t[1-9][0-9]{0,2})|([1-9][0-9]
{0,3})"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- A coverage path is a prioritized sequence of extensions to which
your voice system will route an unanswered call. -->
                <!-- Valid values: CM 5.2 - Path Number between 1-2000, time of day
table, t1-t999, or blank. -->
                <!-- Valid values: CM 6.0 - Path Number between 1-9999, time of day
table, t1-t999, or blank. -->
                <xs:element name="coveragePath2" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="([1-9]{0})|(t[1-9][0-9]{0,2})|([1-9][0-9]
```

```
{0,3})"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- The extension the system should hunt to for this telephone when the
telephone is busy. A station hunting chain can be created by assigning a hunt-to station
to a series of telephones.  -->
                <xs:element name="huntToStation" type="xs:string" maxOccurs="1"
minOccurs="0" />

                <!-- Provides for partitioning of attendant groups and/or stations and
trunk groups. -->
                <!-- Typically this is used for multiple tenants in a building or
multiple departments within a company or organization. -->
                <!-- Valid values: 1 to 250 when TN is ON in special application and 1 to
100 o.w. -->
                <xs:element name="tn" maxOccurs="1" minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:int">
                            <xs:minInclusive value="1" />
                            <xs:maxInclusive value="250" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Typically this is used for multiple tenants in a building or
multiple departments within a company or organization. -->
                <!-- Typically this is used for multiple tenants in a building or
multiple departments within a company or organization. -->
                <!-- Valid values: 0 to 995 -->
                <xs:element name="cor" maxOccurs="1" minOccurs="0">
                      <xs:simpleType>
                        <xs:restriction base="xs:int">
                              <xs:minInclusive value="0"/>
                              <xs:maxInclusive value="995"/>
                        </xs:restriction>
                      </xs:simpleType>
                </xs:element>

                <!-- Class of Service lets you define groups of users and control those
groups' access to features -->
                <!-- Valid values: 1 to 15 -->
                <xs:element name="cos" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:int">
                            <xs:minInclusive value="0" />
                            <xs:maxInclusive value="15" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="xmobileType" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="EC500"/>
                            <xs:enumeration value="DECT"/>
                            <xs:enumeration value="IPDECT"/>
                            <xs:enumeration value="PHS"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="mappingMode" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
```

```
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="termination"/>
                          <xs:enumeration value="origination"/>
                          <xs:enumeration value="both"/>
                          <xs:enumeration value="none"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="configurationSet" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="|[1-9]|[0-9][1-9]"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="mobilityTrunkGroup" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="aar|ars|[1-9]|[1-9][0-9]|[1-9]([0-9]){2}|
[1]([0-9]){3}|2000"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="dialPrefix" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="([0-9]*#){0,4}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="cellPhoneNumber" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]{0,15}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="musicSource" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:int">
                          <xs:minInclusive value="1" />
                          <xs:maxInclusive value="250" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="tests" type="xs:boolean" maxOccurs="1" minOccurs="0" />

                <xs:element name="dataModule" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!-- Controls the behavior of speakerphones. -->
                <xs:element name="speakerphone" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="none"/>
                          <xs:enumeration value="1-way"/>
                          <xs:enumeration value="2-way"/>
                        </xs:restriction>
                    </xs:simpleType>
```

```
                </xs:element>

                <!-- The language that displays on stations -->
                <!-- Time of day is displayed in 24-hour format (00:00 - 23:59) for all
languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59
p.m.). -->
                <!-- unicode: Displays English messages in a 24-hour format . If no
Unicode file is installed, displays messages in English by default. -->
                <xs:element name="displayLanguage" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="english"/>
                            <xs:enumeration value="french"/>
                            <xs:enumeration value="italian"/>
                            <xs:enumeration value="spanish"/>
                            <xs:enumeration value="unicode"/>
                            <xs:enumeration value="unicode2"/>
                            <xs:enumeration value="unicode3"/>
                            <xs:enumeration value="unicode4"/>
                            <xs:enumeration value="user-defined"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Defines the personalized ringing pattern for the station.
                    Personalized Ringing allows users of some telephones to have one of 8
ringing patterns for incoming calls.
                    For virtual stations, this field dictates the ringing pattern on its
mapped-to physical telephone.
                -->
                <!-- L = 530 Hz, M = 750 Hz, and H = 1060 Hz -->
                <!-- Valid Entries  Usage
                    1  MMM (standard ringing)
                    2  HHH
                    3  LLL
                    4  LHH
                    5  HHL
                    6  HLL
                    7  HLH
                    8  LHL
                 -->
                <xs:element name="personalizedRingingPattern" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:int">
                            <xs:minInclusive value="1" />
                            <xs:maxInclusive value="8" />
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <!-- The Message Lamp Extension associated with the current extension -->
                <xs:element name="messageLampExt" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]+([\.\-][0-9]+)*"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Enables or disables the mute button on the station. -->
                <xs:element name="muteButtonEnabled" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!--
```

```
                    When used with Multi-media Call Handling, indicates which extension is
                    assigned to the data module of the multimedia complex. Users can dial
                    this extension to place either a voice or a data call, and voice
                    conversion, coverage, and forwarding apply as if the call were made to
                    the 1-number.
                -->
                <!--
                    Valid Entry Usage A valid BRI data extension For MMCH, enter the
                    extension of the data module that is part of this multimedia complex.
                    H.323 station extension For 4600 series IP Telephones, enter the
                    corresponding H.323 station. For IP Softphone, enter the corresponding
                    H.323 station. If you enter a value in this field, you can register
                    this station for either a road-warrior or telecommuter/Avaya IP Agent
                    application. blank Leave this field blank for single-connect IP
                    applications.
                -->
                <xs:element name="mediaComplexExt" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="([1-9]{0})|[0-9]+([\.\-][0-9]+)*"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Whether this is IP soft phone. -->
                <xs:element name="ipSoftphone" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!--
                    Survivable GK Node Name Identifies the existence of other H.323
                    gatekeepers located within gateway products that offer survivable call
                    features. For example, the MultiTech MVPxxx-AV H.323 gateway family
                    and the SLS function within the H.248 gateways. When a valid IP node
                    name is entered into this field, Communication Manager adds the IP
                    address of this gateway to the bottom of the Alternate Gatekeeper List
                    for this IP network region. As H.323 IP stations register with
                    Communication Manager, this list is sent down in the registration
                    confirm message. This allows the IP station to use the IP address of
                    this Survivable Gatekeeper as the call controller of last resort to
                    register with. Available only if the station type is an H.323 station
                    (46xxor 96xx models).
                    Valid Entry             Usage
                    Valid IP node name         Any valid previously-administered IP node
name.
                    blank                     There are no external gatekeeper nodes
within a customer's network. This is the default value.
                -->
                <xs:element name="survivableGkNodeName" type="xs:string" maxOccurs="1"
minOccurs="0" />

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

                    Valid Entries         Usage
                    emergency             This station can only be used to place
emergency calls.
```

```
                    internal             This station can only make intra-switch calls.
This is the default.
                    local                 This station can only make calls that are
defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing
tables.
                    toll                 This station can place any national toll calls
that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing
tables.
                    unrestricted         This station can place a call to any number
defined in the Survivable Gateway Call Controller's routing tables. Those strings marked
as deny are also denied to these users.
                -->
                <xs:element name="survivableCOR" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="emergency"/>
                            <xs:enumeration value="internal"/>
                            <xs:enumeration value="local"/>
                            <xs:enumeration value="toll"/>
                            <xs:enumeration value="unrestricted"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

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

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

                -->
                <xs:element name="survivableTrunkDest" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!-- Enter the complete Voice Mail Dial Up number. -->
                <xs:element name="voiceMailNumber" maxOccurs="1" minOccurs="0" >

                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[(0-9)(*)(#)(~mwWps)]{0,24}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Analog telephones only. -->
                <!--
                Valid entries         Usage
                        true         Enter true if this telephone is not located in the
same building with the system. If you enter true, you must complete R Balance Network.
                        false         Enter false if the telephone is located in the same
building with the system.
                 -->
                <xs:element name="offPremisesStation" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
```

```
                <!-- If a second line on the telephone is administered on the I-2
channel, enter analog. Otherwise, enter data module if applicable or none. -->
                <xs:element name="dataOption" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="analog"/>
                            <xs:enumeration value="data-module"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <xs:element name="displayModule" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!-- if led or neon then messageLampExt should be enable otherwise its
blank -->
                <xs:element name="messageWaitingIndicator" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="led"/>
                            <xs:enumeration value="neon"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Enter true to use this station as an endpoint in a remote office
configuration. -->
                <xs:element name="remoteOfficePhone" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!-- Defines the source for Leave Word Calling (LWC) messages. -->
                <!--
                Valid entries             Usage
                    audix                 If LWC is attempted, the messages are stored in
AUDIX.
                    spe                  If LWC is attempted, the messages are stored in
the system processing element (spe).
                    none                  If LWC is attempted, the messages are not stored.

                 -->
                <xs:element name="lwcReception" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="audix"/>
                            <xs:enumeration value="msa"/>
                            <xs:enumeration value="spe"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!--
                    Enter true to allow internal telephone users to leave short LWC
messages
                    for this extension. If the system has hospitality, enter true for
                    guest-room telephones if the extension designated to receive failed
                    wakeup messages should receive LWC messages that indicate the wakeup
                    calls failed. Enter true if LWC Reception is audix.
                -->
                <xs:element name="lwcActivation" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
```

```
                <xs:element name="lwcLogExternalCalls" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="cdrPrivacy" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="redirectNotification" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="perButtonRingControl" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="bridgedCallAlerting" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="bridgedIdleLinePreference" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="confTransOnPrimaryAppearance" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="customizableLabels" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="expansionModule" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="ipVideoSoftphone" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="activeStationRinging" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="single"/>
                            <xs:enumeration value="continuous"/>
                            <xs:enumeration value="if-busy-single"/>
                            <xs:enumeration value="silent"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Defines how call rings to the telephone when it is on-hook.-->
                <!--
                    Valid entries             Usage
                    continuous                 Enter continuous to cause all calls to
this telephone to ring continuously.
                    if-busy-single             Enter if-busy-single to cause calls to
this telephone to ring continuously when the telephone is off-hook and idle and calls to
this telephone to
                                              receive one ring cycle and then ring silently
when the telephone is off-hook and active.
                    silent-if-busy             Enter silent-if-busy to cause calls to
ring silently when this station is busy.
                    single                     Enter single to cause calls to this
telephone to receive one ring cycle and then ring silently.
                -->
                <xs:element name="idleActiveRinging" type="xs:string" maxOccurs="1"
minOccurs="0" /> <!-- not found in xhtml -->

                <!-- Must be set to true when the Type field is set to H.323. -->
                <xs:element name="switchhookFlash" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!-- If this field is true, the short switch-hook flash (50 to 150) from
a 2500-type set is ignored. -->
                <xs:element name="ignoreRotaryDigits" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!--
                    H.320 Conversion - Valid entries are true and false (default). This
field is
                    optional for non-multimedia complex voice stations and for Basic
                    multimedia complex voice stations. It is mandatory for Enhanced
                    multimedia complex voice stations. Because the system can only handle
```

```
                    a limited number of conversion calls, you might need to limit the
                    number of telephones with H.320 conversion. Enhanced multimedia
                    complexes must have this flag set to true.
                -->
                            <xs:element name="h320Conversion" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!--
                    The service link is the combined hardware and software multimedia
                    connection between an Enhanced mode complex's H.320 DVC system and the
                    Avaya DEFINITY Server which terminates the H.320 protocol. A service
                    link is never used by a Basic mode complex H.320 DVC system.
                    Connecting a service link will take several seconds. When the service
                    link is connected, it uses MMI, VC and system timeslot resources. When
                    the service link is disconnected it does not tie up any resources.
                    The
                    Service Link Mode can be administered as either 'as-needed' or
                    'permanent' as described below: - As-Needed - Most non-call center
                    multimedia users will be administered with this service link mode. The
                    as-needed mode provides the Enhanced multimedia complex with a
                    connected service link whenever a multimedia call is answered by the
                    station and for a period of 10 seconds after the last multimedia call
                    on the station has been disconnected. Having the service link stay
                    connected for 10 seconds allows a user to disconnect a multimedia call
                    and then make another multimedia call without having to wait for the
                    service link to disconnect and re-establish. - Permanent - Multimedia
                    call center agents and other users who are constantly making or
                    receiving multimedia calls might want to be administered with this
                    service link mode. The permanent mode service link will be connected
                    during the station's first multimedia call and will remain in a
                    connected state until the user disconnects from their PC's multimedia
                    application or the Avaya DEFINITY Server restarts. This provides a
                    multimedia user with a much quicker video cut-through when answering a
                    multimedia call from another permanent mode station or a multimedia
call that has been early answered. ● Multimedia Mode - There are two
                    multimedia modes, Basic and Enhanced, as
                -->
                <xs:element name="serviceLinkMode" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="as-needed"/>
                            <xs:enumeration value="permanent"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!--
                    There are two multimedia modes, Basic and Enhanced, as described
                    below:
                    Basic - A Basic multimedia complex consists of a
                    BRI-connected multimedia-equipped PC and a non-BRI-connected
                    multifunction telephone set. When in Basic mode, users place voice
                    calls at the multifunction telephone and multimedia calls from the
                    multimedia equipped PC. Voice calls will be answered at the
                    multifunction telephone and multimedia calls will alert first at the
                    PC and if unanswered will next alert at the voice station if it is
                    administered with H.320 enabled. A Basic mode complex has limited
                    multimedia feature capability.
                    Enhanced - An Enhanced multimedia complex consists of a
                    BRI-connected multimedia-equipped PC and a non-BRI-connected
                    multifunction telephone. The Enhanced mode station acts as though the
                    PC were directly connected to the multifunction telephone; the service
                    link provides the actual connection between the Avaya DEFINITY Server
                    and the PC. Thus, voice and multimedia calls are originated and
                    received at the telephone set. Voice and multimedia call status are
```

```
                    also displayed at the telephone set. An Enhanced mode station allows
                    multimedia calls to take full advantage of most call control features
                -->
                <xs:element name="multimediaMode" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="basic"/>
                            <xs:enumeration value="enhanced"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Controls the auditing or interrogation of a served user's message
waiting indicator (MWI).
                Valid entries             Usage
                    fp-mwi                 Use if the station is a served user of an fp-
mwi message center.
                    qsig-mwi              Use if the station is a served user of a qsig-
mwi message center.
                    blank                  Leave blank if you do not want to audit the
served user's MWI or
                                          if the user is not a served user of either an fp-
mwi or qsig-mwi message center.
                 -->
                <xs:element name="mwiServedUserType" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="fp-mwi"/>
                            <xs:enumeration value="qsig-mwi"/>
                            <xs:enumeration value="sip-adjunct"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- The AUDIX associated with the station.
                    Must contain a user-defined adjunct name that was previously
administered.
                -->
                          <xs:element name="audixName" type="xs:string" maxOccurs="1"
minOccurs="0" />

                <!--
                    Automatic Moves allows a DCP telephone to be unplugged from one
                    location and moved to a new location without additional Communication
                    Manager administration. Communication Manager automatically associates
                    the extension to the new port.

                    **********CAUTION**********
                    When a DCP telephone is unplugged and
                    moved to another physical location, the Emergency Location Extension
                    field must be changed for that extension or the USA Automatic Location
                    Identification data base must be manually updated. If the Emergency
                    Location Extension field is not changed or if the USA Automatic
                    Location Identification data base is not updated, the DID number sent
                    to the Public Safety Network could send emergency response personnel
                    to the wrong location.
                Valid entries             Usage
                    always              Enter always and the DCP telephone can be moved
anytime without
                                        additional administration by unplugging from one
location and plugging
                                        into a new location.
                    once                Enter once and the DCP telephone can be unplugged
and plugged into a
                                        new location once. After a move, the field is set to
```

```
done the next time that
                                routine maintenance runs on the DCP telephone.
                                Use once when moving a large number of DCP telephones
so each
                                extension is removed from the move list. Use once to
prevent automatic
                                maintenance replacement.
                    no             Enter no to require administration in order to
move the DCP telephone.
                    done           Done is a display-only value. Communication Manager
sets the field to
                                done after the telephone is moved and routine
maintenance runs on the
                                DCP telephone.
                    error          Error is a display-only value. Communication
Manager sets the field to
                                error, after routine maintenance runs on the DCP
telephone, when a
                                non-serialized telephone is set as a movable
telephone.
                -->
                <xs:element name="automaticMoves" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="always"/>
                            <xs:enumeration value="no"/>
                            <xs:enumeration value="once"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>


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

                    Valid entries                Usage
                    as-on-local                Type as-on-local to achieve the following
results:
                                           If the administrator chooses to leave the
Emergency Location
                                           Extension fields (that correspond to this
station's IP address) on
                                           the IP Address Mapping screen blank, the
value as-on-local
                                           sends the extension entered in the Emergency
Location
                                           Extension field in the Station screen to the
Public Safety
```

Mapping screen with functions as follows:	Answering Point (PSAP). If the administrator populates the IP Address
in the Station screen Extension field in the local sends the Point (PSAP).	emergency numbers, the value as-on-local - If the Emergency Location Extension field is the same as the Emergency Location IP Address Mapping screen, the value as-on-extension to the Public Safety Answering
in the Station screen Extension field in the local sends the the Public Safety	- If the Emergency Location Extension field is different from the Emergency Location IP Address Mapping screen, the value as-on-extension in the IP Address Mapping screen to Answering Point (PSAP).
block emergency calls. Use this entry	Enter block to prevent the completion of for users who move around but always have a
circuit-switched telephone from the Avaya S8XXX Server 911 Tandem office.	nearby, and for users who are farther away than an adjacent area code served by the same
from an IP Telephone and nearby circuit-switched	When users attempt to dial an emergency call the call is blocked, they can dial 911 from a telephone instead.
cesid to send the CESID	Enter cesid to allow Communication Manager information supplied by the IP Softphone to
the PSAP. The end user Softphone.	enters the emergency information into the IP Use this entry for IP Softphones with road
warrior service that are near emergency call routed over	enough to the Avaya S8XXX Server that an 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 a local direct-dial number	telephone number, provided that the number is with the local area code, at the physical
location of the IP Softphone. If the the end user enters a	server uses CAMA trunks for emergency calls, specific digit string for each IP Softphone
location, based on advice from	the local emergency response personnel.
option the option (extension, block, or	Enter option to allow the user to select cesid) that the user selected during
registration and the IP Softphone	

Comments on this document? infodev@avaya.com

```
                                        reported. Use this entry for extensions that
can be swapped back and
                                        forth between IP Softphones and a telephone
with a fixed location.
                                        The user chooses between block and cesid on
the softphone. A DCP or
                                        IP telephone in the office automatically
selects extension.
                -->
                <xs:element name="remoteSoftphoneEmergencyCalls" maxOccurs="1"
minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="as-on-local"/>
                            <xs:enumeration value="block"/>
                            <xs:enumeration value="cesid"/>
                            <xs:enumeration value="option"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <!--
                    This field allows the system to properly identify the location of a
                    caller who dials a 911 emergency call from this station. An entry in
                    this field must be of an extension type included in the dial plan, but
                    does not have to be an extension on the local system. It can be a UDP
                    extension. The entry defaults to blank. A blank entry typically would
                    be used for an IP softphone dialing in through PPP from somewhere
                    outside your network. If you populate the IP Address Mapping screen
                    with emergency numbers, the feature functions as follows: If the
                    Emergency Location Extension field in the Station screen is the same
                    as the Emergency Location Extension field in the IP Address Mapping
                    screen, the feature sends the extension to the Public Safety Answering
                    Point (PSAP). If the Emergency Location Extension field in the Station
                    screen is different from the Emergency Location Extension field in the
                    IP Address Mapping screen, the feature sends the extension in the IP
                    Address Mapping screen to the Public Safety Answering Point (PSAP).
                -->
                <xs:element name="emergencyLocationExt" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]+([\.\-][0-9]+)*"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!--
                    A softphone can register no matter what emergency call handling
settings
                    the user has entered into the softphone. If a softphone dials 911, the
                    administered Emergency Location Extension is used. The softphone's
                    user-entered settings are ignored. If an IP telephone dials 911, the
                    administered Emergency Location Extension is used. If a call center
                    agent dials 911, the physical station extension is displayed,
                    overriding the administered LoginID for ISDN Display . Does not apply
                    to SCCAN wireless telephones, or to extensions administered as type
                    h.323.
                -->
                <xs:element name="alwaysUse" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!-- Activates or deactivates Precedence Call Waiting for this station -->
                <xs:element name="precedenceCallWaiting" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
```

```
                <!--
                    Enables or disables automatic selection of any idle appearance for
                    transferred or conferenced calls. Communication Manager first attempts
                    to find an idle appearance that has the same extension number as the
                    call being transferred or conferenced has. If that attempt fails,
                    Communication Manager selects the first idle appearance.
                -->
                            <xs:element name="autoSelectAnyIdleAppearance"
type="xs:boolean" maxOccurs="1" minOccurs="0" />

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

                <xs:element name="coverageMsgRetrieval" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <!--
                    In EAS environments, the auto answer setting for the Agent LoginID can
                    override a station's setting when an agent logs in.
                    Valid Entry            Usage
                    all                 All ACD and non-ACD calls terminated to an idle
station cut through immediately.
                                        Does not allow automatic hands-free answer for
intercom calls. With non-ACD calls,
                                        the set is also rung while the call is cut
through. The ring can be prevented by activating
                                        the ringer-off feature button when the Allow
Ringer-off with Auto-Answer is enabled for the system.
                    acd                 Only ACD split /skill calls and direct agent
calls to auto answer. Non-ACD calls terminated to a station ring audibly.
                                        For analog stations, the station is off-hook and
idle, only the ACD split/skill calls and direct agent calls
                                        auto answer; non-ACD calls receive busy
treatment. If the station is active on an ACD call and
                                        a non-ACD call arrives, the Agent receives call-
waiting tone.
                    none                 All calls terminated to this station receive an
audible ringing treatment.
                    icom                 Allows a telephone user to answer an intercom
call from the same intercom group without pressing the intercom
button.
                -->
                <xs:element name="autoAnswer" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="acd"/>
                            <xs:enumeration value="all"/>
                            <xs:enumeration value="icom"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!--
                    Enables or disables data restriction that is used to prevent tones,
such as call-waiting tones, from interrupting data calls.
                    Data restriction provides permanent protection and cannot be changed
by the telephone user. Cannot be assigned if Auto Answer
                    is administered as all or acd. If enabled, whisper page to this
station is denied.
                 -->
                <xs:element name="dataRestriction" type="xs:boolean" maxOccurs="1"
```

```
minOccurs="0" />

                <!--
                    Indicates which call appearance is selected when the user lifts the
handset and there is an incoming call.
                    Valid Entry                 Usage
                    true                       The user connects to an idle call
appearance instead of the ringing call.
                    false                       The Alerting Appearance Preference is
set and the user connects to the ringing call appearance.
                 -->
                <xs:element name="idleAppearancePreference" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!--
                    enable/disable call waiting for this station
                -->
                <xs:element name="callWaitingIndication" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!--
                     Attendant call waiting allows attendant-originated or attendant-
extended calls to a busy
                     single-line telephone to wait and sends distinctive call-waiting
tone to the single-line user.
                     Enable/disable attendant call waiting
                 -->
                <xs:element name="attCallWaitingIndication" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!--
                    Enter true so the telephone can receive the 3 different types of
ringing patterns which identify the type of incoming calls.
                     Distinctive ringing might not work properly for off-premises
telephones. -->
                <xs:element name="distinctiveAudibleAlert" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!--
                    Valid Entries             Usage
                    true                     Restricts the last idle call appearance used
for incoming priority calls and outgoing call originations only.
                    false                     Last idle call appearance is used for
incoming priority calls and outgoing call originations.
                 -->
                <xs:element name="restrictLastAppearance" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!--
                    Valid entries            Usage
                    true                     Analog disconnect signal is sent
automatically to the port after a call terminates. Analog devices
                                             (such as answering machines and
speakerphones) use this signal to turn the devices off after a call terminates.
                    false                     Hunt group agents are alerted to incoming
calls. In a hunt group environment, the disconnect
                                             signal blocks the reception of zip tone and
incoming call notification by an auto-answer station when a call
                                             is queued for the station.
                 -->
                <xs:element name="adjunctSupervision" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!--
                        Send Calling Number.
```

```
                        Valid Entries         Usage
                        y                     All outgoing calls from the station will
deliver the Calling Party Number
                                             (CPN) information as "Presentation Allowed."
                        n                     No CPN information is sent for the call
                        r                     Outgoing non-DCS network calls from the
station will deliver the Calling
                                             Party Number information as "Presentation
Restricted."
                 -->
                <xs:element name="perStationCpnSendCallingNumber" maxOccurs="1"
minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="r"/>
                            <xs:enumeration value="n"/>
                            <xs:enumeration value="y"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!--
                    Appears on the Station screen for analog telephones, only if the
Without Flash field in the
                    ANALOG BUSY AUTO CALLBACK section of the Feature-Related System
Parameters
                    screen is set to true. The Busy Auto Callback without Flash field
then defaults to true for all analog
                    telephones that allow Analog Automatic Callback.
                    Set true to provide automatic callback for a calling analog station
without flashing the hook.
                 -->
                <xs:element name="busyAutoCallbackWithoutFlash" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!-- Provides audible message waiting. -->
                <xs:element name="audibleMessageWaiting" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!-- Provides extended local calls / imsFeatureSequencing
                Extended Local Calls (ELC) /imsFeatureSequencing allows DCP and H.323
stations to use SIP sequenced applications.  The feature works by routing calls
                involving those stations over SIP IMS trunks.  In other words, CM is
applying the half-call model to those stations.
                That also has the side effect that features which work differently under
the half-call model than under the usual (full-call) model
                also work differently for ELC stations.
                The Extended Local Calls feature is administrable per station.  We're
allowing stations that always use SIP IMS trunks to coexist on
                the same server with stations that dont always use SIP IMS trunks.  In
other words, ELC is changing a previous marketing rule that
                the full-call model (CM-ES) and the half-call model (CM-FS) functions
can't co-exist on the same server.  As noted above, that also
                has the side effect that features which work differently under the half-
call model than under the full-call model now also can work
                differently for two different SIP stations on the same CM
server.
                 -->
                <xs:element name="imsFeatureSequencing" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <!--
                    Only administrable if Hospitality is enabled on the System Parameters
                    Customer-Options (Optional Features) screen. This field affects the
                    telephone display on calls that originated from a station with Client
```

```
                    Room Class of Service. Note: For stations with an audix station
                    type, AUDIX Voice Power ports, or ports for any other type of
                    messaging that needs display information, Display Client Redirection
                    must be enabled.
                    Set true to redirect information for a call originating from a Client
Room and terminating to this station displays.
                -->
                <xs:element name="displayClientRedirection" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!--
                    Valid Entries         Usage
                        true            Indicates that a station's line selection is not
to be moved from the currently selected line button
                                        to a different, non-alerting line button. If you
enter true, the line selection on an on-hook station only moves from the last
                                        used line button to a line button with an audibly
alerting call. If there are no alerting calls, the line selection
                                        remains on the button last used for a call.
                        false            The line selection on an on-hook station with no
alerting calls can be moved to a different line button, which might be serving a different
                                        extension.
                 -->
                <xs:element name="selectLastUsedAppearance" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!-- Whether an unanswered forwarded call is provided coverage treatment.
-->
                <xs:element name="coverageAfterForwarding" type="xs:string" maxOccurs="1"
minOccurs="0" />

                <!-- Allow/disallow direct audio connections between IP endpoints. -->
                <xs:element name="directIpIpAudioConnections" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <!-- Allows IP endpoints to be connected through the server's IP circuit
pack. -->
                <xs:element name="ipAudioHairpinning" type="xs:boolean" maxOccurs="1"
minOccurs="0" />


                <xs:element name="primeAppearancePreference" type="xs:string"
maxOccurs="1" minOccurs="0" />

                <!-- Elements with complex data type. Please refer the appropriate
elements for more details. -->
                <xs:element name="stationSiteData" type="csm:xmlStationSiteData"
maxOccurs="1" minOccurs="0" />
                <xs:element name="abbrList" type="csm:xmlStationAbbreviatedDialingData"
maxOccurs="unbounded" minOccurs="0" />
                <xs:element name="buttons" type="csm:xmlButtonData" maxOccurs="24"
minOccurs="0" />
                <xs:element name="featureButtons" type="csm:xmlButtonData" maxOccurs="24"
minOccurs="0" />
                <xs:element name="expansionModuleButtons" type="csm:xmlButtonData"
maxOccurs="72" minOccurs="0" />
                <xs:element name="softKeys" type="csm:xmlButtonData" maxOccurs="15"
minOccurs="0" />
                <xs:element name="displayButtons" type="csm:xmlButtonData"
maxOccurs="unbounded" minOccurs="0" />
                <xs:element name="stationDataModule" type="csm:xmlStationDataModule"
maxOccurs="1" minOccurs="0" />
                <xs:element name="hotLineData" type="csm:xmlStationHotLineData"
maxOccurs="1" minOccurs="0" />
                <xs:element  name="nativeName" type="csm:xmlNativeNameData" maxOccurs="1"
```

```
minOccurs="0"/>

                <!-- Number of button modules 0-3-->
                <xs:element name="buttonModules" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:int">
                            <xs:minInclusive value="0" />
                            <xs:maxInclusive value="3" />
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <xs:element name="unconditionalInternalDest" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}[#]|[*]
[0-9]{1,17}|[0-9]{1,18}|[*][#]|"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <xs:element name="unconditionalInternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <xs:element name="unconditionalExternalDest" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}[#]|[*]
[0-9]{1,17}|[0-9]{1,18}|[*][#]|"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <xs:element name="unconditionalExternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <xs:element name="busyInternalDest" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}[#]|[*]
[0-9]{1,17}|[0-9]{1,18}|[*][#]|"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="busyInternalActive" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="busyExternalDest" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}[#]|[*]
[0-9]{1,17}|[0-9]{1,18}|[*][#]|"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="busyExternalActive" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="noReplyInternalDest" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
```

```
                        <xs:restriction base="xs:string">
                          <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}[#]|[*]
[0-9]{1,17}|[0-9]{1,18}|[*][#]|"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="noReplyInternalActive" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="noReplyExternalDest" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:pattern value="[*][0-9]{1,16}[#]|[0123456789]{1,17}[#]|[*]
[0-9]{1,17}|[0-9]{1,18}|[*][#]|"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="noReplyExternalActive" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="sacCfOverride" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="a"/>
                          <xs:enumeration value="n"/>
                          <xs:enumeration value="y"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="lossGroup" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:int">
                          <xs:minInclusive value="1" />
                          <xs:maxInclusive value="19" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="timeOfDayLockTable" maxOccurs="1"
minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[1-5]|[0-9]{0}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="emuLoginAllowed" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="ec500State" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="enabled"/>
                          <xs:enumeration value="disabled"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- true/false to enable/disable Mute on Off Hook in Shared Control Mode
feature. -->
                <xs:element name="muteOnOffHookInSCMode" type="xs:boolean" maxOccurs="1"
```

```
minOccurs="0" />

                <xs:element name="type3pccEnabled" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="None"/>
                            <xs:enumeration value="Avaya"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="sipTrunk" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="aar|ars|[1-9]|[1-9][0-9]|[1-9]([0-9]){2}|
[1]([0-9]){3}|2000"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="multimediaEarlyAnswer" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="bridgedApprOrigRestr" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="callApprDispFormat" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="inter-location"/>
                            <xs:enumeration value="intra-location"/>
                            <xs:enumeration value="disp-param-default"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Enter a Group ID between 0-999, or blank -->
                <xs:element name="ipPhoneGroupId" maxOccurs="1" minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]|[0-9][0-9]|[0-9][0-9][0-9]|[0-9]
{0}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="xoipEndPointType" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="auto"/>
                            <xs:enumeration value="fax"/>
                            <xs:enumeration value="modem"/>
                            <xs:enumeration value="tty"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="xid" type="xs:boolean" maxOccurs="1" minOccurs="0" />
                <xs:element name="stepClearing" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="fixedTei" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="tei" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
```

```
                            <xs:pattern value="[0-6][0-3]"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="countryProtocol" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="1"/>
                          <xs:enumeration value="2"/>
                          <xs:enumeration value="3"/>
                          <xs:enumeration value="6"/>
                          <xs:enumeration value="etsi"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="endptInit" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

                <xs:element name="spid" maxOccurs="1" minOccurs="0"  >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]{1,10}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>


                <xs:element name="endptId" maxOccurs="1" minOccurs="0" > <!-- 00 to 62 -->
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:pattern value="[0-6][0-2]"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="isMCTSignalling" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="isShortCallingPartyDisplay" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="passageWay" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="dtmfOverIp" maxOccurs="1" minOccurs="0" >
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="in-band"/>
                          <xs:enumeration value="in-band-g711"/>
                          <xs:enumeration value="out-of-band"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
                <xs:element name="location" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[1-9]{0}|[1-9]|[1-9][0-9]|[1-9]([0-9]){2}|
[1]([0-9]){3}|2000"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

```
<xs:complexType name="xmlStationSiteData">
    <xs:sequence>
        <xs:element name="room" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:maxLength value="10"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="jack" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:maxLength value="5"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="cable" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:maxLength value="5"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="floor" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="building" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="headset" type="xs:boolean" maxOccurs="1" minOccurs="0" />
        <xs:element name="speaker" type="xs:boolean" maxOccurs="1" minOccurs="0" />

        <xs:element name="mounting" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="d"/>
                    <xs:enumeration value="w"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- Enter numeric cord length (0-99) -->
        <xs:element name="cordLength" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:int">
                    <xs:minInclusive value="0" />
                    <xs:maxInclusive value="99" />
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="setColor" type="xs:string" maxOccurs="1" minOccurs="0" />
    </xs:sequence>
</xs:complexType>


<xs:complexType name="xmlStationAbbreviatedDialingData">
    <xs:sequence>
        <xs:element name="listType" maxOccurs="1" minOccurs="1" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="enhanced"/>
                    <xs:enumeration value="group"/>
                    <xs:enumeration value="personal"/>
                    <xs:enumeration value="system"/>
                  </xs:restriction>
```

```
            </xs:simpleType>
        </xs:element>

        <xs:element name="number" type="xs:int" maxOccurs="1" minOccurs="1" />
        <xs:element name="listId" type="xs:int" maxOccurs="1" minOccurs="0" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlButtonData">
    <xs:sequence>
        <xs:element name="number" type="xs:int" maxOccurs="1" minOccurs="1" /><!--
*******Must present******  -->
        <xs:element name="type" type="xs:string" maxOccurs="1" minOccurs="1" /><!--
*******Must present******  -->
        <xs:element name="data1" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="data2" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="data3" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="data4" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="data5" type="xs:string" maxOccurs="1" minOccurs="0" />
        <xs:element name="data6" type="xs:string" maxOccurs="1" minOccurs="0" />
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlStationDataModule">
    <xs:sequence>
        <xs:element name="dataExtension" maxOccurs="1" minOccurs="1" ><!--  *******Must
present******  -->
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="[0-9]+([.-][0-9]+)*"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="name" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:maxLength value="29"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="cor" maxOccurs="1" minOccurs="1" ><!--  *******Must
present******  -->
            <xs:simpleType>
                  <xs:restriction base="xs:int">
                    <xs:minInclusive value="0" />
                    <xs:maxInclusive value="995" />
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="cos" maxOccurs="1" minOccurs="1" ><!--  *******Must
present******  -->
            <xs:simpleType>
                  <xs:restriction base="xs:int">
                    <xs:minInclusive value="0" />
                    <xs:maxInclusive value="15" />
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="itc" maxOccurs="1" minOccurs="1" ><!--  *******Must
present******  -->
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="restricted"/>
                    <xs:enumeration value="unrestricted"/>
```

```
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <!-- CM dependant field - 100 or 250 depends on system params -->
        <xs:element name="tn" maxOccurs="1" minOccurs="1" ><!--  *******Must
present******  -->
            <xs:simpleType>
                <xs:restriction base="xs:int">
                  <xs:minInclusive value="1" />
                  <xs:maxInclusive value="250" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="listType" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="enhanced"/>
                  <xs:enumeration value="group"/>
                  <xs:enumeration value="personal"/>
                  <xs:enumeration value="system"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="listId" type="xs:int" maxOccurs="1" minOccurs="0" />

        <xs:element name="specialDialingOption" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="default"/>
                  <xs:enumeration value="hot-line"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="specialDialingAbbrDialCode" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:maxLength value="4"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlStationHotLineData">
    <xs:sequence>
        <xs:element name="hotLineDestAbbrevList" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                <xs:restriction base="xs:int">
                  <xs:minInclusive value="1" />
                  <xs:maxInclusive value="3" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="hotLineAbbrevDialCode" maxOccurs="1" minOccurs="0" >
                  <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:pattern value="[0-9]*"/>
                        </xs:restriction>
                  </xs:simpleType>
              </xs:element>
    </xs:sequence>
</xs:complexType>

<!-- If displayName,givenName or surname contains characters of multiple scripts then
locale tag should be present.
```

```
       If displayName tag is present then it overwrites native name.
       If displayname is not present then combination of givenName and surname gets
copied in native name.
       Please find below locale for multiscript language
       Language               Locale
       Japanese                       ja, ja-jp
       Simplified Chinese          zh-cn
       Traditional Chinese     zh-tw -->
<xs:complexType name="xmlNativeNameData">
    <xs:sequence>
        <xs:element name="locale" maxOccurs="1" minOccurs="0">
           <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="ja-jp"/>
                    <xs:enumeration value="ja"/>
                    <xs:enumeration value="zh-cn"/>
                    <xs:enumeration value="zh-tw"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="name" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:maxLength value="27"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:sequence>
</xs:complexType>

</xs:schema>
```

Sample XML for bulk import of Collaboration Environment profiles

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:ns2="http://xml.avaya.com/schema/import_ce" xmlns:ns3="http://
xml.avaya.com/schema/import_csm_b5800" xmlns:ns4="http://xml.avaya.com/schema/import1"
xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ns6="http://xml.avaya.com/schema/
import_mmcs" xmlns:ns7="http://xml.avaya.com/schema/import_sessionmanager"
xmlns:ns8="http://xml.avaya.com/schema/mock" xmlns:ns9="http://xml.avaya.com/schema/
import_csm_mm" xmlns:ns10="http://xml.avaya.com/schema/import_csm_cm" xmlns:ns11="http://
xml.avaya.com/schema/import_csm_agent" xmlns:ns12="http://xml.avaya.com/schema/
deltaImport" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
    <tns:user>
        <authenticationType>basic</authenticationType>
        <description></description>
        <displayName>saurabh, tyagi</displayName>
        <displayNameAscii>saurabh, tyagi</displayNameAscii>
        <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>tyagi</givenName>
        <givenNameAscii>tyagi</givenNameAscii>
        <honorific></honorific>
        <loginName>saurabhtyagi@avaya.com</loginName>
        <employeeNo></employeeNo>
        <department></department>
        <organization></organization>
        <middleName></middleName>
        <preferredLanguage>hu</preferredLanguage>
        <source>local</source>
        <status>provisioned</status>
        <surname>saurabh</surname>
        <surnameAscii>saurabh</surnameAscii>
```

```
        <userName>saurabhtyagi</userName>
        <userPassword></userPassword>
        <roles>
            <role>End-User</role>
        </roles>
        <ownedContactLists>
            <contactList>
                <name>list-saurabhtyagi_avaya.com</name>
                <isPublic>false</isPublic>
                <contactListType>general</contactListType>
            </contactList>
        </ownedContactLists>
        <commProfileSet>
            <commProfileSetName>Primary</commProfileSetName>
            <isPrimary>true</isPrimary>
            <commProfileList>
                <commProfile xsi:type="ns2:CeCommProfXML" xmlns:ns2="http://xml.avaya.com/
schema/import_ce">
                    <commProfileType>AUS</commProfileType>
                    <ns2:serviceProfile>ce_service_profile</ns2:serviceProfile>
                </commProfile>
            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema Definition for bulk import of Collaboration Environment 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 Collaboration Environment 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 messaging profiles

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:one="http://xml.avaya.com/schema/import" elementFormDefault="qualified"
    targetNamespace="http://xml.avaya.com/schema/import_csm_mm" xmlns:csm="http://
xml.avaya.com/schema/import_csm_mm">

    <xs:import namespace="http://xml.avaya.com/schema/import"
        schemaLocation="userimport.xsd" />
    <!--Changes in xsd file need to generate jaxb src using this xsd-->
    <xs:complexType name="xmlMessagingProfile">
        <xs:complexContent>
            <xs:extension base="one:xmlCommProfileType">
                <xs:sequence>
                    <!--
                        Specifies the messaging system of the subscriber you
                        want to add. Name as it appears under
                        'Applications/Application Management/Entities
                    -->
                    <xs:element name="messagingName" type="xs:string"
                        maxOccurs="1" minOccurs="1" />
                    <xs:element name="useExisting" type="xs:boolean"
                        maxOccurs="1" minOccurs="0" /><!-- use existing -->

                    <!-- Specifies the messaging template of a subscriber.  -->
```

```
                    <xs:element name="messagingTemplate" type="xs:string"
                        maxOccurs="1" minOccurs="0" />


                    <xs:element name="mailboxNumber" maxOccurs="1"
                        minOccurs="1">
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern value="[0-9]{1,50}" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>

                    <!--
                        Specifies the default password the subscriber must use
                        to log in to his or her mailbox. The password can be
                        from one digit in length to a maximum of 15 digits.
                    -->
                    <xs:element name="password" maxOccurs="1" minOccurs="0">
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern value="[0-9]{0,15}" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>
                    <xs:element name="deleteOnUnassign" type="xs:boolean"
                        maxOccurs="1" minOccurs="0" />

                    <!-- follows overrriding  subscriber  data  -->

                    <!--
                        The class of service for this subscriber. The COS controls
                        subscriber access to many features and provides general
                        settings, such as mailbox size.
                    -->
                    <xs:element name="cos" maxOccurs="1" minOccurs="0">
                    <!-- MM/CMM field -->
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern
                                    value="[0-9]|[0-9]{2}|[0-4][0-9]{2}|[5][0-4][0-9]|[5]
[5][0-1]" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>

                    <!--
                        Specifies the default community ID for the subscriber.
                        Community IDs are used to control message sending and
                        receiving among groups of subscribers.
                        The default value is 1.
                    -->
                    <xs:element name="communityID" maxOccurs="1" minOccurs="0">
                    <!-- MM/CMM field -->
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern value="[0-9]|[0-1][0-5]" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>

                    <!--
                        Specifies the name that appears before the machine name
                        and domain in the subscriber's e-mail address. The machine
                        name and domain are automatically added to the handle you
```

```
                    enter when the subscriber sends or receives an e-mail.
                -->
                <xs:element name="emailHandle" maxOccurs="1" minOccurs="0">
                <!-- MM/CMM field -->
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="^[a-zA-Z0-9\w\.\-]*" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!--
                    Specifies the display name of the subscriber in address book
                    listings, such as those for e-mail client applications.
                    The name you enter can be 1 to 64 characters in length.
                -->
                <xs:element name="commonName" type="xs:string"
                    maxOccurs="1" minOccurs="0" /> <!-- MM/CMM field -->

                <!--
                    Specifies one or more alternate number to reach a
                    subscriber. You can use secondary extensions to specify
                    a telephone number for direct reception of faxes, to
                    allow callers to use an existing Caller Application, or
                    to identify each line appearance on the subscriber's
                    telephone set if they have different telephone numbers.
                -->
                <xs:element name="secondaryExtension" maxOccurs="1"
                    minOccurs="0"> <!-- MM/CMM field -->
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]{0,50}" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="mmSpecific" type="csm:xmlMMSpecific"
                    maxOccurs="1" minOccurs="0" />
                <xs:element name="cmmSpecific" type="csm:xmlCMMSpecific"
                    maxOccurs="1" minOccurs="0" />
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>


<xs:complexType name="xmlMMSpecific">
    <xs:sequence>
        <!--
            Specifies a unique address in the voice mail network. The numeric
            address can be from 1 to 50 digits and can contain the Mailbox
            Number.
        -->
        <xs:element name="numericAddress" maxOccurs="1" minOccurs="0">
        <!-- MM field -->
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:pattern value="([0-9])*" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!-- The primary telephone extension of the subscriber. -->
        <xs:element name="pbxExtension" maxOccurs="1" minOccurs="0">
        <!-- MM field -->
```

```
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:pattern value="([+0-9])*" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!--
            The telephone number of the subscriber as displayed in address book
            listings and client applications. The entry can be a maximum of 50
            characters in length and can contain any combination of digits
            (0-9), period (.), hyphen (-), plus sign (+), and left and right
            parentheses ([) and (]).
        -->
        <xs:element name="telephoneNumber" maxOccurs="1"
            minOccurs="0"> <!-- MM field -->
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:pattern value="([-+\.()0-9])*" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!--
            If the subscriber name is entered in multi-byte character format,
            then this field specifies the ASCII translation of the subscriber
            name.
        -->
        <xs:element name="asciiVersionOfName" type="xs:string"
            maxOccurs="1" minOccurs="0" /> <!-- MM field -->

        <!--
            Specifies whether your password expires or not. You can choose one
            of the following: - yes: for password to expire - no: if you do not
            want your password to expire
        -->
        <xs:element name="expirePassword" type="csm:xmlyesNoType"
            maxOccurs="1" minOccurs="0" />  <!-- MM field -->

        <!--
            Specifies whether you want your mailbox to be locked. A subscriber
            mailbox can become locked after two unsuccessful login attempts.You
            can choose one of the following: - no: to unlock your mailbox - yes:
            to lock your mailbox and prevent access to it
        -->
        <xs:element name="mailBoxLocked" type="csm:xmlyesNoType"
            maxOccurs="1" minOccurs="0" />  <!-- MM field -->

        <!--
            Specifies the mailbox number or transfer dial string of the
            subscriber's personal operator or assistant. This field also
            indicates the transfer target when a caller to this subscriber
            presses 0 while listening to the subscriber's greeting.
        -->
        <xs:element name="personalOperatorMailbox" maxOccurs="1"
            minOccurs="0"> <!-- MM field -->
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:pattern value="[0-9]+([*#,][0-9]+)*" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!--
            Specifies when to route calls to the backup operator mailbox. The
```

```
            default value for this field is Always Active.
        -->
        <xs:element name="personalOperatorSchedule" type="xs:string"
            maxOccurs="1" minOccurs="0" /> <!-- MM field -->

        <!--
            Specifies the order in which the subscriber hears the voice
            messages. You can choose one of the following: - urgent first then
            newest: to direct the system to play any messages marked as urgent
            prior to playing non-urgent messages. Both the urgent and non-urgent
            messages are played in the reverse order of how they were received.
            - oldest messages first: to direct the system to play messages in
            the order they were received. - urgent first then oldest: to direct
            the system to play any messages marked as urgent prior to playing
            non-urgent messages. Both the urgent and non-urgent messages are
            played in the order of how they were received. - newest messages
            first: to direct the system to play messages in the reverse order
            of how they were received.
        -->
        <xs:element name="tuiMessageOrder" maxOccurs="1"
            minOccurs="0"> <!-- MM field -->
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="urgent first then newest" />
                    <xs:enumeration value="oldest messages first" />
                    <xs:enumeration value="newest messages first" />
                    <xs:enumeration value="urgent first then oldest" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!--
            Specifies the intercom paging settings for a subscriber. You can
            choose one of the following: - paging is off: to disable intercom
            paging for this subscriber. - paging is manual: if the subscriber
            can modify, with Subscriber Options or the TUI, the setting that
            allows callers to page the subscriber. - paging is automatic: if
            the TUI automatically allows callers to page the subscriber.
        -->
        <xs:element name="intercomPaging" maxOccurs="1" minOccurs="0">
        <!-- MM field -->
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="paging is off" />
                    <xs:enumeration value="paging is manual" />
                    <xs:enumeration value="paging is automatic" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!--
            Specifies whether a subscriber can receive messages, e-mail messages
            and call-answer messages from other subscribers. You can choose one
            of the following: - yes: to allow the subscriber to create, forward,
            and receive messages. - no: to prevent the subscriber from receiving
            call-answer messages and to hide the subscriber from the telephone
            user interface (TUI). The subscriber cannot use the TUI to access
            the mailbox, and other TUI users cannot address messages to the
            subscriber.
        -->
        <xs:element name="voiceMailEnabled" type="csm:xmlTrueFalseType"
            maxOccurs="1" minOccurs="0" />

        <!--
            Specifies additional, useful information about a subscriber. Entries
```

```
            in this field are for convenience and are not used by the messaging
            system.
        -->
        <xs:element name="miscellaneous1" type="csm:xmlLength51Type"
            maxOccurs="1" minOccurs="0" />

        <!--
            Specifies additional, useful information about a subscriber. Entries
            in this field are for convenience and are not used by the messaging
            system.
        -->
        <xs:element name="miscellaneous2" type="csm:xmlLength51Type"
            maxOccurs="1" minOccurs="0" />

        <!--
            Specifies additional, useful information about a subscriber. Entries
            in this field are for convenience and are not used by the messaging
            system.
        -->
        <xs:element name="miscellaneous3" type="csm:xmlLength51Type"
            maxOccurs="1" minOccurs="0" />

        <!--
            Specifies additional, useful information about a subscriber. Entries
            in this field are for convenience and are not used by the messaging
            system.
        -->
        <xs:element name="miscellaneous4" type="csm:xmlLength51Type"
            maxOccurs="1" minOccurs="0" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlCMMSpecific">
    <xs:sequence>

        <!--
            Specifies the number of the switch on which this subscriber's
            extension is administered. You can enter "0" through "99", or leave
            this field blank. - Leave this field blank if the host switch number
            should be used. - Enter a "0" if no message waiting indicators
            should be sent for this subscriber. You should enter 0 when the
            subscriber does not have a phone on any switch in the network.
        -->
        <xs:element name="switchNumber" maxOccurs="1" minOccurs="0">
        <!-- CMM field -->
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:pattern value="[0-9]|[0-9][0-9]" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!--
            Specifies the Subscriber Account Code. The Subscriber Account Code
            is used to create Call Detail Records on the switch for calls placed
            by the voice ports. The value you enter in this field can contain
            any combination of digits from 0 to 9. If an account code is not
            specified, the system will use the subscriber's mailbox extension as
            the account code.
        -->
        <xs:element name="accountCode" maxOccurs="1" minOccurs="0">
        <!-- CMM field -->
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:pattern value="([0-9])*" />
```

```
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!--
            Specifies the number to be used as the default destination for the
            Transfer Out of Messaging feature. You can enter 3 to 10 digits in
            this field depending on the length of the system's extension, or
            leave this field blank.
        -->
        <xs:element name="coveringExtension" maxOccurs="1"
            minOccurs="0"> <!-- CMM field -->
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:pattern value="[0-9]{0}|[0-9]{3,10}" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <!--
            Specifies additional, useful information about a subscriber. Entries
            in this field are for convenience and are not used by the messaging
            system.
        -->
        <xs:element name="miscellaneous1" type="csm:xmlLength11Type"
            maxOccurs="1" minOccurs="0" />

        <!--
            Specifies additional, useful information about a subscriber. Entries
            in this field are for convenience and are not used by the messaging
            system.
        -->
        <xs:element name="miscellaneous2" type="csm:xmlLength11Type"
            maxOccurs="1" minOccurs="0" />

        <!--
            Specifies additional, useful information about a subscriber. Entries
            in this field are for convenience and are not used by the messaging
            system.
        -->
        <xs:element name="miscellaneous3" type="csm:xmlLength11Type"
            maxOccurs="1" minOccurs="0" />

        <!--
            Specifies additional, useful information about a subscriber. Entries
            in this field are for convenience and are not used by the messaging
            system.
        -->
        <xs:element name="miscellaneous4" type="csm:xmlLength11Type"
            maxOccurs="1" minOccurs="0" />
    </xs:sequence>
</xs:complexType>

<xs:simpleType name="xmlyesNoType">
    <xs:restriction base="xs:string">
        <xs:enumeration value="Yes" />
        <xs:enumeration value="No" />
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="xmlTrueFalseType">
    <xs:restriction base="xs:string">
        <xs:enumeration value="TRUE" />
        <xs:enumeration value="FALSE" />
    </xs:restriction>
```

```
    </xs:simpleType>

    <xs:simpleType name="xmlLength11Type">
        <xs:restriction base="xs:string">
            <xs:maxLength value="11" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="xmlLength51Type">
        <xs:restriction base="xs:string">
            <xs:maxLength value="51" />
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

Sample XML for bulk import of messaging profiles

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
    <tns:user>
        <authenticationType>BASIC</authenticationType>
        <description>description</description>
        <displayName>displayname</displayName>
        <displayNameAscii>displayNameAscii</displayNameAscii>
        <dn>dn</dn>
        <isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>givenName00</givenName>
        <honorific>honorific</honorific>
        <loginName>user00_00xyz@avaya.com</loginName>
        <middleName>middleName</middleName>
        <managerName>managerName</managerName>
        <preferredGivenName>preferredGivenName</preferredGivenName>
        <preferredLanguage>preferredLanguage</preferredLanguage>
        <source>local</source>
        <sourceUserKey>sourceUserKey</sourceUserKey>
        <status>AUTHPENDING</status>
        <suffix>suffix</suffix>
        <surname>surname</surname>
        <timeZone>timeZone</timeZone>
        <title>title</title>
        <userName>userName00</userName>
        <userPassword>userPassword</userPassword>
        <commPassword>commPassword</commPassword>
        <userType>ADMINISTRATOR</userType>
        <commProfileSet>
            <commProfileSetName>
                commProfileSetName00
            </commProfileSetName>
            <isPrimary>true</isPrimary>
            <commProfileList>
                <commProfile xsi:type="ipt:xmlMessagingProfile"
                    xmlns:ipt="http://xml.avaya.com/schema/import_csm_mm">
                    <commProfileType>Messaging</commProfileType>
                    <ipt:messagingName>MM-155-187</ipt:messagingName>
                    <ipt:useExisting>false</ipt:useExisting>
                    <ipt:messagingTemplate>
                        DEFAULT_MM_5_2
                    </ipt:messagingTemplate>
                    <ipt:mailboxNumber>3201</ipt:mailboxNumber>
                    <ipt:password>534456346</ipt:password>
                    <ipt:cos>0</ipt:cos>
```

```
                    <ipt:communityID>1</ipt:communityID>
                    <ipt:mmSpecific>
                        <ipt:numericAddress>3201</ipt:numericAddress>
                        <ipt:pbxExtension>32134</ipt:pbxExtension>
                        <ipt:telephoneNumber>42342</ipt:telephoneNumber>
                        <!--<ipt:expirePassword></ipt:expirePassword>-->
                        <ipt:tuiMessageOrder>newest messages first
</ipt:tuiMessageOrder>
                        <ipt:intercomPaging>paging is off
</ipt:intercomPaging>
                        <ipt:voiceMailEnabled>
                            FALSE
                        </ipt:voiceMailEnabled>
                        <ipt:miscellaneous1>
                            Miscellaneous
                        </ipt:miscellaneous1>
                    </ipt:mmSpecific>
                </commProfile>
            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema Definition for bulk import of agent profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:one="http://xml.avaya.com/
schema/import" elementFormDefault="qualified"
targetNamespace="http://xml.avaya.com/schema/import_csm_agent" xmlns:csm="http://
xml.avaya.com/schema/import_csm_agent">
<xs:import namespace="http://xml.avaya.com/schema/import"
schemaLocation="userimport.xsd"/>

<!--Changes in xsd file need to generate jaxb src using this xsd-->
<xs:complexType name="xmlAgentProfile">
    <xs:complexContent>
           <xs:extension base="one:xmlCommProfileType" >
            <xs:sequence>
                <!-- CM Name as it appears under 'Applications/Application Management/
Entities -->
                <xs:element name="cmName" type="xs:string" maxOccurs="1" minOccurs="1"/>

                <!-- 'true' if already created extension is to be used.  'false' if
available extension is to be used. -->
                <xs:element name="useExistingAgent" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

                <!-- Extension Range which will be used to create Agent using available
extension within given range -->
                <xs:element name="extensionRange" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|([0-9]+([\.\-]
[0-9]+)*:[0-9]+([\.\-][0-9]+)*)"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Agent Login ID extension number that need to be assigned to the
user. -->
                <xs:element name="loginIdExtension" maxOccurs="1" minOccurs="1">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|[nN][eE][xX][tT]"/>
                        </xs:restriction>
```

```
                    </xs:simpleType>
                </xs:element>

                <!-- Template name to be used to create agent. Values defined in Template
will be used if not provided. -->
                <xs:element name="template" type="xs:string" maxOccurs="1" minOccurs="0"/>

                <!-- Security code for station. Value can be digit only.  -->
                <xs:element name="securityCode" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]{0,4}"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="aas" type="xs:boolean" maxOccurs="1" minOccurs="0"/>
                <xs:element name="audix" type="xs:boolean" maxOccurs="1" minOccurs="0"/>

                <xs:element name="password" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]{0,9}" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="portExtension" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="[0-9]+([\.\-][0-9]+)*"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <!-- Whether the agent should be deleted if it unassigned from the user.
-->
                <xs:element name="deleteOnUnassign" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

                <!-- CM dependent field for max value -->
                <xs:element name="tn" maxOccurs="1" minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:int">
                            <xs:minInclusive value="1" />
                            <xs:maxInclusive value="250" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="cor" maxOccurs="1" minOccurs="0">
                      <xs:simpleType>
                        <xs:restriction base="xs:int">
                              <xs:minInclusive value="0"/>
                              <xs:maxInclusive value="995"/>
                        </xs:restriction>
                      </xs:simpleType>
                </xs:element>

                <!--Coverage path = Enter path number between 1-9999, time of day table
t1-t999, or blank - CM Dependent-->
                <xs:element name="coveragePath" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:pattern value="(t[1-9][0-9]{0,2})|([1-9]{0})|([1-9][0-9]
```

```
{0,3})"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="lwcReception" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="audix"/>
                            <xs:enumeration value="msa"/>
                            <xs:enumeration value="spe"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="lwcLogExternalCalls" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="audixNameforMessaging" type="xs:string" maxOccurs="1"
minOccurs="0" />
                <xs:element name="hearsServiceObservingTone" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
                <xs:element name="loginIDforISDNSIPDisplay" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

                <xs:element name="autoAnswer" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="acd"/>
                            <xs:enumeration value="all"/>
                            <xs:enumeration value="none"/>
                            <xs:enumeration value="station"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="miaAcrossSkills" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="n"/>
                            <xs:enumeration value="y"/>
                            <xs:enumeration value="system"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="acwAgentConsideredIdle" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="n"/>
                            <xs:enumeration value="y"/>
                            <xs:enumeration value="system"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="auxWorkReasonCodeType" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="forced"/>
                            <xs:enumeration value="requested"/>
                            <xs:enumeration value="system"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
```

```
                </xs:element>

                <xs:element name="logoutReasonCodeType" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="forced"/>
                            <xs:enumeration value="requested"/>
                            <xs:enumeration value="system"/>
                            <xs:enumeration value="none"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="maximumTimeAgentInAcwBeforeLogoutSec" maxOccurs="1"
minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                              <xs:pattern value="|[3-9][0-9]{1}|[1-9][0-9]{1,3}|(none)|
(system)"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="forcedAgentLogoutTimeHr" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="|[0-9]|[1][0-9]{1}|[2][0-3]{1}"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="forcedAgentLogoutTimeSec" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                              <xs:pattern value="|(00)|(15)|(30)|(45)"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="directAgentSkill" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:pattern value="|[1-9]|[1-9][0-9]{0,2}|[1-7][0-9]{3}|
8000"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="callHandlingPreference" maxOccurs="1" minOccurs="0">
                    <xs:simpleType>
                          <xs:restriction base="xs:string">
                            <xs:enumeration value="greatest-need"/>
                            <xs:enumeration value="percent-allocation"/>
                            <xs:enumeration value="skill-level"/>
                          </xs:restriction>
                    </xs:simpleType>
                </xs:element>

                <xs:element name="serviceObjective" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="directAgentCallsFirst" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
                <xs:element name="localCallPreference" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
```

```
                <xs:element name="skills" type="csm:xmlAgentLoginIdSkillsData"
maxOccurs="unbounded" minOccurs="0" />

                <xs:element  name="nativeName" type="csm:xmlNativeNameData" maxOccurs="1"
minOccurs="0"/>

                <!--

                private String NativeNameScripts;

                 -->
            </xs:sequence>
        </xs:extension>
   </xs:complexContent>
</xs:complexType>

<xs:complexType name="xmlAgentLoginIdSkillsData">
    <xs:sequence>
    <!--
        private AgentLoginIdData agentLoginId;

     -->
        <xs:element name="number" type="xs:string" maxOccurs="1" minOccurs="1" />
        <xs:element name="skillNumber" maxOccurs="1" minOccurs="1">
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="[1-9][0-9]{0,2}|[1-7][0-9]{3}|8000"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="reserveLevel" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="|a|m|n|[1-2]"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="skillLevel" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="|[1-9]|[1-9][0-6]{1}"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>

        <xs:element name="percentAllocation" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:pattern value="|[1-9]|[1-9][0-9]{1}|100"/>
                  </xs:restriction>
            </xs:simpleType>
        </xs:element>


    </xs:sequence>
</xs:complexType>

<!-- If displayName,givenName or surname contains characters of multiple scripts then
locale tag should be present.
       If displayName tag is present then it overwrites native name.
       If displayname is not present then combination of givenName and surname gets
copied in native name.
       Please find below locale for multiscript language
```

```
       Language               Locale
       Japanese                 ja, ja-jp
       Simplified Chinese         zh-cn
       Traditional Chinese     zh-tw-->
<xs:complexType name="xmlNativeNameData">
    <xs:sequence>
        <xs:element name="locale" maxOccurs="1" minOccurs="0">
           <xs:simpleType>
                 <xs:restriction base="xs:string">
                   <xs:enumeration value="ja-jp"/>
                   <xs:enumeration value="ja"/>
                   <xs:enumeration value="zh-cn"/>
                   <xs:enumeration value="zh-tw"/>
                 </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="name" maxOccurs="1" minOccurs="0" >
            <xs:simpleType>
                 <xs:restriction base="xs:string">
                   <xs:maxLength value="27"/>
                 </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:sequence>
</xs:complexType>

</xs:schema>
```

XML Schema for CS1000 and CallPilot Communication Profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     xmlns:one="http://xml.avaya.com/schema/import"
     targetNamespace="http://xml.avaya.com/schema/import1"
     elementFormDefault="qualified"
     xmlns:abc="http://xml.avaya.com/schema/import1">
<xsd:import namespace="http://xml.avaya.com/schema/import"
            schemaLocation="userimport.xsd"/>
<xsd:complexType name="AccountCommProfileType">
    <xsd:complexContent>
        <xsd:extension base="one:xmlCommProfileType" >
            <xsd:sequence>
               <xsd:element name="serviceDetails" type="xsd:string" minOccurs="0"/>
               <xsd:element name="element" type="xsd:string" minOccurs="0"/>
               <xsd:element name="target" type="xsd:string" minOccurs="0"/>
               <xsd:element name="template" type="xsd:string" minOccurs="0"/>
               <xsd:element name="serviceType" type="xsd:string" minOccurs="0"/>
               <xsd:element name="accountDetails" type="xsd:string" minOccurs="0"/>
               <xsd:element name="accountProperties" type="abc:AccountPropertyType"
minOccurs="0" maxOccurs="unbounded"/>
            </xsd:sequence>
        </xsd:extension>
    </xsd:complexContent>
</xsd:complexType>

<xsd:complexType name="AccountPropertyType">
   <xsd:sequence>
      <xsd:element name="propertyName" type="xsd:string"/>
      <xsd:element name="propertyValue" type="xsd:string"/>
    </xsd:sequence>
</xsd:complexType>
</xsd:schema>
```

Sample XML for CS1000 and CallPilot Communication Profiles

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ns3="http://xml.avaya.com/
schema/import1" xmlns:ns4="http://xml.avaya.com/schema/deltaImport" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/
import userimport.xsd">
    <tns:user>
        <authenticationType>basic</authenticationType>
        <description></description>
        <displayName>singleUser, singleUser</displayName>
        <displayNameAscii>singleUser, singleUser</displayNameAscii>
        <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
        <isEnabled>true</isEnabled>
        <isVirtualUser>false</isVirtualUser>
        <givenName>singleUser</givenName>
        <honorific></honorific>
        <loginName>singleuser@avaya.com</loginName>
        <employeeNo></employeeNo>
        <department></department>
        <organization></organization>
        <middleName></middleName>
        <preferredLanguage>en_US</preferredLanguage>
        <source>local</source>
        <sourceUserKe>Ynone</sourceUserKe>Y
        <status>provisioned</status>
        <surname>singleUser</surname>
        <userName>singleuser</userName>
        <userPassword></userPassword>
        <roles>
            <role>End-User</role>
        </roles>
        <ownedContactLists>
            <contactList>
                <name>list-singleuser_avaya.com</name>
                <description></description>
                <isPublic>false</isPublic>
                <contactListType>general</contactListType>
            </contactList>
        </ownedContactLists>
        <commProfileSet>
            <commProfileSetName>Primary</commProfileSetName>
            <isPrimar>Ytrue</isPrimar>Y
            <commProfileList>
                <commProfile xsi:type="ns3:AccountCommProfileType" xmlns:ns3="http://
xml.avaya.com/schema/import1">
                    <commProfileType>accountCommProfile</commProfileType>
                    <ns3:serviceDetails>DN=8054(Marped), TN=004 0 00 12, TYPE=M2602</
ns3:serviceDetails>
                    <ns3:element>CS1K Mock Element Manager</ns3:element>
                    <ns3:target>Target1</ns3:target>
                    <ns3:template>Premium</ns3:template>
<ns3:serviceType>com.nortel.ems.services.account.Telephony</ns3:serviceType>
                    <ns3:properties>
                        <ns3:property name="prefEsn">343-8054</ns3:propert>Y
                        <ns3:property name="prefDn">8054</ns3:propert>Y
                    </ns3:properties>
                    <ns3:isPublished>true</ns3:isPublished>
                </commProfile>
            </commProfileList>
        </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema for IP Office Communication Profiles

```
<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:one="http://xml.avaya.com/schema/import" elementFormDefault="qualified"
    targetNamespace="http://xml.avaya.com/schema/import_csm_b5800" xmlns:csm="http://
xml.avaya.com/schema/import_csm_b5800">

    <xs:import namespace="http://xml.avaya.com/schema/import"
        schemaLocation="userimport.xsd" />

    <!--Changes in xsd file need to generate jaxb src using this xsd-->
    <xs:complexType name="xmlB5800UserProfile">
        <xs:complexContent>
            <xs:extension base="one:xmlCommProfileType">
                <xs:sequence>
                    <!--
                        IPOffice/B5800/B5800L Device Name as it appears under
'Applications/Application
                        Management/Entities
                    -->
                    <xs:element name="deviceName" type="xs:string" maxOccurs="1"
                        minOccurs="1" />

                    <!--
                        Template name to be used to create station. Values defined in
                        Template will be used if not provided.
                    -->
                    <xs:element name="userTemplate" type="xs:string"
                        maxOccurs="1" minOccurs="0" />

                    <xs:element name="useExistingExt" type="xs:boolean"
                        maxOccurs="1" minOccurs="0" />

                    <!-- extension number that need to be assigned to the user. -->
                    <xs:element name="extension" maxOccurs="1" minOccurs="1">
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern value="[0-9]+([\.\-][0-9]+)*" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>

                    <xs:element name="modulePort" type="xs:string"
                        maxOccurs="1" minOccurs="0" />

                    <!-- Specifies the type of the extn  -->
                    <xs:element name="extensionType" maxOccurs="1"
                        minOccurs="1">
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:enumeration value="Analog" />
                                <xs:enumeration value="IPDECT" />
                                <xs:enumeration value="SIPDECT" />
                                <xs:enumeration value="Sip" />
                                <xs:enumeration value="Digital" />
                                <xs:enumeration value="H323" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:element>

                    <xs:element name="deleteExtOnUserDelete" type="xs:boolean"
                        maxOccurs="1" minOccurs="0" />

                    <xs:element name="data" type="csm:xmlB5800UserProfileData"
```

```
                        maxOccurs="1" minOccurs="0" />
                </xs:sequence>

            </xs:extension>

        </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="xmlB5800UserProfileData">
        <xs:sequence>
            <xs:element name="ws_object" type="csm:xmlB5800UserConfig">
            </xs:element>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlB5800UserConfig">
        <xs:sequence>
            <xs:element name="Extension" type="csm:xmlB5800ExtensionInfo">
            </xs:element>
            <xs:element name="User" type="csm:xmlB5800UserInfo">
            </xs:element>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlB5800ExtensionInfo">
        <xs:sequence>
            <xs:element name="Id" type="xs:int" minOccurs="0" />
            <xs:element name="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="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="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="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="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="MobileVoIPClientEnabled" type="xs:boolean" minOccurs="0" />
            <xs:element name="SendMobilityEmail" type="xs:boolean" 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="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: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: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="xmlAdvancedCodecPrefs">
        <xs:sequence>
            <xs:element name="codecPref" type="xs:string" minOccurs="0" />
        </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>user9000</givenName>
 <loginName>user9000@avaya.com</loginName>
 <middleName>middleName</middleName>
 <surname>surname</surname>
 <userPassword>userPassword</userPassword>
 <commPassword>commPassword</commPassword>
 <commProfileSet>
 <commProfileSetName>commProfileSetName5200</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>ABG_178_163</csm:deviceName>
    <csm:userTemplate>userinfo</csm:userTemplate>
    <csm:extension>9000</csm:extension>
    <csm:extensionType>Sip</csm:extensionType>
    <csm:deleteExtOnUserDelete>true</csm:deleteExtOnUserDelete>
</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/mock">
<commProfileType>PS</commProfileType>
<ext:primarySipEntityId>32768</ext:primarySipEntityId>
</commProfile>
</commProfileList>
</commProfileSet>
</tns:user>
</tns:users>
```

XML Schema for Conferencing Communication Profile

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
      xmlns:one="http://xml.avaya.com/schema/import"
      targetNamespace="http://xml.avaya.com/schema/import_mmcs"
      elementFormDefault="qualified"
      xmlns:abc="http://xml.avaya.com/schema/import_mmcs">

<!--
    This is the XML schema for the Avaya Aura Conferencing Profile. It
     defines this profile inside of an XML document that defines a user record
  (see userimport.xsd)
-->

<xsd:import namespace="http://xml.avaya.com/schema/import"
                      schemaLocation="userimport.xsd"/>
   <xsd:complexType name="MmcsCommProfileType">
      <xsd:complexContent>
         <xsd:extension base="one:xmlCommProfileType" >
            <xsd:sequence>
               <xsd:element name="template" type="xsd:string"/>
               <xsd:element name="securityCode" type="xsd:string"/>
               <xsd:element name="moderatorPin" type="xsd:string"/>
               <xsd:element name="eventConfCode" type="xsd:string"/>
               <xsd:element name="location" type="xsd:string" minOccurs="0"/>
               <xsd:element name="autoGeneratedCodeLength" minOccurs="0">
                 <xsd:simpleType>
                   <xsd:restriction base="xsd:int">
                     <xsd:minInclusive value="6"/>
                     <xsd:maxInclusive value="8"/>
                   </xsd:restriction>
                 </xsd:simpleType>
               </xsd:element>
            </xsd:sequence>
         </xsd:extension>
      </xsd:complexContent>
   </xsd:complexType>
</xsd:schema>
```

Sample XML for bulk import of Conferencing Profile

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd ">

    <!-- User Record for: 5555555@domain.com -->
    <tns:user>

(Other user elements are required here - consult the main user record XML schema
reference)
```

```
<!-- Here, a Communication Profile is defined for the user -->
       <commProfileSet>
             <commProfileSetName>Primary</commProfileSetName>
                <isPrimary>true</isPrimary>


<!-- The user must be given one or more handles (of type “SIP” or E.164) -->
                <handleList>
                <handle>
                <handleName>5555555</handleName>
                <handleType>sip</handleType>
                <handleSubType>username</handleSubType>
                <domainName>domain.com</domainName>
                </handle>
                </handleList>

<!-- Here, one or more product-specific profiles may be Defined -->

               <commProfileList>

                  <commProfile xsi:type="ns2:MmcsCommProfileType" xmlns:ns2="http://
xml.avaya.com/schema/import_mmcs">
                  <commProfileType>mmcsCommProfile</commProfileType>
                  <ns2:template>event_1000</ns2:template>
                  <ns2:securityCode></ns2:securityCode>
                  <ns2:moderatorPin></ns2:moderatorPin>
                  <ns2:eventConfCode>777</ns2:eventConfCode>
                  <ns2:location>Location1</ns2:location>
                  <ns2:autoGeneratedCodeLength>6</ns2:autoGeneratedCodeLength>
               </commProfile>
            </commProfileList>
         </commProfileSet>
    </tns:user>
</tns:users>
```

XML Schema Definition for bulk import of global setting records

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ext="http://xml.avaya.com/
schema/import" xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="http://
xml.avaya.com/schema/import" version="1.0">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            This Schema defines schema for bulk import and export of System ACL,Public
Contacts and Shared Address.
        </xs:documentation>
    </xs:annotation>
    <xs:element name="presenceSystemDefault" type="tns:xmlPresSystemDefaultType"/>
    <xs:element name="presenceEnforcedUserACL"
type="tns:xmlPresEnforcedUserACLEntryType"/>
    <xs:element name="presenceSystemRule" type="tns:xmlPresSystemRuleType"/>
    <xs:element name="presenceSystemACL" type="tns:xmlPresSystemACLEntryType"/>
    <xs:element name="publicContact" type="tns:xmlPublicContact"/>
    <xs:element name="globalSettings" type="tns:globalSettingsType"/>
    <xs:element name="sharedAddress" type="tns:xmlSharedAddress"/>
    <xs:complexType name="globalSettingsType">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            ---Root Element 'presenceSystemDefault' represent a global default that
                defines access to presence if none of the more specific rules apply.
                There must be at least one System Default rule defined.
            ---Root Element 'presenceEnforcedUserACL' represent collection of
                Enforced User ACL (containing 1 or more Enforced User ACL).This rule
                is similar to a User ACL in the sense that its entries define access
```

```
                between individual presentities and watchers. However this rule is
                managed by the administrator as opposed to presentities themselves.
                Entries of Enforced User ACL can also be defined with different
                priorities. Entries with higher priority will have more weight than
                entries with lower priority.
            ---Root Element 'presenceSystemRule' represent collection of System
                Rules (containing 1 or more System Rules).Global rules that enforce
                certain level of presence access for everyone in the solution. There
                may be several rules that apply to all presentities and all watchers.
                System Rules are used to enforce global policies. For example, a
                system rule can declare that telephony presence should be available
                to everybody in the company. System Rules can be defined with
                different priorities. Rules with higher priority will have more
                weight than rules with lower priority
            ---Root Element 'presenceSystemACL' represent collection of System ACL
                (containing 1 or more System ACL).
                System ACL (Access Control List) - are enterprise-wide rules that can
                allow a watcher to see presence of all users or deny a watcher from
                accessing anyone's presence.  There may be several entries in the
                list, each entry corresponding to one watcher. System ACL is
                normally used to provide critical system services with a privileged
                access to presence of all users.
            ---Root Element 'publicContact' represent collection of public contacts
                (containing 1 or more public contacts).A personal contact is owned
                by an individual user and is not accessible to all users. A public
                contact can be shared by all users and is owned by the default
                system user.
            ---Root Element 'sharedAddress' represent collection of  shared Address
                (containing 1 or more shared Addresses).A shared Address can be
                shared by all users.
        </xs:documentation>
    </xs:annotation>
        <xs:sequence>
            <xs:element name="presenceSystemDefault" type="tns:xmlPresSystemDefaultType"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="presenceEnforcedUserACL"
type="tns:xmlPresEnforcedUserACLEntryType" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="presenceSystemRule" type="tns:xmlPresSystemRuleType"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="presenceSystemACL" type="tns:xmlPresSystemACLEntryType"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="sharedAddress" type="tns:xmlSharedAddress" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="publicContact" type="tns:xmlPublicContact" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlSharedAddress">
        <xs:sequence>
            <xs:annotation>
                <xs:documentation xml:lang="en">
                    ---addressType:The unique text name of the address type.
                            Possible values are: Home, business.
                    ---name: The Name property defines the unique label by which
                            the address is known. Default format for user specific
                            address should include user name place address type.
                    ---building:The name or other designation of a structure.
                    ---localityName:The name of a locality, such as a city, county
                            or other geographic region.
                    ---postalCode:A code used by postal services to route mail to a
                            destination. In the United States this is the zip code.
                    ---room:Name or designation of a room.
                    ---stateOrProvince:The full name of a state or province.
                    ---country:A country.
                    ---street:The physical address of the object such as an address
```

```
                        for package delivery
                ---postalAddress:A free formed text area for the complete
                        physical delivery address. It may be used in place of the
                        specific fields in this table.
                ---readOnly:A boolean indicator showing whether or not the
                        address can be changed from its default value.
            </xs:documentation>
        </xs:annotation>
        <xs:element name="addressType" type="xs:string"/>
        <xs:element name="name" type="xs:string"/>
        <xs:element name="building" type="xs:string" minOccurs="0"/>
        <xs:element name="localityName" type="xs:string" minOccurs="0"/>
        <xs:element name="postalCode" type="xs:string" minOccurs="0"/>
        <xs:element name="room" type="xs:string" minOccurs="0"/>
        <xs:element name="stateOrProvince" type="xs:string" minOccurs="0"/>
        <xs:element name="country" type="xs:string" minOccurs="0"/>
        <xs:element name="street" type="xs:string" minOccurs="0"/>
        <xs:element name="postalAddress" minOccurs="0">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:maxLength value="1024"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="readOnly" type="xs:boolean" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlPublicContact">
    <xs:sequence>
        <xs:annotation>
            <xs:documentation xml:lang="en">
                ---company:The organization that the contact belongs to.
                ---description: A free text field containing human readable
                    text providing information on this entry.
                ---displayName:The localized name of a contact to be used when
                    displaying. It will typically be the localized full name.
                    This value may be provisioned from the user's enterprise
                    directory entry. If it does not exist, synchronization
                    rules can be used to populate it for other fields
                    e.g. Surname, GivenName, or LoginName.
                ---displayNameAscii:The full text name of the contact
                    represented in ASCII. It is used to support display
                    (e.g. endpoints) that cannot handle localized text.
                ---dn:The distinguished name of the user. The DN is a sequence
                    of relative distinguished names (RDN) connected by commas.
                    An RDN is an attribute with an associated value in the form
                    of attribute=value, normally expressed in a UTF-8 string
                    format. The dn can be used to uniquely identify this
                    record. Note the dn is changeable.
                ---givenName:The first name of the contact.
                ---initials:Initials of the contact.
                ---middleName:The middle name of the contact.
                ---preferredGivenName:The nick name of the contact.
                ---preferredLanguage:The individual's preferred written or
                    spoken language. Values will conform to rfc4646 and the
                    reader should refer to rfc4646 for syntax.  This format
                    uses the ISO standard Language (ISO-639) and region
                    (ISO-3166) codes In the absence of a value the client's
                    locale should be used, if no value is set, en-US should be
                    defaulted.
                ---source:Free format text field that identifies the entity
                    that created this user record.  The format of this field
                    will be either a IP Address/Port or a name representing an
                    enterprise LDAP or Avaya.
                ---sourceUserKey:The key of the user from the source system. If
```

```
                        the source is an Enterprise Active Directory server, this
                        value with be the objectGUID.
                    ---suffix:The text appended to a name e.g. Jr., III.
                    ---surname:The user's last name, also called the family name.
                    ---title:The job function of a person in their organizational
                        context.Examples: supervisor, manager.
                    ---contactAddresses:A Entity used to store a contact’s address.
                    ---addresses:A fully qualified URI for interacting with this
                        contact. Any addresses added to this entity should contain
                        a qualifier e.g. sip, sips, tel, mailto. The address should
                        be syntactically valid based on the qualifier. It must be
                        possible to add via the GUI and Interface. The application
                        must do validation.
                </xs:documentation>
            </xs:annotation>
            <xs:element name="company" type="xs:string" minOccurs="0"/>
            <xs:element name="description" type="xs:string" minOccurs="0"/>
            <xs:element name="displayName" type="xs:string"/>
            <xs:element name="displayNameAscii" type="xs:string"/>
            <xs:element name="dn" type="xs:string" minOccurs="0"/>
            <xs:element name="givenName" type="xs:string"/>
            <xs:element name="initials" type="xs:string" minOccurs="0"/>
            <xs:element name="middleName" type="xs:string" minOccurs="0"/>
            <xs:element name="preferredGivenName" type="xs:string" minOccurs="0"/>
            <xs:element name="preferredLanguage" type="xs:string" minOccurs="0"/>
            <xs:element name="source" type="xs:string"/>
            <xs:element name="sourceUserKey" type="xs:string"/>
            <xs:element name="suffix" type="xs:string" minOccurs="0"/>
            <xs:element name="surname" type="xs:string"/>
            <xs:element name="title" type="xs:string" minOccurs="0"/>
            <xs:element name="contactAddresses" type="tns:xmlContactAddressList"
minOccurs="0"/>
            <xs:element name="addresses" type="tns:xmlAddressList" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlContactAddressList">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                  ContactAddressList: A list containing Contact Addresses
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="contact" type="tns:xmlContactAddress" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlContactAddress">
        <xs:sequence>
            <xs:annotation>
                <xs:documentation xml:lang="en">
                    ---type:The value reflecting the type of handle this is.
                        Possible values are “username”,”e164”, and
                        “privatesubsystem"
                    ---category:The value representing a further qualification to
                        the contact address.
                        Possible values inlcude Office, Home, Mobile.
                    ---handle:This is the name given to the user to allow
                        communication to be established with the user. It is an
                        alphanumeric value that must comply with the userinfo
                        related portion of a URI as described in rfc2396. However,
                        it is further restricted as ASCII characters with only the
                        “+” prefix to signify this is an E.164 handle and "_" and
                        "." special characters supported.The handle and type together
                        are unique within a specific domain. Note, the handle plus
                        domain can be used to construct a user’s Address of Record.
```

```
                    ---label:A free text description for classifying this contact.
                    ---altLabel:A free text description for classifying this
                        contact. This is similar to ContactLabel, but it is used to
                        store alternate language representations.
                </xs:documentation>
            </xs:annotation>
            <xs:element name="type" type="xs:string"/>
            <xs:element name="category" type="xs:string" minOccurs="0"/>
            <xs:element name="handle" type="xs:string"/>
            <xs:element name="label" type="xs:string" minOccurs="0"/>
            <xs:element name="altLabel" type="xs:string" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlAddressList">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                  AddressList: A list containing Addresses
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="address" type="tns:xmlAddress" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlAddress">
        <xs:complexContent>
            <xs:extension base="tns:xmlSharedAddress">
                <xs:sequence>
                    <xs:annotation>
                        <xs:documentation xml:lang="en">
                              private:A boolean indicator to specify if this
                                attribute set could be shared across multiple
                                users. Private attributes sets can only be owned
                                by a single user. Default=false.
                        </xs:documentation>
                    </xs:annotation>
                    <xs:element name="private" type="xs:boolean"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresInfoTypeAccessType">
        <xs:sequence>
            <xs:annotation>
                <xs:documentation xml:lang="en">
                     ---accessLevel:possible values:IM,Telephony
                     ---action:Action possible values: ALLOW, BLOCK, CONFIRM,
                        PENDING, UNDEFINED
                </xs:documentation>
            </xs:annotation>
            <xs:element name="accessLevel" type="xs:string"/>
            <xs:element name="action" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlPresACRuleType">
        <xs:sequence>
            <xs:element name="infoTypeAccess" type="tns:xmlPresInfoTypeAccessType"
minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="xmlPresSystemDefaultType">
        <xs:annotation>
        <xs:documentation xml:lang="en">
            'presenceSystemDefault' represent a global default that defines
                access to presence if none of the more specific rules apply.
```

```
                There must be at least one System Default rule defined.
        </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType"/>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresSystemRuleType">
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType">
                <xs:sequence>
                    <xs:annotation>
                        <xs:documentation xml:lang="en">
                           'presenceSystemRule' represent collection of System
                            Rules (containing 1 or more System Rules).Global rules
                            that enforce certain level of presence access for
                            everyone in the solution. There may be several rules
                            that apply to all presentities and all watchers.
                            System Rules are used to enforce global policies.
                            For example, a system rule can declare that telephony
                            presence should be available to everybody in the
                            company. System Rules can be defined with different
                            priorities.
                            Rules with higher priority will have more weight than
                            rules with lower priority apply to all presentities and
                            all watchers.
                          ---priority:Entries of Enforced User ACL can also be
                            defined with different priorities. Entries with higher
                            priority will have more weight than entries with lower
                            priority.
                         </xs:documentation>
                    </xs:annotation>
                    <xs:element name="priority" type="xs:string"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresSystemACLEntryType">
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType">
                <xs:sequence>
                    <xs:annotation>
                        <xs:documentation xml:lang="en">
                          ---'presenceSystemACL' represent collection of System ACL
                            (containing 1 or more System ACL).System ACL
                            (Access Control List) - are enterprise-wide rules that
                            can allow a watcher to see presence of all users or
                            deny a watcher from accessing anyone's presence.  There
                            may be several entries in the list, each entry
                            corresponding to one watcher. System ACL is normally
                            used to provide critical system services with a
                            privileged access to presence of all users.
                           ---watcherLoginName:LoginName of the watcher. This value
                            needs to be specified if watcher is a user.
                           ---watcherDisplayName:DisplayName of the watcher. This
                            value needs to be specified if watcher is a Contact
                         </xs:documentation>
                    </xs:annotation>
                    <xs:choice>
                        <xs:element name="watcherLoginName" type="xs:string"
minOccurs="0"/>
                        <xs:element name="watcherDisplayName" type="xs:string"
minOccurs="0"/>
                    </xs:choice>
                </xs:sequence>
```

```
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="xmlPresEnforcedUserACLEntryType">
        <xs:complexContent>
            <xs:extension base="tns:xmlPresACRuleType">
                <xs:sequence>
                    <xs:annotation>
                        <xs:documentation xml:lang="en">
                          ---'presenceEnforcedUserACL' represent collection of
                            Enforced User ACL (containing 1 or more Enforced
                            User ACL).This rule is similar to a User ACL in the
                            sense that its entries define access between
                            individual presentities and watchers. However this
                            rule is managed by the administrator as opposed to
                            presentities themselves. Entries of Enforced User ACL
                            can also be defined with different priorities. Entries
                            with higher priority will have more weight than entries
                            with lower priority.
                           ---watcherLoginName:LoginName of the watcher. This value
                            needs to be specified if watcher is a user.
                           ---watcherDisplayName:DisplayName of the watcher. This
                            value needs to be specified if watcher is a Contact
                           ---priority:Entries of Enforced User ACL can also be
                            defined with different priorities. Entries with higher
                            priority will have more weight than entries with lower
                            priority.
                            ---userName:LoginName of the presentity.
                         </xs:documentation>
                    </xs:annotation>
                    <xs:element name="userName" type="xs:string"/>
                    <xs:choice>
                        <xs:element name="watcherLoginName" type="xs:string"
minOccurs="0"/>
                        <xs:element name="watcherDisplayName" type="xs:string"
minOccurs="0"/>
                    </xs:choice>
                    <xs:element name="priority" type="xs:string"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
</xs:schema>
```

Sample XML for bulk import of global setting records

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:globalSettings xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/
import systemPresence.xsd ">

  <!--
    Root Element 'presenceSystemDefault' represent a global default that defines
        access to presence if none of the more specific rules apply. There must
        be at least one System Default rule defined.
     accessLevel:possible values:ALL,Telephony
     action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
  -->
  <tns:presenceSystemDefault>
      <infoTypeAccess>
        <accessLevel>ALL</accessLevel>
        <action>ALLOW</action>
      </infoTypeAccess>
    </tns:presenceSystemDefault>
    <!--
```

```
        Root Element 'presenceEnforcedUserACL' represent collection of Enforced
            User ACL (containing 1 or more Enforced User ACL).This rule is
            similar to a User ACL in the sense that its entries define access
            between individual presentities and watchers. However this rule is
            managed by the administrator as opposed to presentities themselves.
            Entries of Enforced User ACL can also be defined with different
            priorities. Entries with higher priority will have more weight than
            entries with lower priority.
        ---accessLevel:possible values:ALL,Telephony
        ---action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
        ---watcherLoginName:LoginName of the watcher. This value needs to be
            specified if watcher is a user.
        ---watcherDisplayName:DisplayName of the watcher. This value needs to be
            specified if watcher is a Contact
        ---priority:Entries of Enforced User ACL can also be defined with different
            priorities. Entries with higher priority will have more weight than
            entries with lower priority.
        ---userName:LoginName of the presentity.
-->
    <tns:presenceEnforcedUserACL>
      <infoTypeAccess>
        <accessLevel>Telephony</accessLevel>
        <action>BLOCK</action>
      </infoTypeAccess>
      <userName>jmiller@avaya.com</userName>
      <watcherLoginName>userlogin2@avaya.com</watcherLoginName>
      <priority>HIGH</priority>
    </tns:presenceEnforcedUserACL>
    <!--
    Root Element 'presenceSystemRule' represent collection of System Rules
        (containing 1 or more System Rules).Global rules that enforce certain level
        of presence access for everyone in the solution. There may be several rules
        that apply to all presentities and all watchers. System Rules are used to
        enforce global policies. For example, a system rule can declare that
        telephony presence should be available to everybody in the company.
        System Rules can be defined with different priorities. Rules with higher
        priority will have more weight than rules with lower priority
    ---accessLevel:possible values:IM,Telephony
    ---action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
    ---watcherLoginName:LoginName of the watcher. This value needs to be specified
        if watcher is a user.
    ---watcherDisplayName:DisplayName of the watcher. This value needs to be
        specified if watcher is a Contact
    ---priority:Entries of Enforced User ACL can also be defined with different
        priorities. Entries with higher priority will have more weight than
        entries with lower priority.
    -->
    <tns:presenceSystemRule>
      <infoTypeAccess>
        <accessLevel>Telephony</accessLevel>
        <action>ALLOW</action>
      </infoTypeAccess>
      <priority>HIGH</priority>
    </tns:presenceSystemRule>
   <!--
    Root Element 'presenceSystemACL' represent collection of System ACL
        (containing 1 or more System ACL).
        System ACL (Access Control List) - are enterprise-wide rules that can allow
        a watcher to see presence of all users or     deny a watcher from accessing
        anyone's presence.  There may be several entries in the list, each entry
        corresponding to one watcher. System ACL is normally used to provide
        critical system services with a privileged access to presence of all users.
    ---accessLevel:possible values:IM,Telephony
    ---action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
    ---watcherLoginName:LoginName of the watcher. This value needs to be specified
```

```
      if watcher is a user.
-->
  <tns:presenceSystemACL>
    <infoTypeAccess>
      <accessLevel>Telephony</accessLevel>
      <action>BLOCK</action>
    </infoTypeAccess>
    <watcherLoginName>jmiller@avaya.com</watcherLoginName>
  </tns:presenceSystemACL>
<!--
  Root Element 'publicContact' represent collection of public contacts
      (containing 1 or more public contacts).A personal contact is owned by an
      individual user and is not accessible to all users. A public contact can
      be shared by all users and is owned by the default system user.
  ---company:The organization that the contact belongs to.
  ---description: A free text field containing human readable text providing
      information on this entry.
  ---displayName:The localized name of a contact to be used when displaying.
      It will typically be the localized full name. This value may be provisioned
      from the user's enterprise directory entry. If it does not exist,
      synchronization rules can be used to populate it for other fields
      e.g. Surname, GivenName, or LoginName.
  ---displayNameAscii:The full text name of the contact represented in ASCII. It is
      used to support display (e.g. endpoints) that cannot handle localized text.
  ---dn:The distinguished name of the user. The DN is a sequence of relative
      distinguished names (RDN) connected by commas. An RDN is an attribute with
      an associated value in the form of attribute=value, normally expressed in a
      UTF-8 string format. The dn can be used to uniquely identify this record.
      Note the dn is changeable.
  ---givenName:The first name of the contact.
  ---initials:Initials of the contact.
  ---middleName:The middle name of the contact.
  ---preferredGivenName:The nick name of the contact.
  ---preferredLanguage:The individual's preferred written or spoken language.
      Values will conform to rfc4646 and the reader should refer to rfc4646 for
      syntax.
      This format uses the ISO standard Language (ISO-639) and region (ISO-3166)
      codes In the absence of a value the client's locale should be used, if no
      value is set, en-US should be defaulted.
  ---source:Free format text field that identifies the entity that created this
      user record.  The format of this field will be either a IP Address/Port or
      a name representing an enterprise LDAP or Avaya.
  ---sourceUserKey:The key of the user from the source system. If the source is
      an Enterprise Active Directory server, this value with be the objectGUID.
  ---suffix:The text appended to a name e.g. Jr., III.
  ---surname:The user's last name, also called the family name.
  ---title:The job function of a person in their organizational context.
      Examples: supervisor, manager.
  ---contactAddresses:A table used to store a contact's address.
  ---addresses:A fully qualified URI for interacting with this contact.
      Any addresses added to this table should contain a qualifier
      e.g. sip, sips, tel, mailto. The address should be syntactically valid
      based on the qualifier. It must be possible to add via the GUI and
      Interface. The application must do validation.
  -->
  <tns:publicContact>
    <company>ABC</company>
    <description>Company ABC description</description>
    <displayName>John Miller</displayName>
    <displayNameAscii></displayNameAscii>
    <dn>dc=acme,dc=org</dn>
    <givenName>John</givenName>
    <initials>Mr</initials>
    <middleName>M</middleName>
    <preferredGivenName>John</preferredGivenName>
```

```
    <preferredLanguage>English</preferredLanguage>
    <source>ldap</source>
    <sourceUserKey>18966</sourceUserKey>
    <suffix>Jr.</suffix>
    <surname>Miller</surname>
    <title>Manager</title>
    <!--
      ---type:The value reflecting the type of handle this is. Possible values
          are “username”, ”e164”, and “privatesubsystem
      ---category:The value representing a further qualification to the contact
          address. Possible values inlcude Office, Home, Mobile.
      ---handle:This is the name given to the user to allow communication to be
          established with the user. It is an alphanumeric value that must comply
          with the userinfo related portion of a URI as described in rfc2396.
          However, it is further restricted as ASCII characters with only the “+”
          prefix to signify this is an E.164 handle and "_" and "." special
          characters supported.The handle and type together are unique within a
          specific domain. Note, the handle plus domain can be used to construct
          a user’s Address of Record.
      ---label:A free text description for classifying this contact.
      ---altLabel:A free text description for classifying this contact. This is
          similar to ContactLabel, but it is used to store alternate language
          representations.
  -->
    <contactAddresses>
      <contact>
        <type>sip</type>
        <category>office</category>
        <handle>sip:jmiller@abc.com</handle>
        <label>Miller</label>
        <altLabel>John</altLabel>
      </contact>
    </contactAddresses>
    <addresses>
  <!--
      ---addressType:The unique text name of the address type.
          Possible values are:   Home, business.
      ---name: The Name property defines the unique label by which the address is
          known. Default format for user specific address should include user
          name place address type.
      ---building:The name or other designation of a structure.
      ---localityName:The name of a locality, such as a city, county or other
          geographic region.
      ---postalCode:A code used by postal services to route mail to a destination.
          In the United States this is the zip code.
      ---room:Name or designation of a room.
      ---stateOrProvince:The full name of a state or province.
      ---country:A country.
      ---street:The physical address of the object such as an address for package
          delivery
      ---postalAddress:A free formed text area for the complete physical delivery
          address. It may be used in place of the specific fields in this table.
  -->
      <address>
        <addressType>office</addressType>
        <name>John Miller</name>
        <building>building A</building>
        <localityName>Magarpatta</localityName>
        <postalCode>411048</postalCode>
        <room>room 123</room>
        <stateOrProvince>MH</stateOrProvince>
        <country>India</country>
        <street>Hadapsar</street>
        <private>false</private>
      </address>
```

```
      </addresses>
    </tns:publicContact>
    <!--
        ---addressType:The unique text name of the address type.
            Possible values are:   Home, business.
        ---name: The Name property defines the unique label by which the address is
            known. Default format for user specific address should include user
            name place address type.
        ---building:The name or other designation of a structure.
        ---localityName:The name of a locality, such as a city, county or other
            geographic region.
        ---postalCode:A code used by postal services to route mail to a
            destination. In the United States this is the zip code.
        ---room:Name or designation of a room.
        ---stateOrProvince:The full name of a state or province.
        ---country:A country.
        ---street:The physical address of the object such as an address for package
            delivery
        ---postalAddress:A free formed text area for the complete physical delivery
            address. It may be used in place of the specific fields in this table.
        ---readOnly:A boolean indicator showing whether or not the address can be
            changed from its default value.
    -->
  <tns:sharedAddress>
      <addressType>office</addressType>
      <name>Avaya Pune</name>
        <building>building A</building>
         <localityName>Magarpatta</localityName>
         <postalCode>411048</postalCode>
        <room>room 123</room>
        <stateOrProvince>MH</stateOrProvince>
         <country>India</country>
         <street>Hadapsar</street>
         <readOnly>true</readOnly>
    </tns:sharedAddress>


</tns:globalSettings>
```

XML Schema Definition for bulk deletion of global setting records

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/bulkdelete" targetNamespace="http://
xml.avaya.com/schema/bulkdelete"
            elementFormDefault="qualified" version="1.0" xmlns:xs="http://www.w3.org/2001/
XMLSchema">


    <xs:element name="sharedAddress" type="tns:xmlDeleteSharedAddress"/>
    <xs:element name="publicContact" type="tns:xmlDeletePublicContact" />
    <xs:element name="presenceEnforcedUserACL"
type="tns:xmlDeletePresEnforcedUserACLEntry"/>
    <xs:element name="presenceSystemRule" type="tns:xmlDeletePresSystemRule"/>
    <xs:element name="presenceSystemACL" type="tns:xmlDeletePresSystemACLEntry"/>


    <xs:element name="deleteGlobalSettings">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="sharedAddress" type="tns:xmlDeleteSharedAddress"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="publicContact" type="tns:xmlDeletePublicContact"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="presenceEnforcedUserACL"
type="tns:xmlDeletePresEnforcedUserACLEntry" minOccurs="0" maxOccurs="unbounded"/>
```

```
            <xs:element name="presenceSystemRule" type="tns:xmlDeletePresSystemRule"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="presenceSystemACL" type="tns:xmlDeletePresSystemACLEntry"
minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
   </xs:element>

   <xs:complexType name="xmlDeleteSharedAddress">
        <xs:sequence>
            <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlDeletePublicContact">
        <xs:sequence>
            <xs:element name="displayName" type="xs:string" maxOccurs="1" minOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlDeletePresEnforcedUserACLEntry">
        <xs:sequence>
            <xs:element name="userName" type="xs:string" maxOccurs="1" minOccurs="1"/>
            <xs:choice>
                <xs:element name="watcherLoginName" type="xs:string" minOccurs="0"/>
                <xs:element name="watcherDisplayName" type="xs:string" minOccurs="0"/>
            </xs:choice>
            <xs:element name="priority" type="xs:string" maxOccurs="1" minOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlDeletePresSystemRule">
        <xs:sequence>
                    <xs:element name="priority" type="xs:string" maxOccurs="1"
minOccurs="1"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="xmlDeletePresSystemACLEntry">
        <xs:sequence>
            <xs:choice>
                <xs:element name="watcherLoginName" type="xs:string" minOccurs="0"/>
                <xs:element name="watcherDisplayName" type="xs:string" minOccurs="0"/>
            </xs:choice>
        </xs:sequence>
    </xs:complexType>

</xs:schema>
```

Sample XML for bulk deletion of global setting records

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:deleteGlobalSettings xmlns:tns="http://xml.avaya.com/schema/bulkdelete"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
xml.avaya.com/schema/bulkdelete systemPresence_delete.xsd ">

     <tns:presenceSystemRule>
        <tns:priority>LOW</tns:priority>
    </tns:presenceSystemRule>

      <tns:sharedAddress>
        <tns:name>Avaya Pune</tns:name>
      </tns:sharedAddress>

      <tns:publicContact>
```

```
        <tns:displayName>John Miller</tns:displayName>
      </tns:publicContact>

      <tns:presenceEnforcedUserACL>
        <tns:userName>jmiller@avaya.com</tns:userName>
        <tns:watcherDisplayName>John Miller</tns:watcherDisplayName>
        <tns:priority>HIGH</tns:priority>
      </tns:presenceEnforcedUserACL>

      <tns:presenceSystemACL>
           <tns:watcherDisplayName>John Miller</tns:watcherDisplayName>
      </tns:presenceSystemACL>

</tns:deleteGlobalSettings>
```

XML Schema Definition for bulk import of roles

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns="http://xml.avaya.com/bulkimport" xmlns:xs="http://www.w3.org/2001/
XMLSchema" targetNamespace="http://xml.avaya.com/bulkimport"
elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            This Schema defines schema for bulk import and export of roles.
             Root Element 'Roles' represent collection of role
              (containing 1 or more roles)
        </xs:documentation>
    </xs:annotation>
    <xs:element name="Roles">
        <xs:complexType>
            <xs:sequence>
                <xs:annotation>
                    <xs:documentation xml:lang="en">
                         A role is a collection of access permissions on a resource.
                         A user's role will determine the permissions that the user
                         receives to access resources.
                         Examples of Roles: Contact Center Manager, Agent,
                         Administrator.
                         New Roles can be added to the data model using an XML file
                         conforming to this XSD.Existing Roles too can be updated.
                    </xs:documentation>
                </xs:annotation>
    <xs:element name="Role" maxOccurs="unbounded">
        <xs:complexType>
            <xs:sequence>
                <xs:annotation>
                    <xs:documentation xml:lang="en">
                        Operation - Element Containing information about the
                            Operation.The Operation requires to preexist in
                            SMGR database.
                            Examples of Operation:
                            'UserManagement/GlobalUserSettings/ACL';
                            'Settings/Plugin Framework' ;
                        Resource - Element Containing information about the
                            Resource.
                            A Resource can be a User, Role, Operation, Group,
                            Element. The Resource requires to preexist in SMGR
                            database. Examples of Resource:  'Auditor' ;
                    </xs:documentation>
                </xs:annotation>
    <xs:element name="Operation" minOccurs="0" maxOccurs="unbounded">
        <xs:complexType>
            <xs:attribute name="ID" type="xs:string" use="required">
                <xs:annotation>
                    <xs:documentation xml:lang="en">
```

```
                        ID: The ID of the operation.The value of this tag
                            corresponds to the OperationID. Note that it
                            is very important that this value is unique
                            across the system.
                    </xs:documentation>
                </xs:annotation>
            </xs:attribute>
        </xs:complexType>
    </xs:element>
    <xs:element name="Resource" minOccurs="0" maxOccurs="unbounded">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="ResourceAttributes" minOccurs="0" maxOccurs="unbounded">
                    <xs:complexType>
                        <xs:attribute name="ID" type="xs:string" use="required">
                            <xs:annotation>
                                <xs:documentation xml:lang="en">
                                    ResourceAttributesID: The ID of the Resource
                                        Attributes. This specifies the attributes
                                        of a resource.
                                        Examples of    ResourceAttributesID:
                                        'ALL' ; 'LoginName' ;
                                        'First Name' for Resource Type 'user'
                                </xs:documentation>
                            </xs:annotation>
                        </xs:attribute>
                    </xs:complexType>
                </xs:element>
                <xs:element name="Permissions">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:annotation>
                                <xs:documentation xml:lang="en">
                                    Permission: String value specifying Permissions
                                        that can be assigned to the Resource Type.
                                        Examples of Permission: view,delete
                                </xs:documentation>
                            </xs:annotation>
                <xs:element name="Permission" type="xs:string" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
            </xs:element>
                </xs:sequence>
                    <xs:attribute name="ResourceType" type="xs:string" use="required">
                         <xs:annotation>
                            <xs:documentation xml:lang="en">
                                ResourceType: String Value for specifying Type
                                    of the Resource that needs to be imported.
                            </xs:documentation>
                        </xs:annotation>
                    </xs:attribute>
                    <xs:attribute name="NativeResourceID" type="xs:string" use="required">
                        <xs:annotation>
                            <xs:documentation xml:lang="en">
                                NativeResourceID: Native ID of the Resource.
                            </xs:documentation>
                        </xs:annotation>
                    </xs:attribute>
        </xs:complexType>
            </xs:element>
                </xs:sequence>
                    <xs:attribute name="CanAccessAllOperations" type="xs:boolean"
use="required">
                        <xs:annotation>
                            <xs:documentation xml:lang="en">
```

```
                                CanAccessAllOperations - Boolean value specifying
                                whether this role can access all operations.
                            </xs:documentation>
                        </xs:annotation>
                    </xs:attribute>
                    <xs:attribute name="IsServices" type="xs:boolean" use= "required" >
                        <xs:annotation>
                            <xs:documentation xml:lang="en">
                                IsServices - Boolean value specifying whether this
                                Role is a  Services Role.
                            </xs:documentation>
                        </xs:annotation>
                    </xs:attribute>
                    <xs:attribute name="isDefault" type="xs:boolean" use="required">
                        <xs:annotation>
                             <xs:documentation xml:lang="en">
                                 isDefault - Boolean value specifying whether
                                this Role is a  System Role.These Roles can
                                not be deleted.
                            </xs:documentation>
                        </xs:annotation>
                    </xs:attribute>
                    <xs:attribute name="Name" type="xs:string" use="required">
                        <xs:annotation>
                            <xs:documentation xml:lang="en">
                                      Name - String value specifying Role name.
                            </xs:documentation>
                        </xs:annotation>
                    </xs:attribute>
                    <xs:attribute name="AllResourcesPermission" type="xs:string"
use="optional">
                        <xs:annotation>
                            <xs:documentation xml:lang="en">
                                AllResourcesPermission - String value representing
                                    the comma separated permission strings. These
                                    permissions will be applied to all Resources
                                    in the system. The users assigned to this role
                                    will get the specified permissions for all
                                    resources.
                                    Examples of Resource:'view,delete'
                            </xs:documentation>
                        </xs:annotation>
                    </xs:attribute>
                    <xs:attribute name="Description" type="xs:string" use="optional">
                        <xs:annotation>
                            <xs:documentation xml:lang="en">
                                Description - String value specifying Role
                                    description.
                            </xs:documentation>
                        </xs:annotation>
                    </xs:attribute>
                    <xs:attribute name="isNHIRole" type="xs:boolean" use="required">
                        <xs:annotation>
                            <xs:documentation xml:lang="en">
                                isNHIRole - Boolean value specifying whether this
                                    Role is a  non human interface (nhi) role.
                            </xs:documentation>
                        </xs:annotation>
                    </xs:attribute>
                    <xs:attribute name="shareRoles" type="xs:boolean" use="optional">
                        <xs:annotation>
                            <xs:documentation xml:lang="en">
                                shareRoles - Boolean value specifying whether this
                                    Role is a  shared role across applications.
                            </xs:documentation>
```

```
                    </xs:annotation>
                </xs:attribute>
                <xs:attribute name="hasFullAccess" type="xs:boolean" use="optional">
                    <xs:annotation>
                        <xs:documentation xml:lang="en">
                              hasFullAccess - Boolean value specifying full
                             access over all resources.
                             Examples of Role with full access:
                             'System Administrator';
                        </xs:documentation>
                    </xs:annotation>
                </xs:attribute>
                <xs:attribute name="ApplicationId" type="xs:string" use="required">
                     <xs:annotation>
                        <xs:documentation xml:lang="en">
                            ApplicationId - The value of this tag corresponds
                                to the ApplicationID.
                                Examples of ApplicationId: 'SMGR';
                        </xs:documentation>
                    </xs:annotation>
                </xs:attribute>
            </xs:complexType>
        </xs:element>
    </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

Sample XML for bulk import of roles

```
&lt;?xml version="1.0" encoding="UTF-8"?>
<!--
    Root Element 'Roles' represent collection of role
    (containing 1 or more roles)
-->
<Roles xsi:schemaLocation="http://xml.avaya.com/bulkimport BulkImport.xsd" xmlns="http://
xml.avaya.com/bulkimport" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <!--
        A role is a collection of access permissions on a resource. A user's role
        will determine the permissions that the user receives to access resources.
    ---CanAccessAllOperations: Boolean value specifying whether this role can
                access all operations.
    ---IsServices: Boolean value specifying whether this Role is a  Services Role.
    ---isDefault: Boolean value specifying whether this Role is a  System Role.
                These Roles can not be deleted.
    ---Name: String value specifying Role name.
    ---AllResourcesPermission:String value representing the comma separated
                permission strings. These permissions will be applied to all
                Resources in the system. The users assigned to this role will get
                the specified permissions for all resources.
    ---Description:String value specifying Role description.
    ---isNHIRole:Boolean value specifying whether this Role is a non human interface
                (nhi) role.
    ---shareRoles: Boolean value specifying whether this Role is a  shared role
                across applications.
    ---hasFullAccess:Boolean value specifying full access over all resources.
    ---ApplicationId:The value of this tag corresponds to the ApplicationID.
                  Examples of ApplicationId: 'SMGR'
    -->
    <Role CanAccessAllOperations="true" IsServices="true" isDefault="false" Name="test-
role" AllResourcesPermission="view,delete" Description="System Administrator Role"
isNHIRole="false" shareRoles="true" hasFullAccess="false"           ApplicationId="SMGR"
>
    <!--
        Element Containing information about the Operation.The Operation requires
```

```
        to preexist in SMGR database.
        ---ID: The ID of the operation.The value of this tag corresponds to the
            OperationID. Note that it is very important that this value is
            unique across the system
    -->
         <Operation ID="GroupsAndRoles/RBAC/ViewRole"/>
             <!--
                ---Resource : Element Containing information about the Resource.
                            A Resource can be a User, Role, Operation, Group,
                            Element.The Resource requires to preexist in SMGR
                            database.
                ---ResourceType: String Value for specifying Type of the Resource
                               that needs to be imported.
                ---NativeResourceID: Native ID of the Resource.
            -->
            <Resource ResourceType="alarmoperation"
NativeResourceID="ChangeStatusAll">
            <!--
                ResourceAttributesID: The ID of the ResourceAttributes.
                                    This specifies the attributes of a resource
            -->
        <ResourceAttributes ID="ALL" />
            <!--
                ---Permission: String value specifying Permissions that can be
                         assigned to the Resource Type.
            -->
            <Permissions>
            <Permission>view</Permission>
        </Permissions>
        </Resource>
    </Role>
</Roles>
```

Attribute details defined in Import user XSD

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
authenticationType	The type of authentication the user undergoes at runtime to gain access to the system.	Mandatory	Possible values: • BASIC • ENTERPRISE
description	A description of the user. A human readable description of this user instance.	Optional	
displayName	The localized name of the user to be used when displaying. Typically, the value is the localized full name. This value might be provisioned from the enterprise directory entry of the user. If the value does not exist, you can use synchronization rules to populate the value for	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	other fields. For example: Surname, GivenName, or LoginName.		
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.
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.	Optional	Default value is false.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	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.		
givenName	The first name of the user.	Mandatory	
honorific	The personal title used to address a user. This is typically a social title and not the work title which is contained in the title attribute. This attribute can map to PersonalTitle.	Optional	
loginName	The unique login name that you provide for the user. The format for the login name is username@domain. The login 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	
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	Optional	Possible values: • English (United States) - en_US • Chinese (Simplified) - zh_CN

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	locale of the client must be used. If the value is blank, en_US must be used as default.		• 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.
status	The information that helps provisioning activities such as correcting or completing the provisioning of a user. It can also signify that approval is needed (PENDINGAUTHZ) before a user account is sufficiently configured to be a valid user (PROVISIONED).	Optional	Possible values: AUTHPENDING; PENDINGAUTHZ; PROVISIONED
suffix	The text appended to a name. For example, Jr., III.	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
surname	The last name or the family name of the user.	Mandatory	
timeZone	The preferred time zone of the user. For example: America/New_York, Europe/Dublin. The application consuming this information must know how to translate e.g. in Java it is TimeZone.getTimeZone("Europe/Moscow"); In the absence of a value, the system uses the local services timezone. **Note:** You must consider daylight saving time (DST) and summer time adjustments while using the suggested values for **timeZone**. Typically, you add 1 hour to the offset. **Note:** You cannot use the following characters as is in the xml. Make the following modifications while using them in the import xml files: • 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 (+8:0)Beijing, Hong Kong, Singapore; Taipei

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			(+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	
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	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	CommProfile SIP and non SIP. This attribute is shared across different communication profiles and thus different communication services.		
userType	The possible primary user application types. A User can be associated with multiple user types.	Optional	Possible values are administrator, communication_user, agent, supervisor, resident_expert, service_technician, lobby_phone
roles	The text name of a role. This value must be available in the System Manager database.	Optional	
address	The address of the user.	Optional	
securityIdentity	The SecurityIdentity is used to hold any additional identities for a user that can be used for authentication such as loginName, Kerberos account name, or X509 certificate name.	Optional	
ownedContactLists	It is a collection of internal or external contacts. ContactList is owned by a specific user and has a name that a unique name within the context of its owner.	Optional	The system creates a default contactlist per user.
ownedContacts	A non-Avaya application user (external) contact. Contacts can be collected together along with User entities into a contact list. Contacts can be created by an administrator or an end user.	Optional	
presenceUserDefault	The personal rules that are set by presentities to define how much presence information can be shown to watchers that are not explicitly mentioned in an ACL. There can be one User Default rule per presentity (User), or none.	Optional	
presenceUserACL	The personal rules defined by presentities themselves on who can monitor their presence information. There might be	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	several entries in the list for a given presentity, each entry corresponding to one watcher.		
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.
employeeNo	The employee number of the user.	Optional	
department	The department which the employee belongs to.	Optional	
organization	The organization which the employee belongs to.	Optional	
localizedNames	The localized name of the user.	Optional	

Attribute details defined in Delete User XSD

Attribute	Attribute description	Mandatory/Optional	Validation constraints
deleteType	Defines the delete type of the user. If the user selects: • soft: The system does not delete the user record permanently. You can recover the user record. • permanent: The system permanently deletes all attributes associated with the user and the links to public contacts and shared addresses.	Mandatory	Possible values: • soft • permanent
loginName	A unique system login name assigned to the user in the format username@domain or username.	Mandatory	
id	A unique identifier for a user record. The id attribute is included in the XSD for future enhancement. This is not used in System Manager the current release.	Optional	

Attribute details defined in the CM Endpoint profile XSD

Attribute details defined in the CM Endpoint profile XSD

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
CM Name cmName	The name of the Communication Managersystem as it appears in the Applications/Application Management/Entities.	Mandatory	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Use Existing Extension useExistingExtension	Select **true** if you want to use an already created extension. Select **false** if you want to use an available extension.	Optional	
Template Name template	The template name that is used to create the endpoint. Values defined in the template will be used if you do not provide other values.	Optional	
Set Type setType	The set type of the endpoint.	Optional	
Port port	The valid port value.	Optional	01 to 64 First and second numbers are the cabinet numbers having values A to E. The third character is the carrier having values between 01 to 20. Fourth and fifth characters are the slot number between 01 to 32. Sixth and seventh characters are the circuit number having values x or X. Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension has a non-IP set, or that the extension had a non-IP set, and is 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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			since the switch was set up, and the administrator expects that the extension has an IP set. This is autopopulated for certain IP endpoint set types. You can enter the value for a DCP set with softphone permissions. This changes to the s00000 type when the set registers.
Delete endpoint is unassigned deleteOnUnassign	Specifies whether the endpoint must be deleted if it is unassigned from the user.	Optional	
Lock messages feature. lockMessages	Select to enable the lock messages feature.	Optional	Select true or false to enable or disable the lock messages feature respectvely.
Coverage Path 1 coveragePath1	A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call.	Optional	Valid values: Path Number between 1-9999, time of day table between t1-t999, or blank.
Coverage Path 2	A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call.	Optional	Valid values: Path Number between 1-9999, time of day table between t1-t999, or blank.
Hunt To Station huntToStation	The extension the system must hunt to for this telephone when the telephone is busy. A endpoint hunting chain can be created by assigning a hunt-to 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	Mandatory	Valid values: 1 to 250

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	building or multiple departments within a company or an organization.		
Class of Restriction cor	This is used for multiple tenants in a building or multiple departments within a company or an organization.	Mandatory	Valid values: 0 to 995
Class of Service cos	Class of Service lets you define a group of users and control the groups' access to features.	Mandatory	Valid values: 0 to 15
speakerphone	Controls the behavior of speakerphones.	Optional	Valid values : none, 1-way, 2-way
Display Language displayLanguage	The language that displays on the endpoint.	Optional	Time of day is displayed in the 24- hour format (00:00 - 23:59) for all languages except English, which is displayed in the 12-hour format (12:00 a.m. to 11:59 p.m.). unicode: Displays English messages in a 24-hour format . If you do not install the Unicode file, the endpoint displays messages in English by default.
Personalized Ringing Pattern personalizedRingingPattern	The personalized ringing pattern for the endpoint. Personalized Ringing allows the users of some telephones to have one of the eight ringing 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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			8. LHL
Message Lamp Extension messageLampExt	The Message Lamp Extension associated with the current extension.	Mandatory	
muteButtonEnabled	Select to enable the mute button on the endpoint.		
Media Complex Extension mediaComplexExt	When used with Multi-media Call Handling, this field indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to either place a voice or a data call. Voice conversion, coverage, and forwarding apply as if the call were made to the 1-number.	Optional	Valid Entry Usage: A valid BRI data extension. For MMCH, enter the extension of the data module that is part of this multimedia complex. H.323 endpoint extension: For the 4600 series IP Telephones, enter the corresponding H.323 endpoint. For IP Softphone, enter the corresponding H.323 endpoint. If you enter a value in this field, you can register this endpoint on either a road-warrior or elecommuter/Avaya IP Agent application. Blank: Leave this field blank for single-connect IP applications.
IP Softphone ipSoftphone	Specifies whether the endpoint is an IP soft phone.	Optional	
Servivable GK Node Name survivableGkNodeName	Survivable GK Node Name identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the H.248 gateways.	Optional	Valid Entry Usage: Valid IP node name, any valid, previously-administered IP node name.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	When you enter a valid IP node name in this field, Communication Manager adds the IP address of this gateway to the bottom of the Alternate Gatekeeper List for this IP network region. As H.323 IP endpoints register with Communication Manager, this list is sent to the registration confirm message. The IP endpoint can use the IP address of this Survivable Gatekeeper as the call controller of last resort to register with. Survivable GK Node Name is available only if the endpoint is an H.323 endpoint (46xxor 96xx set types).		
Survivable class of restriction survivableCOR	Sets the level of restriction for endpoints to be used with the survivable dial plan to limit certain users to certain types of calls. You can list the restriction levels from the most restrictive to least restrictive. Each level assumes the calling ability of the ones above it. This field is used by the PIM module in Integrated Management to communicate with the Communication Manager 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	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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	H.248 gateways. Survivable COR is valid for all analog and IP endpoint types.		unrestricted - This endpoint can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users.
Survivable Trunk Destination survivableTrunkDest	This field does not allow certain telephones to receive incoming trunk calls when the media gateway is in survivable mode. This field is used by the PIM module in Integrated Management to successfully interrogate the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for SLS on the H. 248 gateways. Survivable Trunk Destination is available for all analog and IP endpoint types.	Optional	Valid Entry Usage: true - Allows this endpoint to be an incoming trunk destination while the media gateway is running in the survivability mode. This is the default value. false - Prevents this endpoint from receiving incoming trunk calls when the endpoint in survivable mode.
Voice Mail Number voiceMailNumber	Enter the complete Voice Mail Dial Up number.	Optional	String
offPremisesStation	Analog telephones only.	Optional	Valid entries Usage: • true - Enter true if this telephone is not located in the same building as the system. If you enter true, you must complete the R Balance Network. • false - Enter false if the telephone is located in the same building as the system.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
dataOption	If a second line on the telephone is administered on the I-2 channel, enter `analog`. Else, enter the data module if applicable, or enter `none`.	Optional	Valid entries: analog, none.
Message Waiting Indicator messageWaitingIndicator	If you select led or neon, then you must enable messageLampExt, else leave this field blank.	Optional	Valid entries: led, neon, none.
remoteOfficePhone	Select **true** to use this endpoint as an endpoint in a remote office configuration.	Optional	Valid entries: • audix - If LWC is attempted, the messages are stored in AUDIX. • spe - If LWC is attempted, the messages are stored in the system processing element (spe). • none - If LWC is attempted, the messages are not stored.
lwcActivation	Select true to allow internal telephone users to leave short LWC messages for this extension. If the system has hospitality, select true for guest-room telephones for the designated extensions to receive failed wakeup messages, and to receive LWC messages that indicate the wakeup calls failed. Select true if LWC Reception is audix.	Optional	Boolean
activeStationRinging	Active endpoint ringing	Optional	Valid entries: • single • continuous • if-busy-single

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			• silent
idleActiveRinging	Defines how a call rings to the telephone when it is on-hook.	Optional	Valid entries • continuous - Select continuous to cause all calls to this telephone to ring continuously. • if-busy-single - Select if-busysingle to cause calls to this telephone to ring continuously when the telephone is off-hook and idle, and calls to this telephone to receive one ring cycle and then ring silently when the telephone is off-hook and active. • silent-if-busy - Select silent-if-busy to cause calls to ring silently when this endpoint is busy. • single - Select single to cause calls to this telephone to receive one ring cycle and then ring silently.
switchhookFlash	Set this field to true when the **Type** field is set to H.323.	Optional	Boolean
ignoreRotaryDigits	If you set this field to true, the short switch-hook flash (50 to 150) from a 2500-type set is ignored.	Optional	Boolean
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	Optional	Boolean

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	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.		
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	Optional	Valid entries: as-needed permenant

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	multimedia call is answered by the endpoint and for a period of 10 seconds after the last multimedia call on the endpoint has been disconnected. Having the service link stay connected for 10 seconds allows a user to disconnect a multimedia call and then make another multimedia call without having to wait for the service link to disconnect and reestablish. • Permanent – Multimedia call center agents and other users who are constantly making or receiving multimedia calls might want to be administered with this service link mode. The permanent mode service link will be connected during the endpoint's first multimedia call and will remain in a connected state until the user 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		

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	mode endpoint or a multimedia call that has been early answered.		
multimediaMode	There are two multimedia modes, Basic and Enhanced.	Optional	Basic - A basic multimedia complex consists of a BRIconnected multimedia-equipped PC and a non-BRI-connected multifunction telephone set. Enhanced - An enhanced multimedia complex consists of a BRI-connected multimediaequipped PC and a non-BRIconnected multifunction telephone.
mwiServedUserType	Controls the auditing or interrogation of a served user's message waiting indicator (MWI).	Optional	Valid entries: 1. fp-mwi - Select this option if the endpoint is a served user of an fp-mwi message center. 2. qsig-mwi - Select this option if the endpoint is a served user of a qsig-mwi message center. 3. sip adjuncts - Select this option if the endpoint is a served user of a sip adjunct message center. 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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
audixName	The AUDIX associated with the endpoint. Must contain a user-defined adjunct name that was previously administered.	Optional	String
automaticMoves	Automatic Moves allows a DCP telephone to be unplugged from one location and moved to a new location without additional Communication Manager administration. Communication Manager automatically associates the extension to the new port.	Optional	Valid entries: 1. always - Select always to move the DCP telephone anytime without additional administration by unplugging the telephone from one location and plugging it into a new location. 2. once - Select once to unplug and plug the DCP telephone into a new location once. After a move, the field is set to done the next time that routine maintenance runs on the DCP telephone. Use once when you want to move a large number of DCP telephones so that each extension is removed from the move list. Use once to prevent automatic maintenance replacement. 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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			the telephone is moved and routine maintenance runs on the DCP telephone. 5. Error - Error is a display-only value. Communication Manager sets the field to error, after routine maintenance runs on the DCP telephone, when a non-serialized telephone is set as a movable telephone.
remoteSoftphoneEmergencyCalls	An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks.	Optional	Valid entries: 1. As-on-local: As-on-local sends the extension entered in the Emergency Location Extension field on the Endpoint screen to the Public Safety Answering Point (PSAP) 2. Block - Block prevents the completion of emergency calls. 3. Cesid - Cesid allows Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP. 4. Option - Option allows the user to select the option (extension, block, or cesid) that the user selected during registration.
emergencyLocationExt	This field allows the system to properly	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	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 Safety Answering Point (PSAP).		
alwaysUse	A softphone can register no matter what	Optional	Boolean

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	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.		
precedenceCallWaiting	Activates or deactivates Precedence Call Waiting for this endpoint.	Optional	
autoSelectAnyIdleAppearance	Enables or disables automatic selection of any idle appearance of transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being 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	Optional	Boolean

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	Calling (LWC) messages for this telephone. Applies only if the telephone is enabled for LWC Reception.		
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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			3. none: All calls ended to this endpoint receive an audible ringing treatment. 4. icom: Allows a telephone user to answer an intercom call from the same intercom group without pressing the intercom button.
dataRestriction	Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Data restriction cannot be assigned if Auto Answer is administered as all or acd. If enabled, whisper page to this endpoint is denied.	Optional	
idleAppearancePreference	Indicates which call appearance is selected when the user lifts the handset and there is an incoming call.	Optional	true - The user connects to an idle call appearance instead of the ringing call. false - The Alerting Appearance Preference is set and the user connects to the ringing call appearance.
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	Optional	Boolean

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	enable or disable attendant call waiting		
distinctiveAudibleAlert	Select true so that the telephone can receive the three different types of ringing patterns which identify the type of incoming calls. Distinctive ringing might not work properly for off-premises telephones.	Optional	
restrictLastAppearance		Optional	Valid entries: 1. true: Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only. 2. false: Last idle call appearance is used for incoming priority calls and outgoing call originations.
adjunctSupervision	Enable or disable Adjunct Supervision.	Optional	Valid entries: 1. true: Analog disconnect signal is sent automatically to the port after a call ends. Analog devices such as answering machines and speakerphones use this signal to 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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			auto-answer endpoint when a call is queued for the endpoint.
perStationCpnSendCallingNumber	Send Calling Number	Optional	Valid entries: 1. y: All outgoing calls from the endpoint will deliver the Calling Party Number (CPN) information as Presentation Allowed. 2. n: No CPN information is sent for the call. 3. r: Outgoing non-DCS network calls from the endpoint will deliver the Calling Party Number information as Presentation Restricted.
busyAutoCallbackWithoutFlash	Appears on the Endpoint screen for analog telephones, only if the Without Flash field in the ANALOG BUSY AUTO CALLBACK section of the Feature-Related System Parameters screen is set to true. The 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
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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			2. false: The line selection on an on-hook endpoint with no alerting calls can be moved to a different line button, which might be serving a different extension.
coverageAfterForwarding	Specifies whether an unanswered forwarded call is provided coverage treatment.	Optional	
directIpIpAudioConnections	Select to allow or deny direct audio connections between IP endpoints.	Optional	
ipAudioHairpinning	Allows IP endpoints to be connected through the server's IP circuit pack.	Optional	
primeAppearancePreference	Set prime appearance preference.	Optional	
endpointSiteData	This is applicable for Site Data fields		
room	This is a Site Data field.	Optional	Max length 10
jack	This is a Site Data field.	Optional	Max length 5
cable	This is a Site Data field.	Optional	Max length 5
floor	This is a Site Data field.	Optional	
building	This is a Site Data field.	Optional	
headset	This is a Site Data field.	Optional	
speaker	This is a Site Data field.	Optional	
mounting	This is a Site Data field.	Optional	Valid values d, w.
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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
number	This is a Station Abbreviated Dialing Data field.	Mandatory	A number.
buttons	This is applicable for button data.	Optional	
Number	This is a button data field.	Mandatory	
Type	This is a button data field.	Optional	
data1	This is a button data field.	Optional	
data2	This is a button data field.	Optional	
data3	This is a button data field.	Optional	
data4	This is a button data field.	Optional	
data5	This is a button data field.	Optional	
data6	This is a button data field.	Optional	
endpointDataModule	This is a Station Data module field.	Optional	
dataExtension	This is a Station Data module field.	Mandatory	
name	This is a Station Data module field.	Optional	Max length 29
Class of restriction cor	This is a Station Data module field.	Mandatory	Valid range from 0 to 995.
Class of Service Cos	This is a Station Data module field.	Mandatory	Valid range from 0 to 15.
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

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			3. personal 4. system
listId	This is a Station Data module field.	Optional	
specialDialingOption	This is a Station Data module field.	Optional	Valid values: 1. default 2. hot-line
specialDialingAbbrDialCode	This is a Station Data module field.	Optional	
hotLineDestAbbrevList	This is a Station Hot Line Data field.	Optional	Valid range 1 to 3
hotLineAbbrevDialCode	This is a Station Hot Line Data field.	Optional	Numeric string
nativeName	This is a Native Name Data field.	Optional	
locale	This is a Native Name Data field. **Note:** If the **displayName**, **givenName**, or **surname** contains characters of multiple scripts then the locale tag should be present. The locale for the multiscript languages are: • Japanese: **ja** • Simplified Chinese: **zh-cn** • Traditional Chinese: **zh-tw** • Korean: **ko-kr** • Vietnamese: **vi-vn** The locale tag is case sensitive. You can use the preferredLanguage tag to specify the locale if	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	displayName, nativeName, and Name are in multibytes. If the locale tag is present in the xml, locale tag is preferred over the preferredLanguage tag.		
Name	This is a Native Name Data field.	Mandatory	Max length 27

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	
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	Optional	The default value is 1.

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	IDs are used to control message sending and receiving among groups of subscribers.		
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
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	Optional	

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	50 digits and can contain the Mailbox Number.		
pbxExtension	This is field of Messaging specific data. The primary telephone extension of the subscriber.	Optional	
telephoneNumber	This is field of Messaging specific data. The telephone number of the subscriber as displayed in address book listings and client applications.	Optional	The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses ([) and (]).
asciiVersionOfName	This is field of Messaging specific data. If the subscriber name is entered in multibyte character format, then this field specifies the ASCII translation of the subscriber name.	Optional	
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.	Optional	

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	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.		
personalOperatorSchedule	This is field of Messaging specific data. Specifies when to route calls to the backup operator mailbox. The default value for this field is Always Active.	Optional	
tuiMessageOrder	This is field of Messaging specific data. Specifies the order in which the subscriber hears the voice messages.	Optional	You can choose one of the following: • urgent first then newest: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. 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.

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
			• newest messages first: to direct the system to play messages in the reverse order of how they were received.
intercomPaging	This is field of Messaging specific data. Specifies the intercom paging settings for a subscriber.	Optional	You can choose one of the following: • paging is off: to disable intercom paging for this subscriber. • paging is manual: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber. • paging is automatic: if the TUI automatically allows callers to page the subscriber.
voiceMailEnabled	This is field of Messaging specific data. Specifies whether a subscriber can receive messages, e-mail messages and callanswer messages from other subscribers. You can choose one of the following: - yes: to allow the subscriber to create, forward, and receive messages. - no: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address	Optional	

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	messages to the subscriber.		
miscellaneous1	This is field of Messaging specific data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.		Max length 51
miscellaneous2	This is field of Messaging specific data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.		Max length 51
miscellaneous3	This is field of Messaging specific data. Specifies additional, useful information about 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
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.

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
			• Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.
accountCode	This is field of CMM data. Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.	Optional	
coveringExtension	This is field of CMM data. Specifies the number to be used as the default destination for the Transfer Out of Messaging feature.	Optional	You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.
miscellaneous1	This is field of CMM data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.	Optional	Max length 11
Miscellaneous2	This is field of CMM data. Specifies additional, useful information about a subscriber. Entries in this field are for	Optional	Max length 11

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	convenience and are not used by the messaging system.		
Miscellaneous2	This is field of CMM data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.	Optional	Max length 11
Miscellaneous4	This is field of CMM data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.	Optional	Max length 11

Attribute details defined in the Session Manager communication profile XSD

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
Primary Session Manager primarySM	Specify the name of the Session Manager instance that must be used as the home server for a Communication Profile. As a home server, the primary Session Managerinstance is used as the default access point for connecting devices associated with the Communication Profile to the Aura network.	Mandatory	-
Secondary Session Manager	If a secondary Session Manager instance is	Optional	-

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
secondarySM	specified, this Session Manager provides continued service to SIP devices associated with this communication profile when the primary Session Manageris not available.		
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 in the event that 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	Optional	-

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	must be the main Communication Manager for the Communication Manager remote survivability server resident with the Branch Session Manager.		
Max. Simultaneous Devices maxSimultaneousDevices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.		
Block New Registration When Maximum Registrations Active blockNewRegistrationWhenMaxActive	Set the value to true or false. If you do not set the attribute, the system sets the attribute to false, the default. 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.		
Origination Application Sequence originationAppSequence	Specify an Application Sequence that will be	Optional	-

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	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.		
Termination Application Sequence terminationAppSequence	Specify an Application Sequence that will be 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	-
Home Location homeLocation	Specify a Home Location (the name of a Location – navigate to Routing > Locations) to support mobility for a user. When this user calls numbers that are not associated with an administered user, dial-plan rules	Mandatory	-

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	(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.		
Conference Factory Set confFactorySet	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.	Optional	-

Attribute details defined in the Avaya Aura® Conferencing profile XSD

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
User Template template	Specify the name of the User Template. User Templates are created in Avaya Aura Conferencing Provisioning Client. The following default templates always exist: executive, desktop_user_with_video, desktop_user_no_video, desktop_user_low_priority, guest_user_no_video, event_1000, event_2000, event_3000.	Mandatory	-

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Location location	Specify location for the user. Location is a mandatory field. However, Conferencing can get the value of location from the **Location** field in Conferencing Profile. Conferencing can also get the value of location from the **Home Location** field in Session Manager Profile if Session Manager profile is configured and the location in Conferencing Profile is not configured.	Mandatory	-
Participant Security Code securityCode	The participant code for the chairperson bridge.	Mandatory if the autoGeneratedCodeLength parameter is not set.	-
Moderator Security Code moderatorPin	The unique participant code that you use to login to a conference as a moderator.	Mandatory if the autoGeneratedCodeLength parameter is not set.	-
Auto Generated Participant and Moderator Security Codes Length autoGeneratedCodeLength	This parameter shows that Participant and Moderator Security Codes must be auto-generated and must specify the length of such auto-generated codes.	Optional	The value can be integers between 6 and 8.
Presenter Security Code eventConfCode	Specify Presenter Security Code. In an Event Conference, when you enter the Presenter Security Code, the system assigns you 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.	-

Index

A

abort
  global user settings import job on first error 181
abort a user import job 173
abort global user settings import job on first error 181
about
  CAC administration 268
about Adaptations 269
about Call Routing Testing 549, 581
about Connection Status 511, 594
about Domains 254
about E911 Services 363
About regular expressions 350
about routing policies 329
about Security Module Status 508, 591
about Session Manager Administration 363
about SIP entity references 317
about SIP Firewall 441
about SIP Tracing 547, 578
About the time ranges 324
about Tracer Configuration 543, 575
accessing log harvest 646
accessing scheduler 689
accessing the Backup and Restore service 665
accessing the Data Retention Rules service 677
accessing the Log Settings service 640
access log harvesting 646
access profile 66
activating
  new Identity Certificate 96
activating agent 726
activating serviceability agent 726
Adaptation deletion confirmation
  field descriptions 282
adaptation details 289
adaptation example 277
adaptation module
  Adaptation Details 271
  administration 271
adaptations 288
Adaptations
  deleting 282
adapters
  AT&T Adapter (AttAdapter) 285
  Cisco Adapter (CiscoAdapter) 283
  Diversion Type Adapter (DiversionTypeAdapter) 283
  Verizon Adapter (VerizonAdapter) 284
add
  communication profile for user 104
Add Communication Manager
  field descriptions 59
Add Communication Manager field descriptions 59
adding
  Root CA to Session Manager trusted list 94
  System Manager root certificate to phones 77
  third party root certificate to phones 80
  trusted certificates 81, 85
  users 99
adding a CM Endpoint profile 107
adding a contact in contact list 123
adding a CS 1000 or CallPilot profile 114
adding a CS 1000 profile 114
adding a messaging profile 110
adding an IP Office endpoint profile 116
adding an SNMP target profile 722
adding Applications in an existing Application Sequence 482
adding a RBAC role
  with limited permissions 147
adding a RBAC role with full permissions 148
adding communication profile for user 104
adding communication profiles
  IP Office endpoint 116
adding Root CA
  to System Manager trusted list 94
adding System Manager CA
  to Communication Manager 76
adding third party CA
  to Communication Manager 79
Add Trusted Certificate page 86
admin
  logon information 27
administering
  backup storage configuration 535, 619
  Call History 538, 623
  implicit applications for SIP users 498
  initial setup of the Session Manager 248
  SIP Identity Certificate 95
  SIP Team button 710
  users 97
administering Branch Session Manager 393
administering ELIN Server 377
advanced Searching 517, 522, 601, 606
alarming 625
Alarm List page 630
alarms
  forward to secondary System Manager 628
  standby mode 628
alarms; export 626
alarms; search 627
AMSAdapter 288
appender; modify 643
Application Editor field descriptions 478
application instance
  create 58
  new 58

application management page 64
applications 474
Application Sequence Editor field descriptions 483
application Sequences 480
Application Sequences field description 482
Applications field descriptions 477
applying SIP phone template
to existing user 707
assigning an appender to a logger 642
assigning an RBAC role to a user 149
AT&T Adapter (AttAdapter) 285
Attach Appender page 645
attach contacts page 125
attribute details defined in Delete user XSD 848
attribute details defined in Import User XSD 839
attribute details defined in the CM Endpoint profile XSD 848
attribute details defined in the Conferencing communication profile XSD 883
attribute details defined in the Messaging communication profile XSD 872
attribute details defined in the Session Manager communication profile XSD 879
audit
run on Backup Storage Location 537, 621
Automatic Entity Link Generation 417
AutoRefresh Alarm List page 629
auto-refresh log list page 639
Avaya Media Server Adapter 288
Avaya SIP AST endpoints 131

B

backing up
User Data Storage 536, 620
backup 662–664
remote server 666
backup and restore 662–665
field descriptions for User Data Storage 534, 618
Backup and Restore page 672
backup and restore service; access 665
backup and restore time 664
backup files; view 665
backup file size 663
backup on System Manager and System Platform 665
Backup page 673
backup storage configuration
administering 535, 619
Backup Storage Configuration
changing administration 536, 620
field descriptions 536, 620
Backup Storage location
run audit 537, 621
Branch Configuration 388
Branch Session Manager
adding SIP entities as Branch Session Manager 394
deleting a Branch Session Manager 406
modifying administration settings 401
overview 387
viewing administration settings 400
Branch Session Manager Administration page field descriptions 379
Branch Session Manager page field descriptions 407
bulk export 153, 159
key features 159
bulk export global settings 178
bulk export of global user settings 177
bulk export of users 164
bulk export of users partially 167
bulk export users 163
bulk import 153, 159
global settings options 176
key features 159
sample XMLs 183
schema definitions 183
bulk import and export 153, 159
bulk import and export of user by using Excel file 155
bulk import and export using Excel 153
BulkImportEncryptionUtil 169, 170
bulk import encryption utility 168
Bulk Import example for Adaptations 294
Bulk Import example for Dial Patterns 349
Bulk Import example for Domains 257
Bulk Import example for Entity Links 324
Bulk Import example for Locations 266
Bulk Import example for Regular Expressions 357
Bulk Import example for Routing Policies 338
Bulk Import example for SIP Entities 315
Bulk Import example for Time Ranges 328
bulk import of global user settings 176
bulk import of partial user attributes 166
bulk import users 160
bulk import XML for users with SIP phone 195

C

CAC administration
about 268
administration
CAC 268
CAC
administration 268
CAC Behavior 267
Call Admission Control 267
Call Counts 552
Call Counts Report Types 553
call history 538, 622
Call History
administering 538, 623
Call History administration
using Communication Profile Editor 539, 623
call history management 532, 617
call history status 540, 624
field descriptions 540, 624
call history status screen

call history status screen *(continued)*
viewing 539, 624
Call Routing Test page field descriptions 549, 581
cancel
global user settings import job 182
cancel a global user settings import job 182
cancel a user import job 174
certificate management 74
changing alarm status 626
Changing compatibility view setting 26
Cisco Adapter (CiscoAdapter) 283
client audit 680
CM Endpoint profile
delete 109
CM station data
export 153
import 153
command
exportUpmGlobalsettings 178
exportUpmUser 165
command line restore 672
commands
restricted 713
communication address
modify 105
Communication Manager
add 59
trusting system Manager CA 76
trusting third party CA 79
communication profile
add 104
Presence 106
Communication profile 198
Communication Profile Edit Confirmation page field descriptions 417
Communication Profile Editor 410
administering Call History 539, 623
field descriptions 414
communication profile for user
delete 104
Communication profiles 103
communication profiles for a user 107
communication profile worksheets
communication profile hierarchy 157
hierarchy 157
parent-child communication profile 157
relationship 157
worksheets 157
compatibility mode 26
completed jobs
view 690
Completed Jobs Page 696
Conference Factory 485
Conference Factory Set
adding
setting the parameters 488
deleting 491
editing 490
viewing 490
Conference Factory URI
about 484
configuration 162, 165
configuration options for bulk import of users 165
configuration options for bulk import through Excel 162
configure permissions
to access System Manager web pages 150
configuring
Session Manager Serviceability Agent 717
configuring trap listener 728
Connection Links
monitoring 511, 594
Connections Status
field descriptions 511, 594
contact
add in default contact list 123
modify 123
contact list member
edit 126
contacts
attach 125
copying permission mapping for a role 151
create
log harvesting profile 647
user provisioning rule 134
create a new instance 58
create log harvesting profile 647
Create New Profile page 655
creating
Entity Links 319
new SIP phone template 706
routing policies 330
scheduler operation role 146
SIP phone template from default 706
System Manager backup 665
creating Adaptations 275
creating a Device Settings Group - Location Group 460
creating a Device Settings Group - Terminal Group 461
creating an application 476
creating an Application Sequence 480
creating a new communication address for a profile 105
creating an Implicit User Rule 495
creating an messaging instance 62
creating an NRS Proxy User Rule 499
creating an SNMP target profile 722
creating an SNMPv3 user profile 718
creating data backup on remote server 666
creating dial patterns 343
creating domains 255
creating duplicate user provisioning rule 135
creating duplicate users 122
creating locations 260
creating regular expressions 352
creating SIP entities 298
creating system data backup on a local server 666

creating time ranges 325
creating TPS instance 499
creating user provisioning rule 134
CS1000 Adapter 285
CS 1000 and CallPilot profile administration 113
CS1000 Presence users 116
customizing column display 411, 520, 604

D

dashboard
Session Manager 361
data backup
create 666
remote server 666
data backup; schedule 667
data backup from local server 669
Database size 663
data distribution and redundancy link test 542, 573
Data entry warning in Excel 159
Data entry warning in Microsoft Excel 159
Data link error in Excel 158
Data link error in Microsoft Excel 158
data replication 679, 680
data replication service 679
Data Retention page 678
data retention rules 677
data retention rules; edit 678
data retention rules; modify 678
data retention rules; view 678
data retention rules service; access 677
data server status
field descriptions 533, 617
Deep inspection filtering 442
default contact
add contact list 123
default settings 359
delete
communication profile 104
global user settings import job on first error 182
user provisioning rule 135
delete a global user settings import Job 182
delete a user import job 174
Delete Confirmation Page 704
Delete Confirmation page field descriptions 379
Deleted Trusted Certificate Confirmation page 88
deleted user
restore 122
Delete Local Host Name Entries Confirmation page field descriptions 436
Delete NRS Proxy User rule Confirmation page field descriptions 500
delete Session Confirmation page field descriptions 407
delete SNMPv3 user profiles 719
deleting
Adaptations 282
Branch Session Manager instance 406
Domains 255
locations 261
NRS Proxy User rule 500
Session Manager instance 377
deleting a communication address 106
deleting a communication profile 104
deleting an CM Endpoint profile 109
deleting an SNMP target profile 724
deleting an SNMPv3 user profile 719
deleting a profile 649
deleting a station profile 112
deleting completed jobs 692
deleting contacts from the contact list 124
deleting dial patterns 345
deleting Entity Links 320
deleting IP Office endpoint profile of a user 118
deleting jobs 692
deleting pending jobs 692
deleting regular expressions 354
deleting routing policies 332
deleting scheduled backup job 669
deleting SIP entities 303
deleting SNMP target profiles 724
deleting time ranges 326
deleting user provisioning rule 135
demo certificates 83
installing 83
Denial of Service protection 443
denied locations for Dial Patterns 349
Deny new service for entity links 297, 319
Device Settings Group — Default Group field descriptions 464
Device Settings Group - Location Group field description 467
Device Settings Groups 459
Device Settings Groups field description 463
Device Settings Group — Terminal Group field descriptions 470
dial pattern deletion 345
dial pattern details 347
dial patterns 339, 346
Dial Plan Ranges 342
Dial Plan Transparency 259
Disable Confirmation page 702
Disabling
pending jobs
completed jobs 693
disk space for
System Manager backup 663
displaying SIP entity references 318
documentation
related 20
document changes 19
domain deletion confirmation 256
domain Details 257
domain Management 256
Domains
deleting 255

download
harvested log files 651
SNMP MIB 550, 582
Downloading Excel template 162
downloading harvested log files 651
DRS 679, 680
DRS client audit 680
DRS clients 680
duplicate
UPR 135
user provisioning rule 135
Duplicate User Provisioning Rule
field descriptions 136
duplicating routing entity data 254
duration
backup and restore 664

E

edit
scheduled job 699
Edit Appender page 645
edit contact in a contact list 123
edit contact list member page 126
Edit Element page 66
Editing
pending jobs
completed jobs 668, 691
editing a logger in a log file 642
editing an IP Office endpoint profile 117
editing an SNMP target profile 723
editing an SNMPve user profile 718
editing logger 642
editing password policies 29
editing session properties 30
field description 32
editing SNMPv3 user profiles 718
editing the logon warning banner 30
Edit Local Host Name Entries page field descriptions 435
Edit Logger page 643
edit password policies
field description 31
Edit User Profile 216
Edit User Provisioning RuleView User Provisioning Rule
field descriptions 136
element
create 58
new 58
Element Manager
redirect CallPilot user 113
redirect CS 1000 user 113
Emergency Numbers 341
enable
password strength policy 28
Enabling
pending jobs
completed jobs 693
encrypt passwords 169, 170
endpoint settings
modifying for existing group 708
modifying for existing user 708
enhanced validation certificates
installing 77
Entity Link Connection Status 505, 588
entity links 322
Entity Links 319
creating 319
modifying 320
Example
bulk import and export of user by using Excel file 155
Excel
bulk import 162
Data entry warning 159
Data link error 158
import 153
Excel file
bulk import and export of user 155
import users 183
Excel template
download 162
existing user
applying SIP phone template 707
export
communication profile 164
contacts 164
global user settings 177
user data 153, 159
export alarms 626
export CM station data 153
export global settings 178
exporting
location performance data 555
routing element data 251
Session Manager Certificate 88
System Manager CA 75
exporting analysed call counts data 553
exporting analysed SIP performance data 558
exporting analysed System Performance data 563
export logs 634
export to Excel
user data 153, 159
exportUpmGlobalsettings command, ...178
exportUpmUser command, ...165
export users 163
System Manager UI 164
Export Users 188

F

failback of selected AST devices for Device Registration 517, 600
failback of selected AST devices for User Registration 522, 606
Failover Group 417

Failover Group *(continued)*
adding ... 421
deleting ... 425
editing ... 423
field description
password policies ... 31
field descriptions
Adaptation deletion confirmation ... 282
Add Communication Manager ... 59
Duplicate User Provisioning Rule ... 136
Edit User Provisioning Rule ... 136
Export Users ... 188
Import Global Settings page ... 190
location ... 262
maintenance tests ... 541, 572
Manage Elements ... 64
New User Profile ... 198
New User Provisioning Rule ... 136
session properties ... 32
TrapListener ... 728
User Provisioning Rules ... 136
View User Provisioning Rule ... 136
filtering alarms ... 627
filtering jobs ... 691
filtering log harvesting profiles ... 652
Filtering log harvesting requests ... 653
filtering logs ... 634
filtering of sequenced applications based on media attributes ... 474
filtering SNMPv3 user profiles ... 720
filtering target profiles ... 724
filter users ... 130
Firewall configuration
auditing ... 449, 514, 597
forced unregistration of device registration ... 521, 604
forward the secondary alarms to primary System Manger 628

G

General Guidelines and Capabilities of User Provisioning Rules ... 132
general guidelines for using user provisioning rules ... 133
Geographic Redundancy ... 680
backup and restore ... 664
failure use cases and recovery ... 46
managing Session Manager ... 39
scenarios ... 35
Setting up a Geographic Redundancy enabled system ... 54
System Manager ... 34
System Verification Tests ... 56
terminology ... 35
Upgrading to a Geographic Redundancy-enabled system ... 55
global Settings ... 379
global user settings import job
abort ... 181

H

Harvest Archives page ... 657, 659
Harvest Criteria Edit page ... 656
harvested log files; download ... 651
Hierarchy in communication profile worksheets ... 157
host name resolution test ... 542, 573
HTTP identity certificates
replacing ... 77
HTTPS Identity Certificate
extensions and attributes table ... 90

I

Identity Certificate
activating new ... 96
replacing ... 92
Identity Certificates ... 89
viewing ... 92
Identity Certificates page ... 91
implicit applications
administering for SIP users ... 498
implicit sequencing ... 495
Implicit User Rule Editor field description ... 497
Implicit User Rules field description ... 496
Implicit Users ... 495
import
user data ... 153, 159
import CM station data ... 153
import from Excel
user data ... 153, 159
Import Global Settings page ... 190
import job on the Scheduler page
view ... 175
import of users ... 162, 165
Import Routing Data ... 253
import user considerations ... 171
import users ... 160
Import Users ... 183
Inactive session termination policy ... 29
initial setup of the Session Manager ... 248
installing
demo certificates ... 83
enhanced validation certificates ... 77
third party certificates ... 80
Internet Explorer
compatibility view setting ... 26
investigating
Security Module status ... 509, 591
IP Office endpoint profile ... 116
delete ... 118
edit ... 117
view ... 117

J

Job Details page ... 186, 190

Job Scheduling -Edit Job page 699
Job Scheduling -On Demand Job page 701
Job Scheduling -View Job page 698

K

key features
bulk export 159
bulk import 159

L

legal notice .....
list of XML Schema Definitions and Sample XMLs for bulk import 736
Local Host Name Resolution page field descriptions 433
local Performance Data Storage 568
location
field descriptions 262
location deletion 261
location details 262
location performance 554
location performance Report Types 555
locations 258
deleting 261
location Settings 473
Location Settings field description 473
lockout policy
password 29
Log; log settings 640
log details; view 633
log file; search for text 650
logger; edit 642
Logging Configuration page 641
logging on to System Manager
admin 27
Logging page 635
logging to System Manager 27
log harvest; access 646
log harvester overview 646
Log Harvester page 654
log harvesting 646
log harvesting profile
create 647
log harvesting profile; view details 648, 653
log harvesting profiles; filter 652
log harvest requests; filter 653
logon banner 30
logon information
admin 27
logon warning banner 29
edit 30
logs; export 634
logs; log viewer 633
logs; search 635
Log Settings 640
Logs Settings service; access 640
Log Viewer 633

M

maintenance tests 540, 541, 572, 573
Test Call Processing status 542, 573
Test sanity of Secure Access Link (SAL) agent . 542, 574
maintenance tests page
field descriptions 541, 572
managed bandwidth
viewing usage 506, 589
managed bandwidth usage 506, 589
Managed Bandwidth Usage 507, 589
Manage Elements field descriptions 64
management link functionality test 542, 574
managing
users 97
managing SNMPv3 user profiles 726
managing target profiles 727
managing user profiles 726
map permission 151
messaging data
synchronize 64
MIB 729
modify
communication address 105
user provisioning rule 134
modify appender 643
modifying
Branch Session Manager administration settings 401
endpoint settings for existing group 708
endpoint settings for existing user 708
Entity Links 320
Session Manager administration settings 370
modifying a CM Endpoint profile 108
modifying a CS 1000 or CallPilot profile 116
modifying Adaptations 280
modifying a Device Settings Group - Location Group 461
modifying a Device Settings Group - Terminal Group 462
modifying a messaging profile 111
modifying an appender 643
modifying an application 476
modifying an Application Sequence 481
modifying an existing Implicit User Rule 496
modifying an IP Office endpoint profile 117
modifying an NRS Proxy User Rule 500
modifying Communication Profiles 412
modifying contact in a contact list 123
modifying data retention rules 678
modifying dial patterns 344
modifying domains 255
modifying locations 260
modifying Location Settings 473
modifying regular expressions 353
modifying routing policies 331
modifying SIP entities 301
modifying SNMPv3 user profiles 718

modifying the communication address 105
modifying the default settings 357
modifying time ranges 325
modifying user account 119
modifying user provisioning rule 134
Modular Messaging Adapter 288
monitoring
Connection Links 511, 594
Multi Device Access 103
Multilocation Dial Plan 343
multiple SIP endpoints
register 103
Multi Tenancy
Avaya SIP AST endpoints 131

N

NCS 498
network connections test 543, 574
New Element page 66
new Identity Certificate
activating 96
New Local Host Name Entries page field descriptions 434
New log harvesting profile 655
New SIP phone template
creating 706
New User Profile page 198
New User Provisioning Rule
field descriptions 136
NIC bonding 364
nodes; remove 683
notifications 734
NRS Proxy User Rule Editor field description 501
NRS Proxy Users 498
NRS Proxy Users field description 501

O

on-demand job 688
OPTION Requests 297
Orange Adapter 287
overview of SIP entity references 318

P

Password aging policy enforcement 28
password history enforcement policy 29
password lockout policy enforcement 29
password policies
edit 29
password policies field description 31
password policy; logon warning banner 29
password strength policy enforcement 28
pattern list 337
PCNs
viewing 734
PCN updates 734
peer SIP entities
adding 426
managing 426
removing 428
pending jobs
view 690
pending jobs; stop 694
pending jobs; view 689
Pending Jobs page 694
performance Data Collection 566
Performance Data Collection field description 569
Port 66
Postgres database sanity test 542, 574
pre-administration
for Session Manager profile 97
pre-configuration template
for SIP phones 705
Presence communication profile administration 106
product notification enrollment 735
product notifications
e-notifications 735
profile
delete 649
Profile Criteria View page 656
provision
users 131
PSNs
viewing 734
PSN updates 734
Purpose and usage of SIP subscriptions 463

Q

quick start to importing users 193

R

RBAC permissions
Bulk Communication Profile edits 146
Local Host Name Resolution 146
routing import/export 145
rearranging Applications in an Application Sequence 481
rebooting of selected AST devices for Device Registration 516, 599
rebooting of selected AST devices for User Registration 521, 605
recommendations for data backup 665
redirect
CallPilot user to Element Manager 113
CS 1000 user to Element Manager 113
redirecting CallPilot user to Element Manager 113
redirecting CS 1000 to Element Manager 113
redirecting UNIStim Phone 498
register
multiple SIP endpoints 103
registration Summary 515, 599

Registration Summary field description 518, 601
Regular Expression constructs 351, 714
regular expression deletion 354
regular expression details 355
regular expression list 338
regular expressions 354
related documentation 20
Reloading of selected AST devices for device registration 516, 600
Reloading of selected AST devices for User Registration 521, 605
Remote Access
    Session Manager 436
Remote Access configuration
    creating 436
    deleting 437
    modifying 437
Remote Access Configuration page field descriptions 440
Remote Access page field descriptions 440
Remote Worker
    core redundancy 438
remove replica node from queue 683
remove user account 120
removing
    SIP phone template 709
    trusted certificates 87
removing access permissions
    for Session Manager and Routing web pages 152
removing an appender from a logger 643
removing an association between a subscriber and a user 111
removing a node 683
Removing applications 477
Removing Application Sequences 481
removing association between an endpoint and a user 109
removing deleted users from database 121
Removing Device Settings Groups - Location Groups 461
Removing Device Settings Group - Terminal Group 462
removing existing Implicit User Rules 496
repairing a replica node 681
Replace Identity Certificate page 92
replace identity certificates field descriptions 92
replacing
    HTTP identity certificates 77
    Identity Certificate 92
    SIP identity certificates 77
replacing identity certificates
    field descriptions 92
replica group; remove nodes 683
replica group; remove replica node from queue 683
replica groups; view 681
Replica Groups page 683
Replica Nodes page 684
Replication Node Details page 686
resolving
    local host name 429
restore 662
restore deleted user 122
restore on System Manager Geographic Redundancy 664
Restore page 676
restoring
    default SIP Identity Certificate 96
    User Data Storage 536, 621
restoring a backup from a remote server 670
restoring a system backup from a local server 669
restoring backup; remote server 670
restoring data backup 669
restoring the backup data through CLI 672
restoring through command line 672
restricted commands 713
role
    copy permission mapping 151
Role Based Access Control 144
root certificate
    adding to phones 77
routing
    of a call using routing policy data 247
    prerequisites for Routing Setup 246
    Routing overview 246
    Session Manager 246
Routing
    about 246
    exporting and importing element data about 249
    import job operations 252
    import job scheduling 252
routing element data
    exporting 251
routing policies 333
    creating 330
routing policy deletion 332
routing policy details 334
routing policy list 356
Rule page field descriptions 454
rule precedence and traversal 442
rules 131
Rule Set
    assignment of Rule Sets
        all Branch Session Managers 447
        all core Session Managers 447
        all core Session Managers and Branch Session Managers 448
    deletion 447
    duplication 446
    modification 446
    selecting Session Managers and Branch Session Managers 449, 513, 596
    selecting Session Managers and Branch Session Managers for Rule Set assignment 448
    viewing 446
    viewing assigned Session Managers and Branch Session Managers 448
Rule Setcreate 443
Rule Set page field descriptions 451
running

running *(continued)*
maintenance tests 541, 573

S

sample XML file for a user with SIP Communication Profile 197
sample XML files
for bulk import 155
sample XMLs
for bulk import 183
sample XML with a single user profile 194
saving
Global Session Manager settings 378
saving configuration changes 254
schedule
on-demand job 688
schedule a user import job 171
Schedule Backup page 675
schedule data backup; remote server 667
scheduled backup job
deleting 669
scheduled job
edit 699
scheduled jobs
completed 696
scheduler 688
scheduler; access 689
scheduler operation role
creating 146
scheduler service 688
scheduling a data backup on a local server 667
scheduling a data backup on a remote server 667
scheduling a global user settings import job 179
schema definitions
for bulk import 183
Search Archives page 659
searching contacts on Avaya SIP AST endpoints 131
searching for alarms 627
searching for a text in a log file 650
searching for logs 635
searching logs 635
searching users 131
secondary server alarms
view 628
security management 74
Security Module Reset Confirmation page field descriptions 511, 594
Security Module status
investigate 509, 591
Security Module Status
field descriptions 510, 592
security module status page actions 508, 591
security module status test 543, 574
security settings 30
serviceability agent
activate 726
serviceability agents list 727
Session license usage 530, 614
Session Manager
adding SIP entities as Session Manager 364
deleting a Session Manager instance 377
local host name resolving 429
managed bandwidth viewing usage 506, 589
modifying administration settings 370
remote access 436
routing 246
viewing administration settings 370
Session Manager Administration page field descriptions 379
Session Manager Certificate
exporting 88
Session Manager Communication profile administration 102, 103
Session Manager Dashboard 361
field descriptions 361
Session Manager Entity Link Connection Status 505, 587
Session Manager page field descriptions 382
Session Manager profile
pre-administration 97
Session Manager trusted list
adding Root CA 94
session properties; edit 30
session properties field descriptions 32
Session termination policy 29
SIP Call Loop 298
SIP elements
authentication 296
TLS layer validation 296
SIP entities
IP and transport layer validation 296
SIP Entities
description 295
SIP entity 305
SIP entity deletion 303
SIP Entity details 306, 310
SIP entity link deletion 321
SIP Entity Link Monitoring Status 504, 586
SIP entity list 336
SIP Firewall
blacklist 441
creating a new SIP Firewall rule 445
default Rule Set 441
rules 441
status 443
whitelist 441
SIP Firewall Configuration page field descriptions 450
SIP Firewall Status page field descriptions 458, 514, 597
SIP Identity Certificate
administering 95
extensions and attributes table 89
restoring the default 96
SIP identity certificates
replacing 77
SIP monitoring

SIP monitoring *(continued)*
viewing the SIP Monitoring Status Summary page 503, 586
SIP Monitoring 502, 585
SIP Performance 557
SIP Performance Report Types 558
SIP phone
pre-configuration template 705
SIP phone template
apply to existing user 707
creating from default 706
removing 709
SIP responses
handling 247
SIP Team button 710
administering 710
SNMP attributes 66
SNMP MIB 729
download 550, 582
SNMP support 716
SNMP target profile
add 722
edit 723
SNMP target profile; view 723
SNMP target profile list 724
SNMP target profiles; delete 724
SNMP target profiles field descriptions 725
SNMP traps 728
SNMP user profile list 720
SNMPv3 user profile; add 718
SNMPv3 user profile; create 718
SNMPv3 user profile; delete 719
SNMPv3 user profile; edit 718
SNMPv3 user profile; filter 720
SNMPv3 user profile; view 719
SNMPv3 user profiles
assign 726
manage 726
SNMPv3 user profiles field description 721
Stop Confirmation page 703
stopping Communication Profile editing jobs 413
stopping import jobs 430
stopping pending jobs 694
submitting a request for harvesting log files 649
support 22
Survivable Public Remote SIP Trunking
about 388
administration 393
call scenarios 390
synchronization 680
DRS clients 680
synchronizing
CM data 63
Communication Manager and System Manager 58
configuring options 63
synchronizing CM data 63
synchronizing messaging data 64
synchronizing System Manager master database and replica computer database 681, 682
system
scheduled job 688
System Manager
adding CA to Communication Manager 76
Geographic Redundancy 34
overview 24
System Manager backup 665
System Manager CA
exporting 75
using 75
System Manager Geographic Redundancy 34
System Manager login 27
System Manager trusted list
adding Root CA 94
System Manage UI
export users 164
System Performance 562
System Performance Report Types 563

T

target profile; manage 727
target profiles
edit 723
target profiles; delete 724
target profiles; filter 724
target profiles field descriptions 725
tenant partitioning
Avaya SIP AST endpoints 131
third party CA
using 78
third party certificates
installing 80
third party root certificate
adding to phones 80
time range deletion 326
Time Range List 327, 336
time ranges 326
TLS version
viewing 83
Tracer Configuration page field descriptions 544, 575
Trace Viewer 547, 579
TrapListener 728
field descriptions 728
Trap listener field description 728
TrapListener service 728
Traplistener service; alarming UI 728
TrapListener service; configure 728
trusted certificates
adding 81, 85
removing 87
viewing 84
Trusted Certificates page 88
trust management 74
turn off compatibility mode 26

two-tier routing 417
Two-Tier Routing 418

U

unassigning the RBAC role from a user 152
UPM 103
UPR
    duplicate 135
user
    restore 122
user account
    remove 120
user data storage 532, 617
User Data Storage
    backing up 536, 620
    backup and restore 534, 618
    restoring 536, 621
User Data Storage backup
    overview 534, 618
user data storage sanity test 543, 575
user data storage status screen
    viewing 533, 617
User Delete Confirmation page 245
user details; view 119
user import job
    cancel 174
    delete 174
    schedule 171
user management 97
User Profile Edit page 216
User Profile View page 232
user provisioning rule 131
    create 134
    delete 135
    duplicate 135
    modify 134
    view 135
User Provisioning Rule 198
User Provisioning Rules
    field descriptions 136
User Registrations 519, 602
User Registrations field description 523, 607
users
    adding 99
    bulk export 164
users; filter 130
using
    System Manager CA 75
    third party CA 78
using init -d 83
utility
    bulk import encryption 168

V

Verizon Adapter (VerizonAdapter) 284
Verizon ANI Feature 284
videos 22
view
    global user settings import job details 180
    import global user settings job 181
    secondary server alarms 628
    user import job details 175
    user provisioning rule 135
view an import global user settings job 181
view an import global user settings job on the Scheduler page 181
view backup files 665
view completed jobs 690
view contact list member page 128
view contents; log harvested files 651
view details; log harvesting request 650
view details of a global user settings importing job 180
view details of import job 180
View Element page 66
viewing
    call history status 539, 624
    Communication Profile edit failures 413
    failed job entries 430
    Identity Certificates 92
    PCNs 734
    PSNs 734
    SIP Monitoring Status Summary page 503, 586
    TLS version 83
    trusted certificates 84
    user data storage status 533, 617
viewing alarms 626
viewing a messaging profile of a user 111
viewing an SNMP target profile 723
viewing an SNMPv3 user profile 719
viewing applications 476
viewing application sequences 480
viewing a station profile of a user 108
viewing background edit job status 412
viewing call counts data 552
viewing Communication Profiles 411, 566
viewing data retention rules 678
viewing deleted users
    view deleted users 121
viewing details of a log harvesting profile 648, 653
viewing details of a log harvesting request 650
viewing details of a user 119
viewing Device Settings Groups 460
viewing harvested log files in an archive 648
viewing Implicit User Rules 495
viewing import job status 429
viewing IP Office endpoint profiles 117
viewing list of backup files 665
viewing location performance data 554
viewing location settings 473
viewing log details 633
viewing loggers for a log file 641
viewing pending jobs 689

viewing Registration Summary 516, 599
viewing replica groups 681
viewing replica node details 682
viewing replica nodes in a replica group 681
viewing replication details for a replica node 682
viewing SIP performance data 557
viewing system performance data 562
viewing the contents of harvested log files 651
viewing the details of a contact in the contact list 124
viewing user provisioning rule 135
viewing User Registrations 519, 603
view log details 633
view loggers 641
view log harvested files; archive 648
view logs
    completed jobs 690
    pending jobs 690
view replica groups 681
view secondary server alarms 628
view the details of a user import job 175
View Trust Certificate page 84
view user import job on the Scheduler page 175

W

warning
    data entry in Excel 159
warranty 23
Well Known Conference URI
    adding 486
    editing 487
    removing entry 488

X

XML file
    import users 183
XML for user with core attributes 193
XML Schema definitions 155